EC-Council

C|CISO

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

VERSION 3

Join the New Generation of Information Security Leaders

CEI Material

Certified Chief Information Security Officer

This Edition

This CCISO Body of Knowledge represents a significant effort on the part of the authors and editors. These industry leaders, as you will see from the bios provided in the following pages, are volunteers who were provided with the opportunity to share their knowledge and experience. We at EC-Council are grateful for their hard work and dedication.

The CCISOs who helped write this book collectively have *over 390 years of experience.* They individually have an average of over 22 years of knowledge they are sharing within this edition of the CCISO Body of Knowledge. This provides you with access to a powerful volume of materials consisting of executive-level guidance and a deep perspective of the role of a leader within the security profession. Eighteen authors and editors have delivered this volume of management and program knowledge that enables you to create robust security programs and portfolios of services. This will enable you to meet the needs of the business and manage complex capabilities according to proven methodologies focused on *how* you perform the role of a security leader.

Our goal is to provide the highest quality of program materials across the various parts of this certification that reflect the value expected by industry executives. This level of quality is enabled by committees organized according to their four primary supporting functions within the CCISO Program:

- A Scheme Committee that determines the tasks and knowledge required by security leaders and executives.
- An Exam Committee is responsible for reviewing all available materials and creating test questions to ensure the knowledge of aspiring CCISOs meets the standards of this certification.
- A CCISO CEI Committee consists of CCISO course instructors who deliver classroom training and exercises, ensuring the materials are current and applicable.
- And lastly, the CCISO Body of Knowledge (BoK) Committee is responsible for this book's content.

Over 70 CCISO global volunteers are currently working within these committees to make sure this certification consists of materials that are not only current and relevant to the security executive leader but also clearly organized and delivered in the most professional manner possible.

From all of us – thank you, and welcome to this community of professional security leaders.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein or perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use or reliance of this material.

C|CISO BODY OF KNOWLEDGE

EC-Council Executive Management:

Sanjay Bavisi, President

Steven Graham, Sr. Vice President

Sean Lim, Sr. Vice President

Eric Lopez, Vice President

EC-Council C|CISO Body of Knowledge Editing and Management:

Keith Rayle, Senior Director of C|CISO

Authored By:

Keith Rayle, Senior Director of C|CISO

Chris Campbell, Sr. Director of Information Security public company, Committee Chair EC-Council BOK Committee

Vincent Lewis, Cloud Security Engineer Information System Security Manager, Dept. of the U.S. Air Force, Committee Vice-Chair EC-Council BOK Committee

Ayodeji Akinola, Senior Security Consultant for Mariner Partners Inc.

Jeffrey Aschenbach, Chief Information Security and Privacy Officer, Cooler Screens Inc.

Dr. Jerry Craig, Chief Information Security Officer, Ntiva, Inc

Dr. Thomas "Tom" Duffey, ITEGRITI Director Cybersecurity and Compliance

Justen Dyche, Head of Information Security Delivery, BBC

Brandon Gettert, Founder and CEO of Curated Cyber

Jorge L Gomez, Cloud Security Architect/Engineer, Twilio

Corlette Grobler, Chief Information Security Officer, HAYVN

Karin Höne, Group Chief Information Security and Risk Officer at a South African multinational

Federico Iaschi, Head of Cyber Security Resilience & Observability, Virgin Media 02

Jari Kiero, Senior Resilience Officer, Allianz Technology SE

Paul Lynch, Senior Director of Information Security and Infrastructure, CubeSmart Self Storage

Peter Pandula, Senior Advisor, BMO Financial Group

Daniel Pinsky, CSO & Head of Security Governance and Compliance, CDW Canada

Keyaan Williams, Managing Director, CLASS-LLC

Bjoern Voitel, Owner and CEO of three information security companies

Edited By:

Keith Rayle, Senior Director of C|CISO

Vincent Lewis, Cloud Security Engineer Information System Security Manager, Dept. of the U.S. Air Force, Committee Vice-Chair EC-Council BOK Committee

Chris Campbell, Sr. Director of Information Security public company, Committee Chair EC-Council BOK Committee

Ayodeji Akinola, Senior Security Consultant for Mariner Partners Inc.

Jorge L Gomez, Cloud Security Architect/Engineer, Twilio

Preface

The advancement of the security executive role in corporate governance has followed proportionately with the increase in criminal activities focused on critical data and systems supporting public and private organizations. The velocity, creativity, and focus of cyberattacks continues to escalate, resulting in the need for clear executive leadership that delivers the ability to enable resilient business outcomes. Within two decades, the role of the Chief Information Security Officer has grown from being rarely seen beyond financial or government institutions to the current state in which many globally recognized regulatory agencies specify the presence of strategic security leadership to satisfy compliance requirements. A properly functioning security capability has become critical for the successful transaction of all forms of business. Security executives are now required to apply clearly defined, organizationally aligned portfolios that deliver focused capabilities to identify, communicate, and manage cyber risk according to the needs of the organization. Fulfilling the role of a leader within the security industry requires the ability to orchestrate people, technologies, and processes into a highly functioning, highly efficient portfolio of services and capabilities purposefully implemented to protect critical assets.

Today's Chief Information Security Officer must rely on a wide range of tools to be successful. True security leadership requires deep dedication to the security industry, years of technical and non-technical security program experience, visibility into the constantly changing threat landscape, and the ability to create strategies and implement them according to a carefully planned schedule. Successful security executives also need deep knowledge of business operations, a wide perspective of industry trends, strong leadership capabilities, and communications skills that are effective throughout all organizational levels and up to the Board of Directors.

EC Council's C|CISO Program is defined, designed, and delivered by seasoned security executives. The dozens of individuals that contribute their time and knowledge for this program have led security teams, created strategies, regularly briefed at the Board level, and delivered complex capabilities orchestrated to protect critical assets and infrastructure. Their dedication to the security profession is evident within the materials of the C|CISO Program. EC Council's dynamic knowledge model and delivery methodology not only provides you with the necessary tools to realize your career goals, but also provides assurance of the value of this certification through the hundreds of years of deep security leadership experience behind this program.

Welcome to your future as a security industry leader.

Foreword

A 2023 Perspective

Hello to my fellow global C|CISOs!

2023 was an interesting year full of challenges for security executives for a variety of different reasons. The most interesting shift (in my opinion) from our perspective was not necessarily encapsulated within the topics of technology, cyberattacks, or changes in the demand for security expertise. Don't get me wrong – they were all important factors within the security landscape of 2023.

Technology certainly advanced, providing a wide range of new ideas that, over time, will resolve into stand-alone mainstream solutions or become integrated into similar verticals of products. However, I think the velocity of those types of changes has been somewhat predictable and certainly provide security professionals with the usual choices…adopt early, delay until a certain degree of maturity exists, or 'wait-and-see' to determine if the technology matures into steady mainstream usage. It seems that technology was relatively consistent with what one would expect to see from an innovation perspective. One example is cloud technologies. Cloud security capabilities, such as security management platforms, instance baseline templates, and access brokering have become mainstream and are often 'baked in' to the foundational cloud vendor offering. Another technology, Artificial Intelligence (AI), has been integrated into a wide range of products (or, in some cases, only the marketing materials). Quantum computing is mostly relegated to research while stability issues are resolved, hindering availability of commercially viable platforms. Overall, I do not see a technology that has radically redefined our approach to security in this past year.

Criminal activities have remained relatively consistent with expectations, and ransomware leads the list of cyber concerns from the business perspective (much as it has for the past few years). There are some advances, but nothing apart from what one would expect. More successful attacks are being experienced (and particularly at the lower end of the business-size scale), payouts are larger, the attacks are more violent and vicious in nature, and cybercriminal organizations seem more…organized. But the primary methodology of a successful ransomware attack remains relatively consistent: successful phishing or other unauthorized access attack allows vulnerable technology implementations to be leveraged for broader manipulation of critical systems and information. Digital currencies still enable transactional ransom resolution. Meantime, nation/state actors continue to increase their negative global impact as they continue stealing national secrets, intellectual property, and personal information. Some are certainly better at it than others, but activity continues along a somewhat expected trend line of proliferation and capability.

Security expertise shortages continued throughout 2023, with most open labor requisition estimates following trends as we have seen for the past 10 years. Clusters of technologies, such as cloud, continue to morph and evolve, but demand for security professionals within the tech towers seems to have remained relatively constant. Worth noting is an estimated 333K technology workers were laid off over the 22-month period of January 2022 through October of 2023. My suspicion for cause is the mainstream and rapid transition to cloud as a primary factor. This shift appears to have created pockets of competition for open security roles that can make the shortage appear somewhat antithetical. Artificial Intelligence (AI) is hitting stride, but security skills specifically focused on it do not represent a major shift in the percentages of high-demand security skills within this industry. Core capabilities and resources, such as security analysts, risk program resources, forensics experts, and others, fall into similar demand as we have seen in the recent past.

Security management has not radically changed. Organizations still need executives that can create and integrate strategies that align closely to the business goals while meeting the needs of the workforce, senior leadership, and the Board of Directors. Chief Information Security Officers communicate in terms of risk to the business and advise accordingly. Regulatory measures regarding security and privacy increase at an expected rate. Security executives build programs based on relatively static frameworks and standards. Security executives still manage their security program regardless of resource challenges. The trend towards DevOps and DevSecOps continues, underscoring the importance of security leadership working collaboratively with their software development and engineering counterparts to enable cyber risk controls within applications and cloud-centric environments. There is one thing that has changed in the past couple of years from a leadership perspective – the need to effectively deliver the portfolio of security services using, for the most part, a distributed workforce.

I think the most significant recent change impacting the security landscape was the safe enablement of the decentralized workforce. The 2020 pandemic has, for all practical purposes, changed the business operational model significantly (and, it appears, permanently). As a rule (with exceptions, of course), employees no longer spend the hour or so to get ready for the day and commute to a mandatory place of work, then leave the workplace for the day. Now they log in remotely from the house, apartment, or some other convenient location. They communicate via email and instant chat, collectively gather as groups using online meetings, and use collaboration tools to rapidly accept and complete assignments individually or within groups. And they can do this from anywhere.

We have had Work-From-Home (WFH) capabilities for years, but they have now become centrally critical to conducting business and retaining skilled resources. We have settled into the new norm.

2023 brought about the implementation and overall user community acceptance of integrated security controls supporting the WFH model. Security solutions focused on remote endpoints have deployed at an accelerated and expanded pace, being pushed downward into smaller sized organizations and throughout all levels of business sizes. Safe remote connection was enabled through the implementation of security guardrails within externally facing services such as VPN, web services, and remote desktop protocols. We leveraged virtualized environments on a much broader scale. Multi-Factor Authentication (MFA) is nothing new but is foundational for securing the WFH model. We are seeing a shift to password-less authentication models to further ease password fatigue among remote workers - while retaining MFA levels of protection.

Endpoint Detection and Response, coupled with managed services (EDR/MDR), has become mainstream. An interesting shift in thinking has occurred due to expanded MDR adoption. We have come to terms with integrating external entities into another facet of operational security models. Security professionals and the broader business have more readily embraced 3rd party monitoring, management, and issue containment at the mobile endpoint (to include BYOD).

Mobile device management is used not only to protect sensitive corporate data, but it is also being leveraged to push other controls such as removing local administrative rights, pushing rapid patches and updates across OS and applications, and forcing regular reboots and sign-ins. Through endpoint management systems we have deeper visibility into the security status of our user base and faster access to logs for analysis of potential issues.

I think 2023 was the year of maturing and integrating foundational endpoint security in support of the WFH model. Let's see what 2024 brings.

Keith Rayle

Senior Director, C|CISO Program

November 2023

The EC-Council Certified CISO Program

EC-Council developed the Certified Chief Information Security Officer (C|CISO) Program to fill a gap within the information security industry. At that time, security certifications focused on technical skills, historic security perspectives, specific tools, or narrow practitioner responsibilities such as risk or compliance program support. There needed to be a clear path from security practitioner to the executive leadership role. No certifications recognized the knowledge, skills, and capabilities required of the security executive role. More shared knowledge was needed to direct experienced information security professionals to the level of performing the duties of an effective, competent security industry leader. At that time, there were more questions than answers about what being a CISO meant. It wasn't easy to communicate the real value of the security executive's contribution to an organization's success.

EC-Council created the C|CISO Program to bridge the gap within the security profession and enable a clear path to the role of an executive-level security professional. This certification is aligned closely with the overall leadership trend of the security industry. Today, the CISO is a global business enabler, creating information risk management capabilities that help define organizational strategies and success factors. International laws, regulations, and standards often mandate the security leadership role. EC-Council's C|CISO Program meets the needs of the security leadership profession by providing the tools, knowledge, and capabilities to protect against today's cyber threats.

The C|CISO Program uses four core pillars of knowledge transference to enable qualified individuals wishing to attain this certification. They include classroom instruction, a blueprint for defining an organized hierarchy of C|CISO capabilities, the certification examination, and this Body of Knowledge.

The Body of Knowledge represents the foundational skills and knowledge required to be a successful security executive. It also represents decades of direct security leadership experience provided by the C|CISO Body of Knowledge Committee, which consists of current C|CISOs and seasoned security executives from multiple industries and regions worldwide. With their input to this Body of Knowledge, these experts provide a clear view into the C|CISO role and security program capabilities this person needs to deliver within an organization.

The C|CISO Program consists of five domains that provide deeper insight into the foundational capabilities of a successful security executive:

- Domain 1 – Governance & Risk Management (Policy, Legal & Compliance)
- Domain 2 – Information Security Controls, Compliance, and Audit Management
- Domain 3 – Security Program Management and Operations
- Domain 4 – Information Security Core Competencies
- Domain 5 – Strategic Planning, Finance, Procurement and Vendor Management

The details within these five domains of the C|CISO Program provide the basis for being an effective information security program leader.

EC-Council enhances this program by offering additional professional insight from certified instructors via in-classroom, remote attendance, or self-study (video) training. Materials used for instruction, like this Body of Knowledge, are maintained by a committee of deeply experienced security executives with the C|CISO title. A global community of professional instructors actively teaches the C|CISO course, imparting knowledge based on years of experience within the security leadership profession.

EC-Council then evaluates the knowledge of C|CISO candidates with a rigorous exam that evaluates competence across the five domains representing a seasoned security leader's knowledge base. The C|CISO Examination Committee, also consisting of deeply experienced C|CISOs, creates questions for use within the tests. These questions are based on their knowledge of all C|CISO Program materials and years of executive leadership experience in security.

The C|CISO Scheme Committee provides two primary functions. The C|CISOs within it maintain the C|CISO Blueprint and Job Task Analysis catalogs of the knowledge required by security executives. This committee, consisting of C|CISOs with deep leadership experience, reviews and approves questions for inclusion in the C|CISO certification examination.

The C|CISO Program was the first to offer a security industry certification recognizing an individual's accumulated skills for developing, executing, and leading an information security management strategy. The C|CISO certification demonstrates an information security leader's commitment to the profession. It provides assurance they have the foundational knowledge and skills to help protect the organization against the ever-growing attacks against critical infrastructure and data. C|CISOs know how to identify and communicate risk, implement security strategies, adapt to threats, and align security programs to broader strategic goals. EC-Council C|CISOs are the critical leadership component for protecting globally connected organizations and businesses.

Acknowledgments

While many people contributed to this Body of Knowledge, the EC-Council would like to thank the principal authors of the work.

Keith Rayle

Keith has functioned as CISO in large multinational corporations, designed and implemented security governance programs, and created risk management approaches for organization operations and specific programs such as large mergers and acquisitions.

Keith advises multibillion-dollar private equity firms and has delivered multimillion-dollar security engagements comprised of multiple discreet technical and non-technical projects. He has provided executive security consulting in every industry on a global basis. Keith has a Bachelor of Science degree in Computer Science and a Master of Science degree in Information Systems.

Chris Campbell

As chairperson for the EC-Council Body of Knowledge Committee, Chris brings seasoned information security leadership with over 23 years of experience in technology and cybersecurity across the energy, financial, and real estate sectors. He is currently the Senior Director and Head of Information Security and Compliance for a publicly traded financial technology company.

He was previously a cybersecurity leader for a Fortune 150 energy company within the U.S. critical infrastructure. He has an M.S. in Management Information Systems and a B.A. in Finance and Marketing from Florida International University. He holds the C|CISO, CISM, CRISC, CDPSE, CISA, CISSP, CHFI, and GCIH industry certifications.

Vincent Lewis

Committee Vice-Chair for the EC-Council Body of Knowledge Committee, Vincent is a United States Air Force retired IRAQI war veteran with over 23 years of cyber security experience. He currently performs the role of Cloud Security Engineer and Information System Security Manager for the Department of the Air Force, protecting government information traversing commercial cloud providers. He also performed the NIST Risk Management Framework, governance, compliance, and regulation work for the Department of the Air Force global cloud instances.

He has a Master of Arts degree in Management and Leadership with an emphasis in Cybersecurity, a Master of Science degree in Cybersecurity, a Graduate level certificate in cyber threat detection, and a bachelor's degree in information technology. He holds the C|CISO, CISSP, Security+, and Microsoft Certified Professional industry certifications.

Ayodeji Akinola

Ayodeji is an Information Technology enthusiast with a bias for security and over 20 years of experience working across various verticals, including telecommunications, insurance, and finance. He currently works as a senior security consultant for Mariner Partners Inc. Earlier in his career, he worked for IBM and Wipro Limited in various roles.

He graduated from Obafemi Awolowo University, Nigeria, with a bachelor's degree in civil engineering. He has since pivoted fully into Information Technology and Security. He holds industry certifications such as the C|CISO, C|EH, CISSP, Microsoft Certified: Azure Solutions Architect Expert, and AWS Certified Solutions Architect – Associate, amongst others. He is also PMP certified.

Jeffrey Aschenbach

Jeffrey is an accomplished Information Security, Compliance, and Data Privacy leader with over 20 years of experience in the financial service, healthcare, manufacturing, and, most recently, advertising industries. He currently sits as the Chief Information Security and Privacy Officer for Cooler Screens Inc.

Before joining Cooler Screens, he was an influential Vice President of Global IT Security for Mediaocean, a Vista Equity Partners Company. He has a B.S. in Organizational Leadership and Supervision with an emphasis on Computer Information Systems Technology from Purdue University. He holds the C|CISO, CISSP, and CISA industry certifications.

Dr. Jerry Craig

A 20+ year IT management and security career recognized for innovation and strategic direction. Dr. Craig is the Chief Information Security Officer (CISO) at Ntiva, Inc., a large Managed Service Provider (MSP) based out of the Northern Virginia area, where he serves as the corporate CISO, as well as a virtual CISO to his clients. He was formerly the Vice President of Security Systems for a $1B+ intellectual property-led healthcare solutions provider. Dr. Craig has led a distinguished career driving concurrent programs and projects and building and leading teams of security professionals. He is recognized for developing and implementing strategies for growth while reducing organizational risk and expenditures.

Dr. Craig is a trusted advisor to CEOs, Boards of Directors, and C-Suite executives. In addition to his IT career, Dr. Craig has a 14+ year career in higher education, supporting multiple universities with student recruitment and teaching and providing positive mentorship outreach to ensure student success and inspire the next generation of leaders. Dr. Craig informally serves as a Chief Data Officer (CDO) and Chief Privacy Officer (CPO) for numerous clients and extensively participates on the Business Development Team supporting proposal efforts.

Dr. Thomas "Tom" Duffey

ITEGRITI Director of Cybersecurity and Compliance. Dr. Tom specializes in critical infrastructure cybersecurity and regulatory compliance for the energy (utilities and oil & gas), defense, and healthcare sectors. He has over 30 years of experience in different roles and is passionate about protecting operational technology (OT) and the Internet of Things (IoT) for various industries. Dr. Tom's diverse consulting, training, and project management experience also includes supporting multiple military branches at numerous CONUS and OCONUS facilities across the globe. Dr. Tom currently resides in Houston, where he leads OT/IT/IoT critical infrastructure protection delivery efforts for multiple ITEGRITI clients, assisting them with their cybersecurity and compliance needs, including NERC CIP and TSA SD02 regulatory criteria.

Teaching and learning are two of Dr. Tom's biggest passions. He contributed to numerous security thought leadership efforts, including co-authoring a World Economic Forum whitepaper and co-leading domain rewrites for the EC-Council C|CISO Body of Knowledge. Dr. Tom earned his Doctoral degree in Computer and Information Security, authoring a dissertation exploring the impact of NERC CIP regulatory compliance on security and risk. Dr. Tom currently also participates in various NERC/TSA-related efforts and supporting roles, including Education Director for ISSA South Texas, Meeting Logistics Director for the Houston InfraGard Energy Cross-Sector Council, NERC Supply Chain Working Group Vice Chair, Co-Education Lead for Houston ISACA, and Houston ISA Assistant Education Director. Recently, he presented on NERC/TSA compliance at the 2023 Houston API cybersecurity conference.

Justen Dyche

Justen has been a media professional for over 30 years. He has been responsible for delivering Information Security to the BBC for the past eight years. Currently Head of Strategy, he is responsible for creating and maintaining the information security strategy, ensuring alignment with a continually evolving BBC operating model that reflects the corporation's leading role in the modern digital-first media sector.

Justen recently led an ambitious transformation program that fundamentally re-engineered the BBC's InfoSec provision: designing and delivering a clear and comprehensive strategic framework underpinned by tailored tools and processes that capture and exploit a rich data set. The program drove culture change across the department, gaining recognition in the SC Awards 2022. Justen was honored in the C|CISO Hall of Fame in 2023 and holds C|CISO, C|EH, CISSP, CCSP, CGRC, CISM, CRISC, CISA, and ISO27001 Lead Auditor industry certifications.

Brandon Gettert

Brandon is a seasoned cybersecurity expert with 24 years of experience spanning compliance, governance, networking, IT infrastructure, and management. Renowned for his ability to identify and mitigate risks, he specializes in ethical hacking, vendor management, and information security program development. As a gifted communicator and educator, Brandon is a sought-after speaker on cybersecurity topics nationwide.

He is the founder and CEO of Curated Cyber, managing a team of vCISOs, and the founder and President at Lithium Advisors, a cybersecurity board advisory service. Additionally, he teaches at Elite CEU, leveraging his broad experience in financial services, education, the public sector, and software development to offer real-world insights. Brandon is an industry leader, innovator, and educator dedicated to advancing the cybersecurity field.

Jorge L Gomez

Jorge is a cybersecurity professional with over 15 years of practical experience in the energy, financial, cloud infrastructure, and technology industries. He has led and matured numerous cybersecurity programs, including identity & access management, incident response, threat intelligence, security architecture & engineering, application/product security, and cloud security.

More recently, he has become a specialist in the cloud and product security domains by applying a pragmatic approach and focusing on developer-first security practices. He studied at the University of Miami and holds Electrical and Computer Engineering degrees.

Corlette Grobler

Over two decades of IT experience, including experience in executive and management positions in multinational corporations across various industries, including Banking, Financial Services, Retail, Logistics, and Telecommunications. For the past five years, she has been focused intently on Information Security.

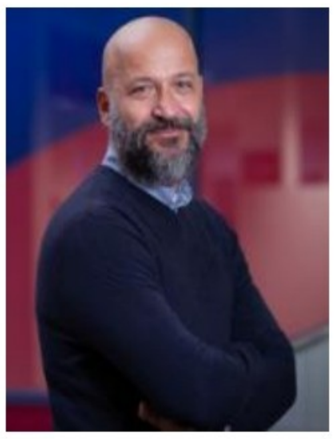
She is pursuing a Master of Science degree in Cybersecurity through the University of Liverpool's correspondence program, intending to acquire advanced specialist skills and knowledge to better mitigate the increasing threat of cyberattacks.

Over the past three years, she successfully designed a comprehensive Cybersecurity Awareness Programme (Bank) to increase cybersecurity awareness among end users through various channels such as email, intranet, posters, and mandatory training courses. The program included social engineering simulations, such as phishing, SMS, and whaling attacks, to boost users' awareness. In addition, she has made significant contributions to the design and development of a DevSecOps maturity analysis tool for a major South African Bank. She has also played a key role in crafting the business and technology architecture for a multinational insurance organization with a strong focus on security. She is currently assisting a major bank with its cloud adoption journey, with a specific emphasis on FinOps and cybersecurity.

Karin Höne

Karin is an enthusiastic IT Security and Risk professional with more than 20 years of experience in the industry in various roles. She currently holds the position of Group Chief Information Security and Risk Officer at a South African multinational. In her role, she challenges herself to craft easy-to-understand IT security and risk strategies linked to the business challenges and objectives of the day. These strategies support executive and board reporting that makes the IT Security and Risk topic accessible and demonstrates the value of the discipline.

Her other area of focus is demystifying IT risk and ensuring risk ownership is understood and placed where it belongs. Karin holds a master's degree in informatics (cum laude) specializing in information security from the Rand Afrikaans University. She holds the certifications of C|CISO, CISSP, and AMBCI. She has received numerous global accolades, such as being inducted into the 2022 – 2023 Certified CISO Hall of Fame and included in various global Top 100 CISO lists in 2022 and 2023.



Federico Iaschi

A seasoned leader in information security and risk management, with a combination of leadership, technical, and managerial experience developed over 20 years within private and public sector enterprises with global and local companies.

He combines multifaceted business insight with excellent interpersonal and leadership skills to build trusting relationships and deliver strong personal and team results. During his career, Federico has achieved extensive professional certifications such as C|CISO, CISSP, CISM, CGEIT, CRISC, CDPSE, ISO27001 LA, and more. He regularly presents at conferences and industry events and assists in writing industry certification material.

Jari Kiero

Jari has worked in information technology for over 25 years, guiding organizations in protecting their most important assets against various threats. He has served in various management positions at well-known IT services, telecommunications, manufacturing, and insurance companies. Currently, he is working on digital operational resilience topics, anticipating and formulating scenarios from risk management and cyber resilience perspectives.

Jari holds a master's degree in industrial engineering and management from the Lappeenranta University of Technology and a second master's in human factors in manufacturing systems from the University of Nottingham. Additionally, he has obtained 15 industry certifications, including C|CISO, CISM, C|EH, CISSP, CCSP, CISA, and ITIL 4 Managing Professional.

Paul Lynch

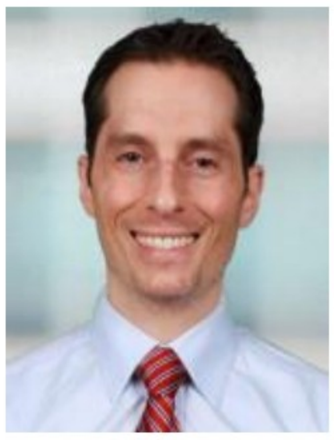
Paul is currently the Senior Director of Information Security and Infrastructure for CubeSmart Self Storage. He has more than 20 years of experience in information technology. He has established security governance programs and best practices for government, non-profit, private, and publicly traded organizations ranging from technology startups to city governments.

He holds several information security certifications, including C|CISO, CISSP, ISSMP, and CCSP. He has served as an exam content subject matter expert for EC-Council and (ISC)2, specializing in security governance and cloud security. He serves on the Customer Advisory Board for both eSentire and Lacework.

Peter Pandula

Peter has over 25 years of industry experience and works at BMO Financial Group. He earned his master's degrees in psychology, Physics, Computer Science, and Business Administration.

He holds industry certifications and credentials in project management, investment management, marketing, risk management, artificial intelligence, information technology (IT) governance, emergency management leadership, payment card cybersecurity, and information security.

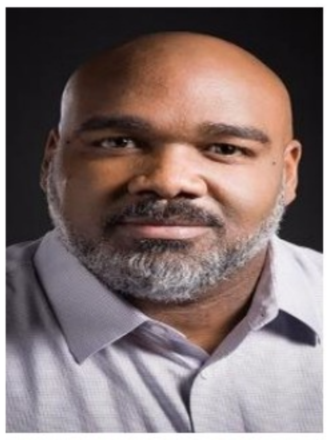


Daniel Pinsky

Daniel is a seasoned cybersecurity leader with over 23 years of experience. He has worked across various industries and sectors in North America and Europe, showcasing his expertise in governance, program development, and implementing and certifying different control frameworks.

Currently, Daniel leads the national cybersecurity program and serves as the CSO for a Fortune 200 company. He earned his degree from McGill University, where he studied business and technology. He has multiple certifications, including C|CISO, CISM, CISA, and CISSP.

Daniel's enthusiasm extends to leadership, effective communication, and personal development. He generously shares his insights and wisdom through various mediums, including writing, public speaking, and mentoring.



Keyaan Williams

Keyaan J Williams has been building and managing cybersecurity and privacy programs to support enterprise risk management for more than two decades. After many years in various departments of the Centers for Disease Control and Prevention (CDC), he started a global consulting firm that supports government, critical infrastructure, and commercial customers. Keyaan actively serves as a board member for commercial and non-profit companies. He also serves as a mentor and advisor for corporate directors and early-stage entrepreneurs.

He regularly shares interesting insights on LinkedIn based on ideas he has published in books and professional journals.

Bjoern Voitel

Bjoern is a privacy and information security professional with over 20 years of experience in several fields, including the financial and critical infrastructure sectors and public and governmental agencies. He is the owner and CEO of three information security companies. He is also a penetration tester and seasoned instructor for EC-Council, ISC², ISACA, Offensive Security, and CompTIA.

He has a diploma in business administration (with a focus on information systems) from the University of Osnabrueck. He holds the C|CISO, CPENT, C|EH Master, CND, CSA, CISM, CRISC, CDPSE, CISA, CGEIT, CISSP-ISSAP, CCSP, CCSLP, SSCP, OSCP and ISO 27001 Lead Auditor industry certifications.

EC-Council

C|CISO
Certified Chief Information Security Officer

Certified Chief Information Security Officer (CCISOv3)

Instructor Presentation

The C|CISO logo is protected by the United State Patent and Trademark Office under registration number 4,175,755.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein or perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use or reliance up this material.

Table of Contents

C|CISO

CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER

WELCOME

GETTING TO KNOW EACH OTHER

INTRODUCTIONS

- Name
- Title
- Company
- What do you hope to get from this course?
- What is your biggest challenge in the field of information security?

C|CISO

CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER

DOMAIN 1

INTRODUCTION

- This domain teaches students how to:
  - Align information security programs with business models.
  - Raise the maturity level of an information security program.
  - Build a personal CISO brand.
  - Improve information security policies.
  - Create hybrid risk management programs.
  - Improve existing risk management practices.

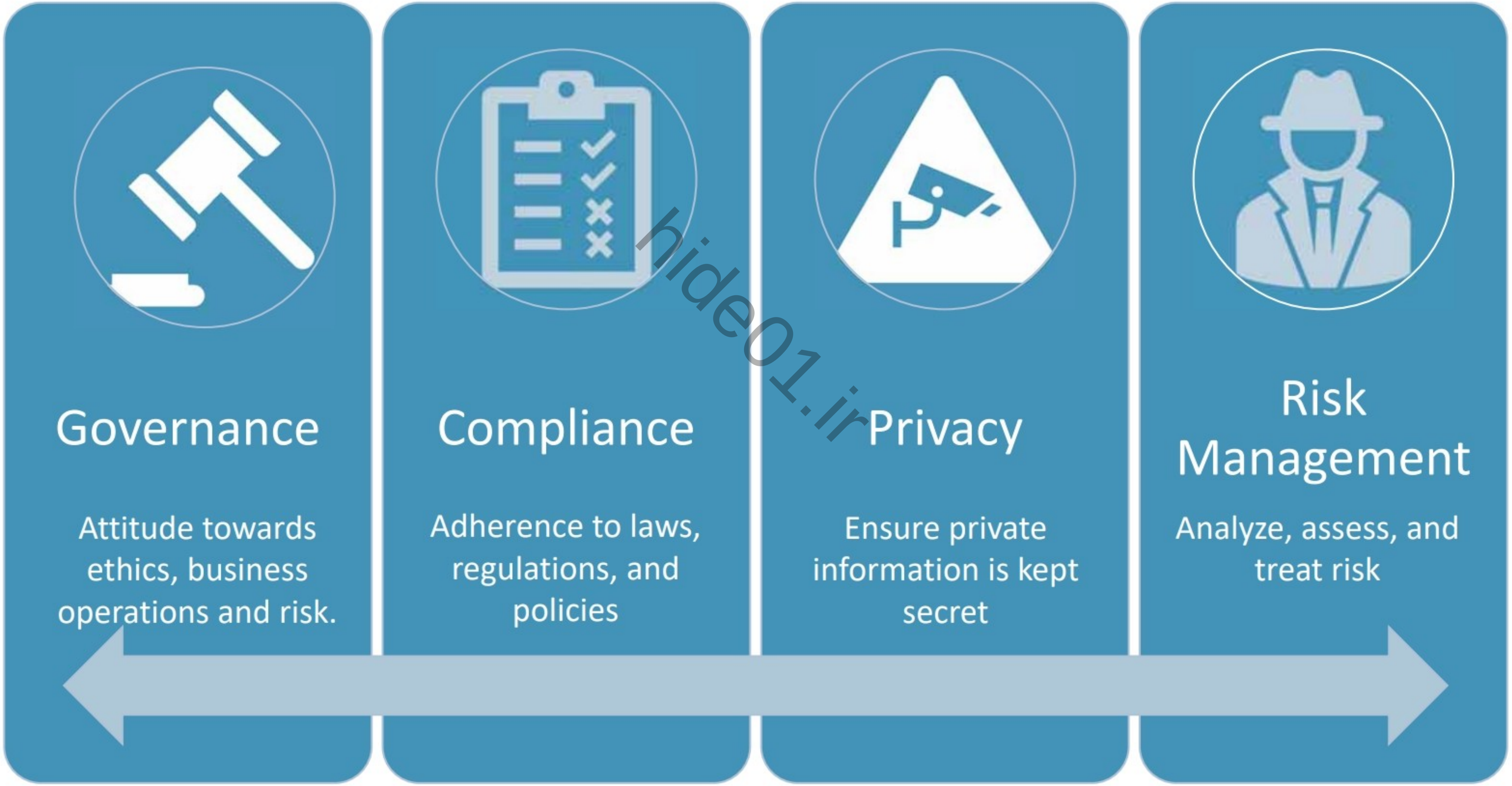
KNOWLEDGE ASSUMPTIONS

- Students are expected to have:
  - Five years of domain experience.
  - An understanding of security Governance, Risk, and Compliance (GRC).
  - Familiarity with GRC vocabulary.
  - The ability to create information security policies.
  - Strong business and personal ethics.
  - A working knowledge of risk management frameworks.
  - An understanding of process maturity models.
  - A working knowledge of risk management.

GOVERNANCE AND RISK MANAGEMENT

DOMAIN 1

DEFINITIONS



Governance

Attitude towards ethics, business operations and risk.

Compliance

Adherence to laws, regulations, and policies

Privacy

Ensure private information is kept secret

Risk Management

Analyze, assess, and treat risk

GOVERNANCE AND RISK MANAGEMENT

DOMAIN OUTLINE

1. Define, Implement, Manage, and Maintain an InfoSec Governance Program

2. Information Security Drivers

3. Establishing an Information Security Management Structure

4. Laws/Regulations/Standards as Drivers of Organizational Policy/Standards/Procedures

5. Managing an Enterprise Information Security Compliance Program

6. Introduction to Risk Management

Summary and Practice Questions

1. DEFINE, IMPLEMENT, MANAGE AND MAINTAIN AN INFORMATION SECURITY GOVERNANCE PROGRAM

DEFINE, IMPLEMENT, MANAGE AND MAINTAIN AN INFORMATION SECURITY GOVERNANCE PROGRAM

- A business driver is a condition, process, requirement, or other concern that influences the way in which an organization directs or manages activities.
- The CISO must understand the purpose of an organization and how it conducts business when creating or modifying existing information security governance.

FORM OF BUSINESS ORGANIZATION

- The form of business organization, its hierarchical structure, the industry in which it operates, and its maturity influence an organization's governance processes.

Three most common structures used to organize a business:

Proprietorship

Partnership

Corporation

FORM OF BUSINESS ORGANIZATION: PROPRIETORSHIP

Proprietorship

- A proprietorship is the simplest form of ownership. It exists when a single individual owns the organization.
- The proprietor defines the mission, vision, and purpose of the organization.
- This person typically makes most, if not all, decisions for the organization.

FORM OF BUSINESS ORGANIZATION: PARTNERSHIP

Partnership

- A partnership is an organization in which two or more individuals share the profits and responsibility for liabilities of the organization.
- Partnerships allow owners to pool their knowledge and experience.
- As additional partners are added, governance becomes more complex.
- Larger partnerships have layered executive levels.
  - Partner, senior partner, managing partner, etc.

FORM OF BUSINESS ORGANIZATION: CORPORATION

Corporation

- Corporations are business entities that are legally separated from the owners.
- Governance is directed because owners (typically investors) and their representatives (Board of Directors) make the major decisions of the organization according to articles of incorporation.
- Shareholder value is the primary force driving governance for corporations.

INDUSTRY

- The industry in which an organization operates influences corporate governance.
- Highly regulated industries create more complex and thorough governance structures.
- Industries have unique norms, requirements, and regulations that drive governance decisions.

Largest Global Industries

E-Commerce

Construction

Financial Services

Real Estate

Life and Health insurance

Information Technology

Food Industry

Oil and Gas (E&P)

Automobile Manufacturing

Telecommunications

INDUSTRY: CYBER ATTACKS

Top Targeted Industries

Retail
11%

Transportation
13%

Professional Service
12%

Finance & Insurance
19%

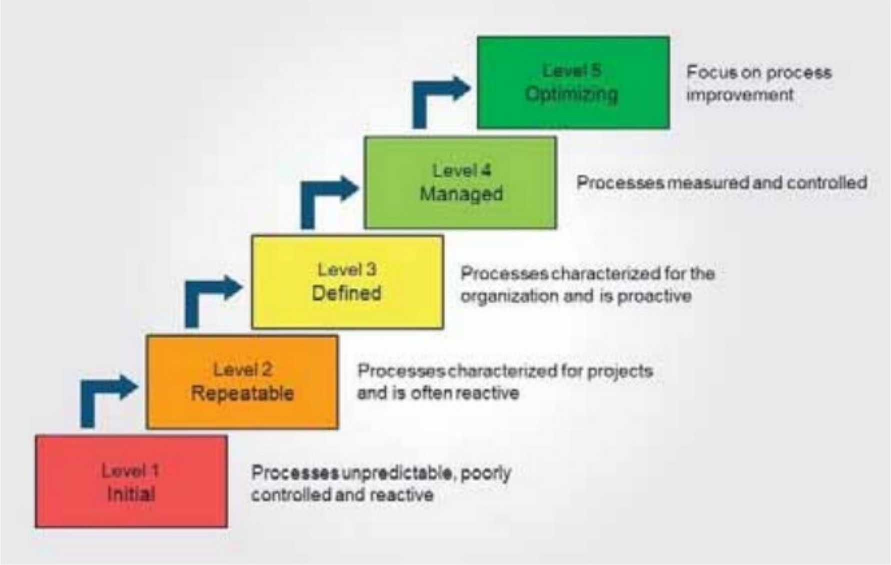
Manufacturing
10%

65%

Source: Bulletproof Annual Cyber Security Report 2020

ORGANIZATIONAL MATURITY

- Maturity can be influenced by a wide range of factors such as the size of an organization, the structure, leadership, industry, and many others.
- An organization's maturity can typically be mapped to models such as the Capability Maturity Model Integration (CMMI).



Level 5 Optimizing — Focus on process improvement

Level 4 Managed — Processes measured and controlled

Level 3 Defined — Processes characterized for the organization and is proactive

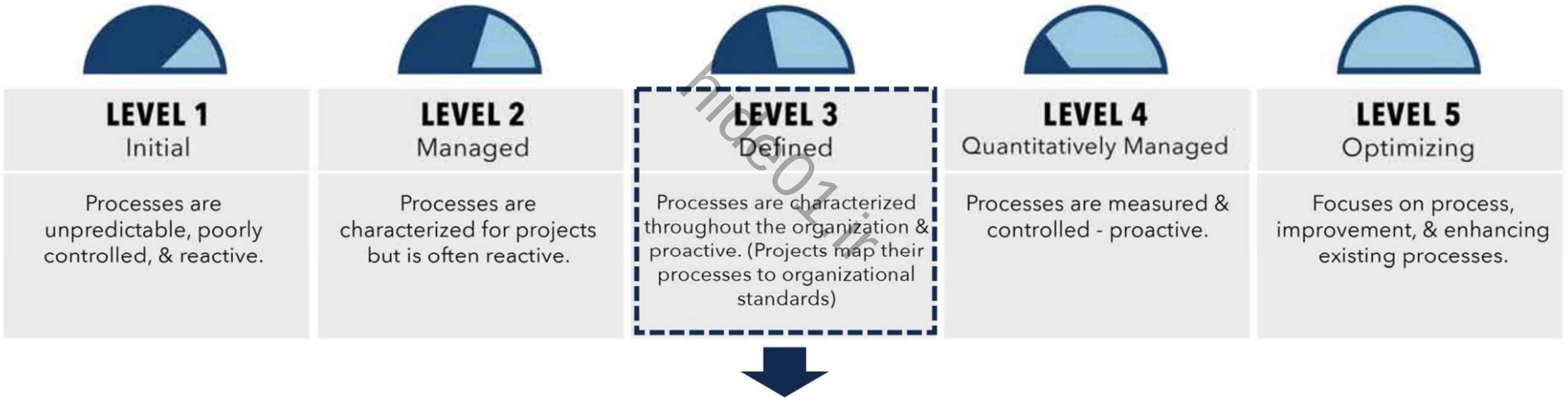
Level 2 Repeatable — Processes characterized for projects and is often reactive

Level 1 Initial — Processes unpredictable, poorly controlled and reactive

- Maturity models are useful to define the current state of maturity and describe what an organization should do to facilitate improved performance and maturity.

ORGANIZATIONAL MATURITY: SCALE

Capability Maturity Model Integration (CMMI)



LEVEL 1 Initial	LEVEL 2 Managed	LEVEL 3 Defined	LEVEL 4 Quantitatively Managed	LEVEL 5 Optimizing
Processes are unpredictable, poorly controlled, & reactive.	Processes are characterized for projects but is often reactive.	Processes are characterized throughout the organization & proactive. (Projects map their processes to organizational standards)	Processes are measured & controlled - proactive.	Focuses on process, improvement, & enhancing existing processes.

Typically, organizations cannot begin to realize the benefits of mapping processes to organizational standards to achieve consistency across the enterprise until CMMI Level 3.

ORGANIZATIONAL MATURITY: STATE

Reactive versus Proactive Organizations

Reactive	Attribute	Proactive
Making money and short-term shareholder returns	Focus	Long-term returns and strategic thinking
Reacting to immediate problems	Priorities	Taking a preemptive approach
Control is centralized	Control	Control is localized
Reliance on instinct or experience people	Analysis	Focus on data to improve processes
People counted as a cost	Personnel	People valued as an asset
Training is a benefit or perk	Training	Training is essential to success
Distrust between management and employees	Leadership	Leaders and personnel collaborate and work together

2. INFORMATION SECURITY DRIVERS

How does information security influence the direction and management of activities in an organization?

INFORMATION SECURITY DRIVERS

- Business drivers affect the decisions made in an organization. Information security drivers are similar because of their effect on the management and operation of the organization.
- Alignment with business compliance and privacy needs are among the most important information security drivers.

INFORMATION SECURITY DRIVERS: ALIGNMENT

- Security executives achieve harmony and alignment between the business and security by mapping information security governance to the broader organization's governance model.

- This alignment to the organization is one of the most important success factors for effective information security governance.

INFORMATION SECURITY DRIVERS: FACTORS

- The CISO must thoroughly understand the organization in order to successfully align to it.
- A wide variety of factors influence the organization, to include:
  - Organizational objectives.
  - Policies, procedures and processes supporting those objectives.
  - Information and technology supporting business operations.
  - Threats that could disrupt operations.

INFORMATION SECURITY DRIVERS: ORG VARIABLES

Industry

Complexity

Company Size

Technology

Regulations

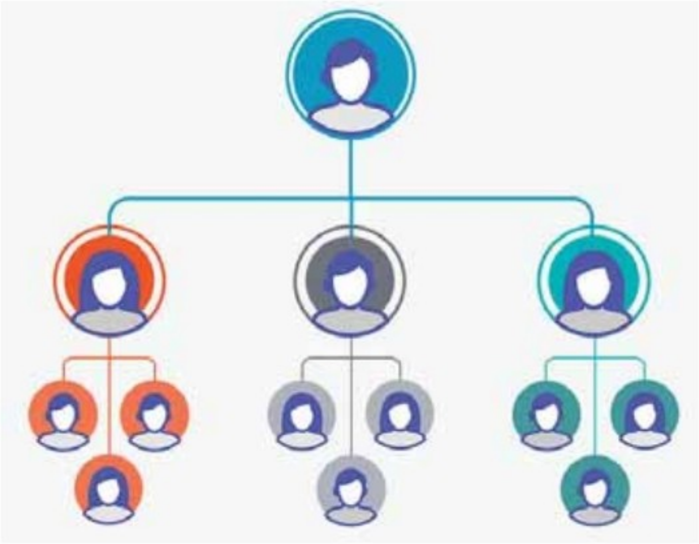
Can you name other drivers?

1. ____________________________
2. ____________________________
3. ____________________________
4. ____________________________

3. INFORMATION SECURITY MANAGEMENT STRUCTURE

INFORMATION SECURITY MANAGEMENT STRUCTURE

- The hierarchical structure of an organization usually relates to the form of business organization.
- Example: the owner of a proprietorship often acts as the CEO and the organizational chart expands from this central figure.
- The larger the organization the more complex the reporting structure.

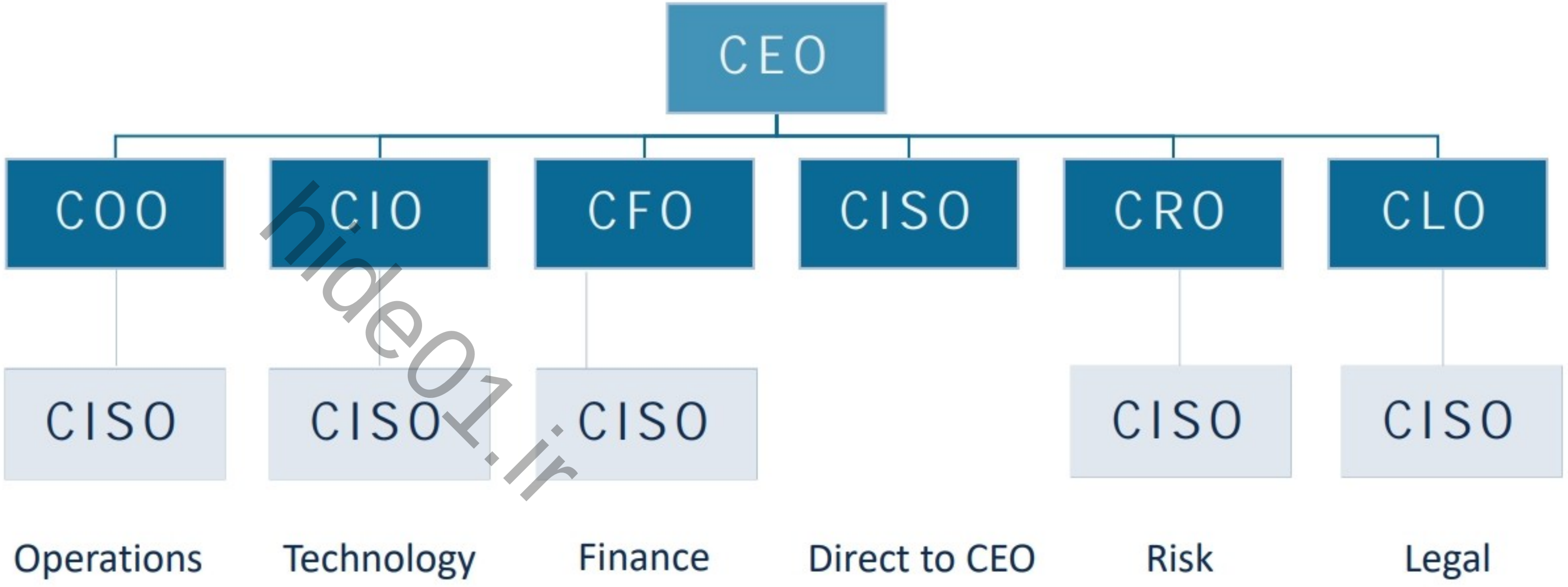


WHERE DOES THE CISO FIT WITHIN THE ORGANIZATIONAL STRUCTURE?

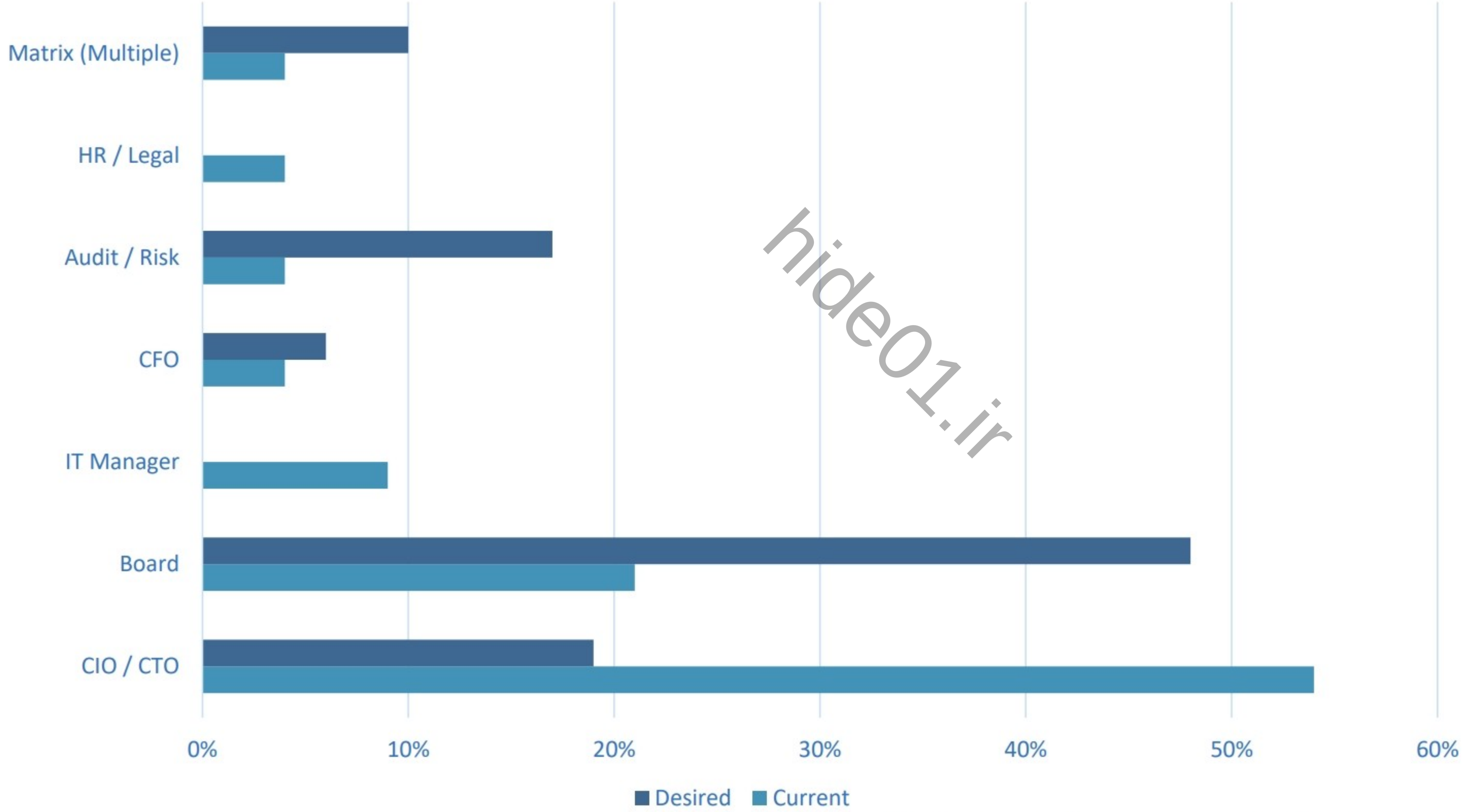
- To whom should the CISO report?
- The majority of CISOs report indirectly to the CIO.
- While this is the most common reporting structure, arguments can be made that this may not be the most effective placement of the CISO.
- Placement of the security function is often at the discretion of the highest levels of leadership, such as CEO/EVP, Board of Directors, or business owner.

WHERE DOES THE CISO FIT WITHIN THE ORGANIZATIONAL STRUCTURE?

There is no standard that establishes the optimal placement of a CISO within an organizational hierarchy.



WHERE DOES THE CISO FIT WITHIN THE ORGANIZATIONAL STRUCTURE?



Source: ClubCISO – 2019 Information Security Maturity Report

THE EXECUTIVE CISO

The Executive CISO

- CISOs provide leadership as corporate executives and are influential because they have the advantage of executive positioning within the organization.

C-LEVEL ATTITUDES TOWARD THE CISO

C-Level Attitudes toward the CISO

CISO Grade	
A - Excellent	23%
B – Above Average	42%
C - Average	30%

- A ThreatTrack survey of 200+ US-based C-level executives by the data security firm ThreatTrack found:
  - 61% - CISOs would not be successful outside of information security.
  - 44% - CISOs should be accountable for data breaches.
  - 46% - CISOs should be responsible for cybersecurity purchases.

Source: ThreatTrack - https://media.scmagazine.com/documents/89/threattrack_study_on_cisos_22034.pdf

NONEXECUTIVE CISO

The nonexecutive CISO

Office of the CISO

- It is not uncommon to place the CISO in a nonexecutive leadership role.
- These individuals typically focus only on information security technology or limited risk management objectives rather than influencing broader business operations.

4. LAWS/REGULATIONS/ STANDARDS AS DRIVERS OF ORGANIZATION POLICY/STANDARDS/ PROCEDURES

LAWS/REGULATIONS/STANDARDS AS DRIVERS OF ORGANIZATION POLICY/STANDARDS/PROCEDURES

- Many activities or actions of a CISO directly relate to laws, regulations, and corporate standards.
- These guiding articles result in the development of an organization's information security policies, standards and procedures.
- Domain 2 will provide more details about the most common laws, regulations and standards a CISO could encounter.

LAWS/REGULATIONS/STANDARDS AS DRIVERS OF ORGANIZATION POLICY/STANDARDS/PROCEDURES

Terms and Definitions

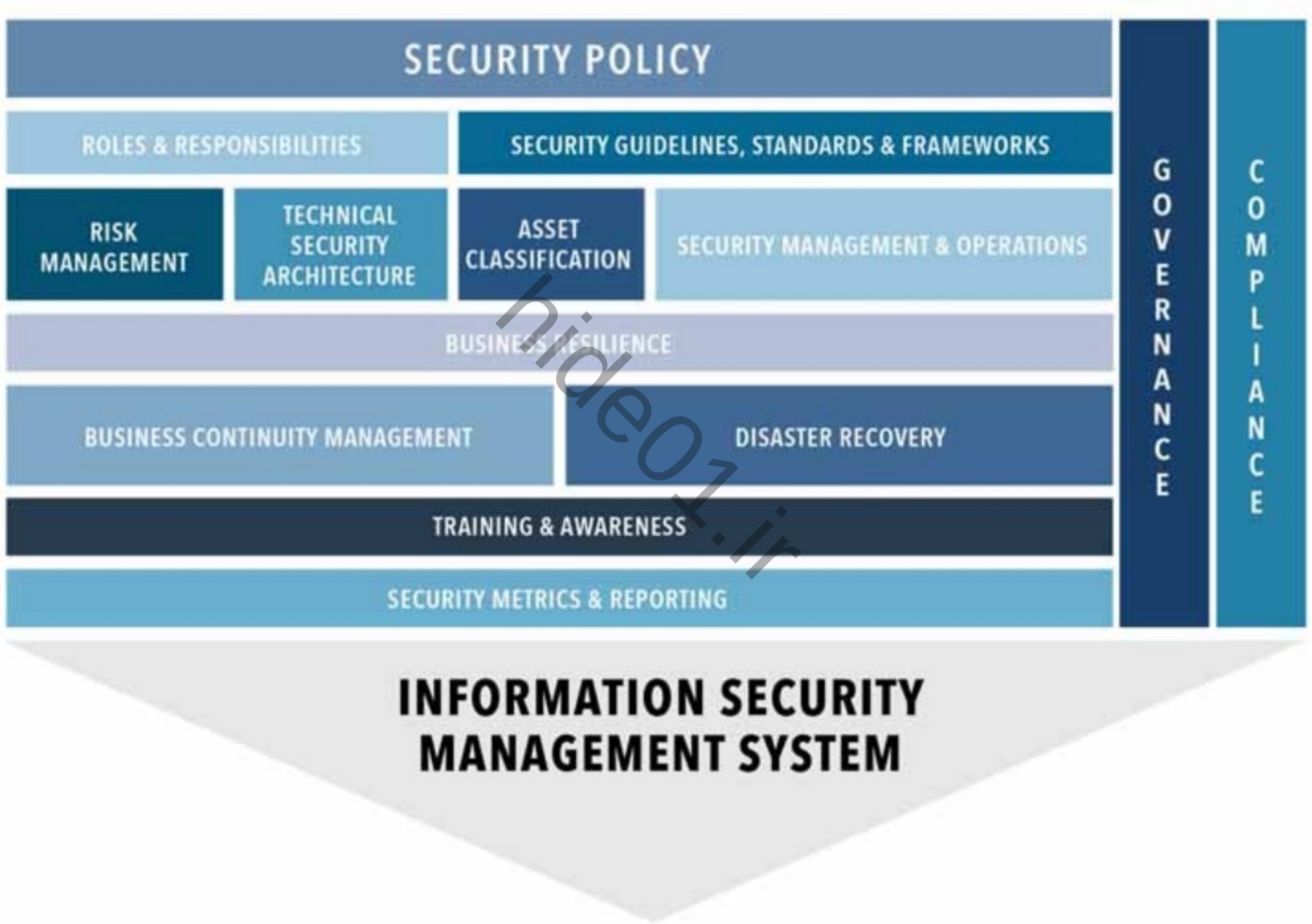
- **Regulations** – written laws of industry standards passed by legislative body or central authority.
- **Policies** - a course or principle of action adopted or proposed by a government, party, business, or individual.
- **Standards** - something used as a measure, norm, or model in comparative evaluations.
- **Procedures** – a series of actions conducted in a certain order or manner.

5. MANAGING AN ENTERPRISE INFORMATION SECURITY COMPLIANCE PROGRAM

MANAGING AN ENTERPRISE INFORMATION SECURITY COMPLIANCE PROGRAM

- The information security program is the practical mechanism for adhering to security and privacy compliance with internal organizational requirements, laws, and regulations.
- Frameworks are used as industry-proven foundational guides for implementing a security program or various parts of it.
- These various parts of a security program are often referred to as the security portfolio.

INFORMATION SECURITY POLICIES: FRAMEWORK



SECURITY POLICY
ROLES & RESPONSIBILITIES
SECURITY GUIDELINES, STANDARDS & FRAMEWORKS
RISK MANAGEMENT
TECHNICAL SECURITY ARCHITECTURE
ASSET CLASSIFICATION
SECURITY MANAGEMENT & OPERATIONS
BUSINESS RESILIENCE
BUSINESS CONTINUITY MANAGEMENT
DISASTER RECOVERY
TRAINING & AWARENESS
SECURITY METRICS & REPORTING
GOVERNANCE
COMPLIANCE
INFORMATION SECURITY MANAGEMENT SYSTEM

Table - Information Security Management System/Framework

SECURITY POLICY

The security policy provides an executive statement of how your company will implement information security principles and technologies.

A security policy should include the following information:

- Stakeholders of the information security of the organization.
- Who is responsible for adhering to the policy.
- The confidentiality and privacy of information.
- The principle of least access to information.
- The integrity of information.
- The availability of information.
- The balance of risk exposure with the cost of risk mitigation.
- The implementation of security measures.
- The classification of information.
- The importance of security awareness and information governance.

NECESSITY OF A SECURITY POLICY

- A security policy can provide legal protection to an organization by demonstrating an organization's commitment to adhere to legal and regulatory requirements.
- This is often legally referred to as showing *due care and diligence*.
- Policies often fulfill regulatory requirements or adhere to industry standards that specify security for digital information. The more common ones include:
  - The Payment Card Industry (PCI) Data Security Standard (DSS).
  - The Health Insurance Portability and Accountability Act (HIPAA).
  - The Health Information Technology for Economic and Clinical Health (HITECH) Act.
  - The Sarbanes-Oxley Act (SOX).
  - The ISO family of security standards.
  - The Graham–Leach–Bliley Act (GLBA).
  - EU General Data Protection Regulation (GDPR).

SECURITY POLICY CHALLENGES

- The process of writing a security policy can be difficult, time consuming, and expensive.
- To be effective, a security policy should be clearly and simply written.
- It should be consistent in format and content with other organizational policies.
- A security policy must be easily understood by the target audience.
- Poorly written policies can detract from your efforts in several ways:
  - Induce misunderstanding or confusion within the target audience which can result in non-compliance.
  - Reflects poorly on the professionalism of the security function. Remember that all public documentation will influence the perception of you and your security team.

POLICY CONTENT

The Big Pieces of a Policy

- **Overview**: Provides background information what the policy defines.
- **Purpose**: Specifies why the policy is needed.
- **Scope**: Explains the boundaries of what must be done.
- **Target audience**: Describes who is responsible for acting on the policy.
- **Policies**: This is the main section of the document and provides statements as to what must be done.
- **Definitions**: Provides clarity of the terms used within the policy.
- **Version**: Provides consistent history of the policy to reflect changes and updates.

POLICY CONTENT

- There are many general guidelines, practices, samples, and even advice on how to create successful information security policies.
- Generally, a security policy should be:
  - No longer than necessary.
  - Written in common language.
  - Consistent with applicable laws and regulations.
  - Reasonable.
  - Enforceable.
- A major mistake when writing policies: trying to sound really, really, smart.
  - Successful policies are simple, direct, and readily understood.
  - Keep them professional and easy to read – again, it will reflect well on the security function.

TYPES OF POLICIES

- Organizations have different needs and focus.
- Policies need to align to the organization to be effective within the specific environment.
- There are numerous 'standard' policy lists available out on the Web.
- Some companies may need many security policies, while some only need a few.
- Selecting policies is typically based on several factors:
  - The industry – is it highly regulated?
  - Organizational maturity.
  - Internal controls complexity across the business.
  - The risk appetite of the organization
  - ...and many other characteristics of the organization.

TYPES OF POLICIES

Certain policies can be considered essential to security management.

- Acceptable Use
- Authentication
- Asset Management
- Backup
- Business Continuity/Disaster Recovery
- Confidential Data
- Data Classification
- Encryption
- Incident Response
- Mobile Device
- Network Access
- Network Security
- Outsourcing
- Password
- Physical Security
- Remote Access
- Retention
- Third Party Management
- VPN
- Wireless Use
- Email
- Guest Access

POLICY IMPLEMENTATION

- Once the security policy has been created, perhaps the hardest part of the process is deploying it within an organization.
- There are many things to consider when creating policy, such as:
  - Are there formal processes for policy approval?
  - Are there barriers to adopting a policy?
  - Is the policy reasonable given the culture of the organization?
  - Can the requirements within the policy be supported given available resources?
- A security policy must be supported by the organization's senior management team.
  - Without support, the implementation will likely fail.

SECURITY ROLES AND RESPONSIBILITIES

- Traditionally the role of the CISO has been to design and monitor enterprise security controls to support the security program's objectives:
  - Enable risk management in the IT environment.
  - Establish and implement effective security policies, standards, processes and guidelines.
  - Establish effective security standards and controls.
  - Respond to information systems incidents.

STANDARDS AND BEST PRACTICES

- There are a variety of standards and leading practices – each organization has unique challenges and focus.
- For instance, a healthcare company might focus on maintaining patient privacy.
  - That same approach will not work for a social network company focused on sharing personal information between customers.
- If you are the first CISO at an organization you will probably establish standards, frameworks, and best practices for your company.

LEADERSHIP AND ETHICS

- **Leadership:**
  - An intangible quality that is very difficult to define, but easily recognized when a strong leader is present.
  - There is a significant difference between a manager and a leader.
    - A manager maintains requirements, a leader enables performance
- **Ethics:**
  - Defines the moral principles governing the behavior of a person or group.
  - The behavior of the CISO is highly visible and influences the behavior of other people throughout the organization.
  - Ethical behavior by the CISO is crucial for security adoption within the organization.

LEADERSHIP AND ETHICS: FRAMEWORK

The following framework for making ethical decisions consists of seven questions that, in answering, will serve as an aid to identify what is right.

When evaluating a decision, ask the following:

1. What decision alternatives are available?
2. What individuals or organizations have a stake in the outcome of my decision?
3. Will an individual or an organization be harmed by any of the alternatives?
4. Which alternative will do the best with the least harm?
5. Would someone I respect find any of the alternatives objectionable?

After deciding on a course of action, but before acting, ask the following:

6. Am I comfortable with the decision I've made?
7. Will I be comfortable telling my friends and family about this decision?

EC-COUNCIL CODE OF ETHICS

- EC-Council provides the expectations for ethical behavior by certification holders within the EC-Council Code of Ethics.
- This code reflects the values and behavior expected of all professionals within the security industry.
- This code also expresses the consensus of the profession on ethical issues.
- The code is a means to educate everyone - both the public and those entering the security profession - regarding the ethical obligations of security professionals.

EC-COUNCIL CODE OF ETHICS

1. Keep information within your professional work private and confidential.
2. Protect intellectual property within your span of control.
3. Disclose attacks and criminal activities to the appropriate persons or authorities.
4. Provide the best service possible within your abilities as a security professional.
5. Never knowingly use illegally or unethically obtained software or products.
6. Do not engage in deceptive financial practices.
7. Use the property of organizations as intended and authorized.
8. Disclose potential conflicts of interest to all concerned parties when discovered.
9. Provide good management and risk controls for projects you lead to deliver the highest quality product possible.

9. Add to the knowledge of the profession through personal knowledge improvement and sharing within the cybersecurity community.

10. Conduct yourself in the most ethical and competent manner by never compromising your integrity.

11. Do not associate with malicious entities nor engage in malicious activities.

12. Do not purposefully or intentionally expose or compromise an organization's systems or data.

13. Ensure all systems scanning and penetration testing activities are authorized and performed within the applicable laws and statutes.

14. Do not make inappropriate reference to the CCISO (or any) certification, and never use your certification in a misleading manner or cause adverse perceptions to the CCISO community.

6. INTRODUCTION TO RISK MANAGEMENT

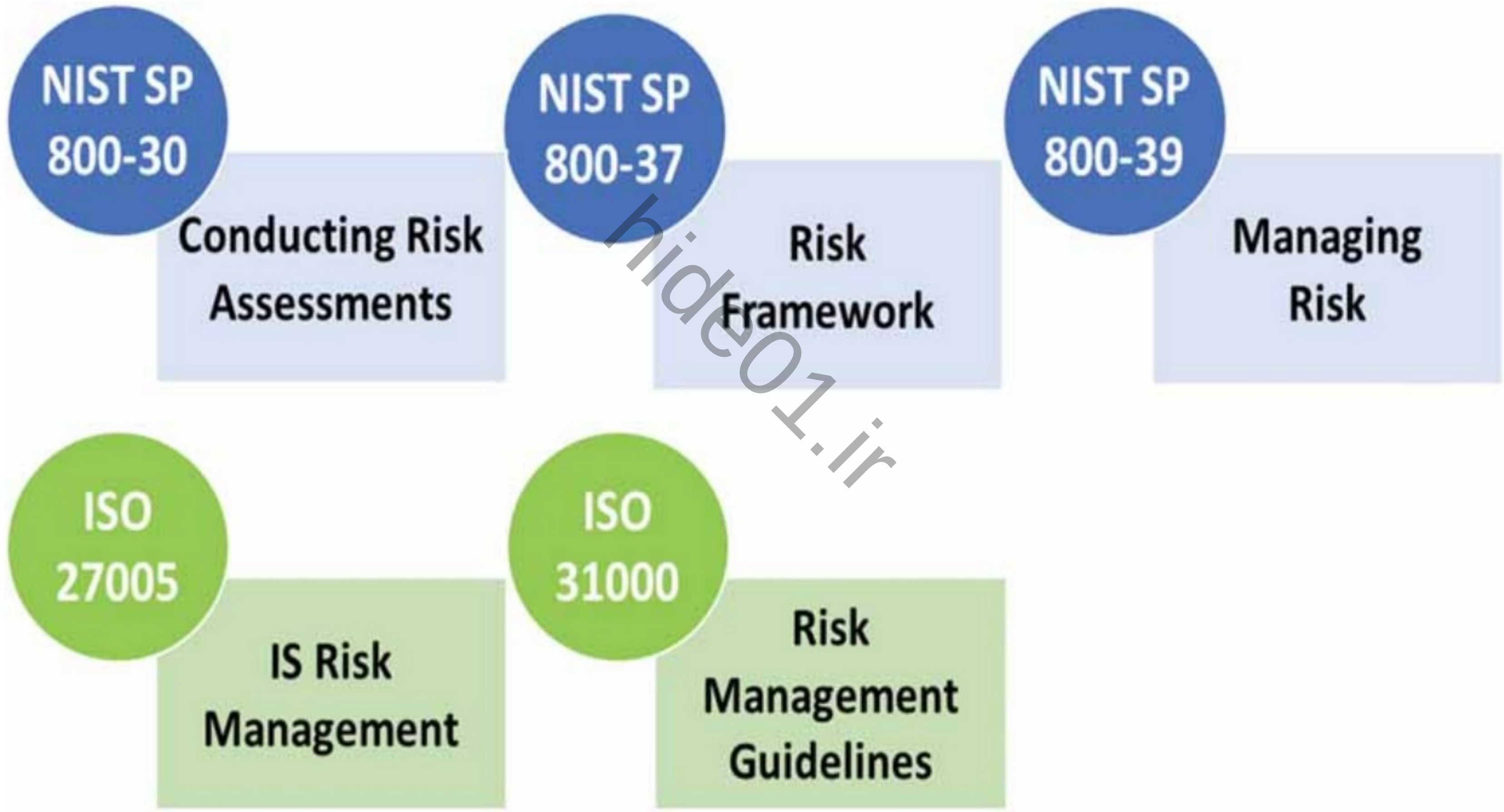
INTRODUCTION RISK MANAGEMENT

Risk management is the identification, assessment, and prioritization of risks followed by a coordinated and economical application of resources to minimize, monitor, and control the probability and impact of adverse events.

There are two approaches to risk management:

- **Risk appetite** – level of risk an organization is willing to accept in pursuit of its objectives.
  - Generally defined as a subjective perspective.
- **Risk tolerance** – degree of loss an organization is willing to withstand.
  - Generally defined by objective boundaries.

RISK MANAGEMENT: STANDARDS



NIST SP 800-30 Conducting Risk Assessments

NIST SP 800-37 Risk Framework

NIST SP 800-39 Managing Risk

ISO 27005 IS Risk Management

ISO 31000 Risk Management Guidelines

RISK MANAGEMENT: STANDARDS

NIST

- NIST SP 800-30 Rev. 1 | Guide for Conducting Risk Assessments
- NIST SP 800-37 Rev. 2 | Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39 | Managing Information Security Risk: Organization, Mission, and Information System View

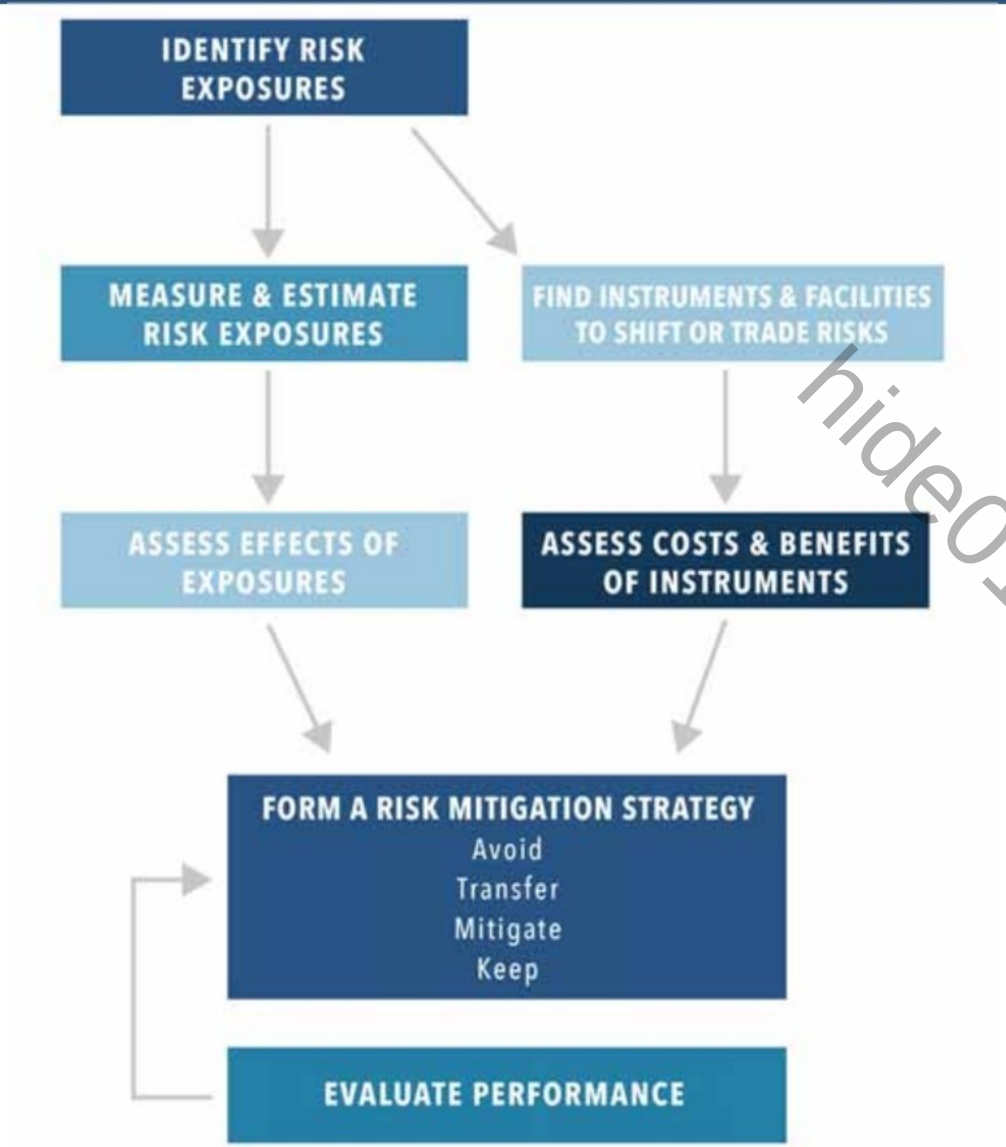
ISO

- ISO/IEC 27005:2018 | Information technology -- Security techniques -- Information security risk management
- ISO/IEC 31000:2018 | Risk management – Guidelines, provides principles, framework and a process for managing risk

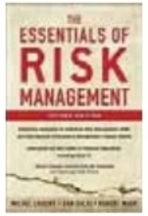
RISK MANAGEMENT: ESSENTIALS

Program Essentials Checklist	
1. Understand the context of risk evaluation.	✓
2. Create a risk management policy.	✓
3. Instill common organizational risk terms - risk appetite, risk tolerance, etc.	✓
4. Obtain executive buy-in on risk policy and terms.	✓
5. Inventory and know the assets requiring protection.	✓
6. Assign risk to asset/data owners.	✓
7. Understand the threats most likely to affect the organization.	✓
8. Understand the vulnerabilities within the enterprise.	✓
9. Adopt an accepted risk management framework and/or standard.	✓
10. Create a standardized risk assessment form to evaluate risks to the organization.	✓
11. Create a risk register to track risk scores, risk treatment and residual risk.	✓
12. Perform risk compliance monitoring, including third parties.	✓
13. Communicate risk treatment and risk management to organization.	✓
14. Continuously monitor organization and assets for emerging risks.	✓

RISK MANAGEMENT: ESSENTIALS

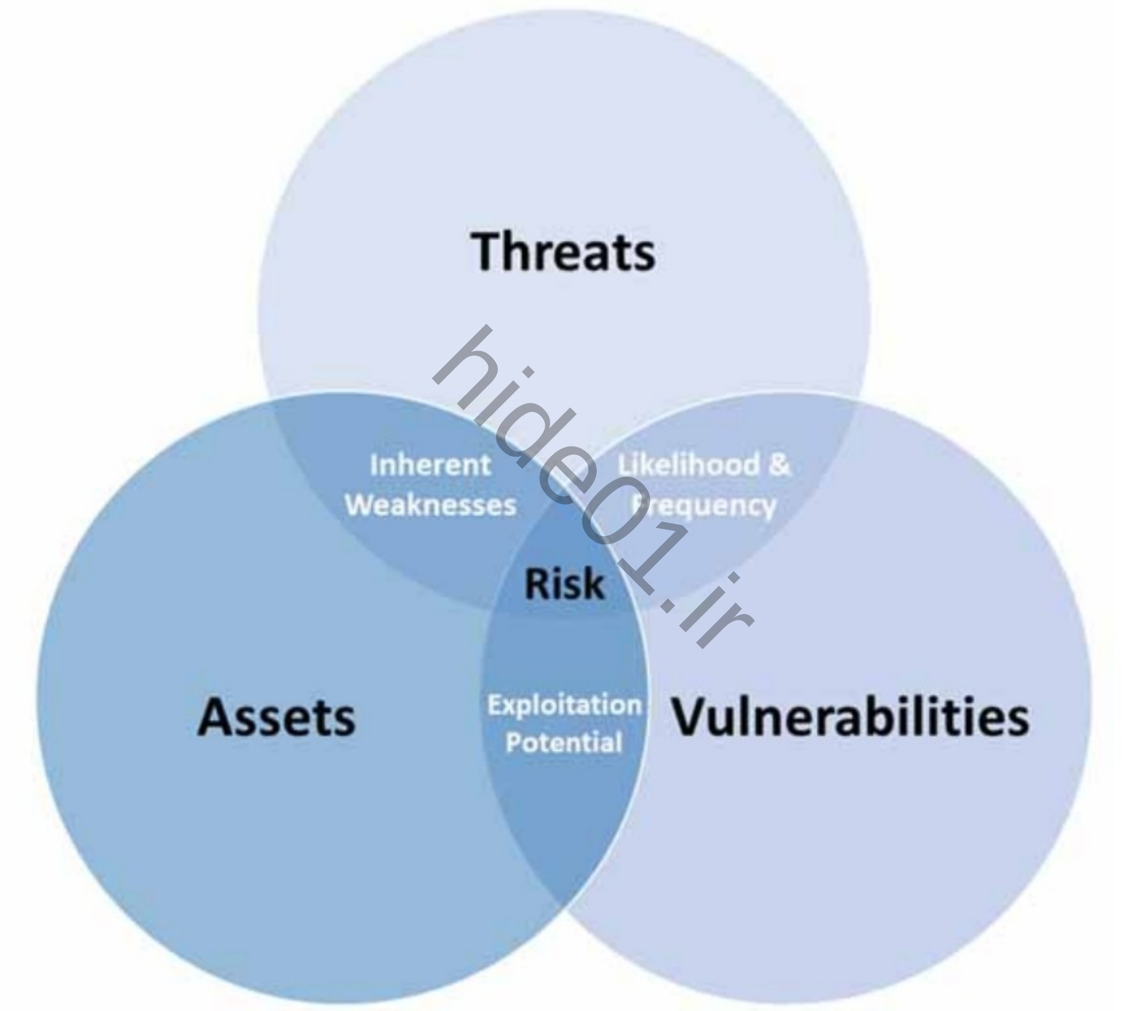

IDENTIFY RISK EXPOSURES
MEASURE & ESTIMATE RISK EXPOSURES
FIND INSTRUMENTS & FACILITIES TO SHIFT OR TRADE RISKS
ASSESS EFFECTS OF EXPOSURES
ASSESS COSTS & BENEFITS OF INSTRUMENTS
FORM A RISK MITIGATION STRATEGY
Avoid
Transfer
Mitigate
Keep
EVALUATE PERFORMANCE

Managing risks requires the identification, analysis and control of the exposure to risk.



One Source: "The Essentials of Risk Management"

WHERE RISK RESIDES



Risk Confluence Diagram

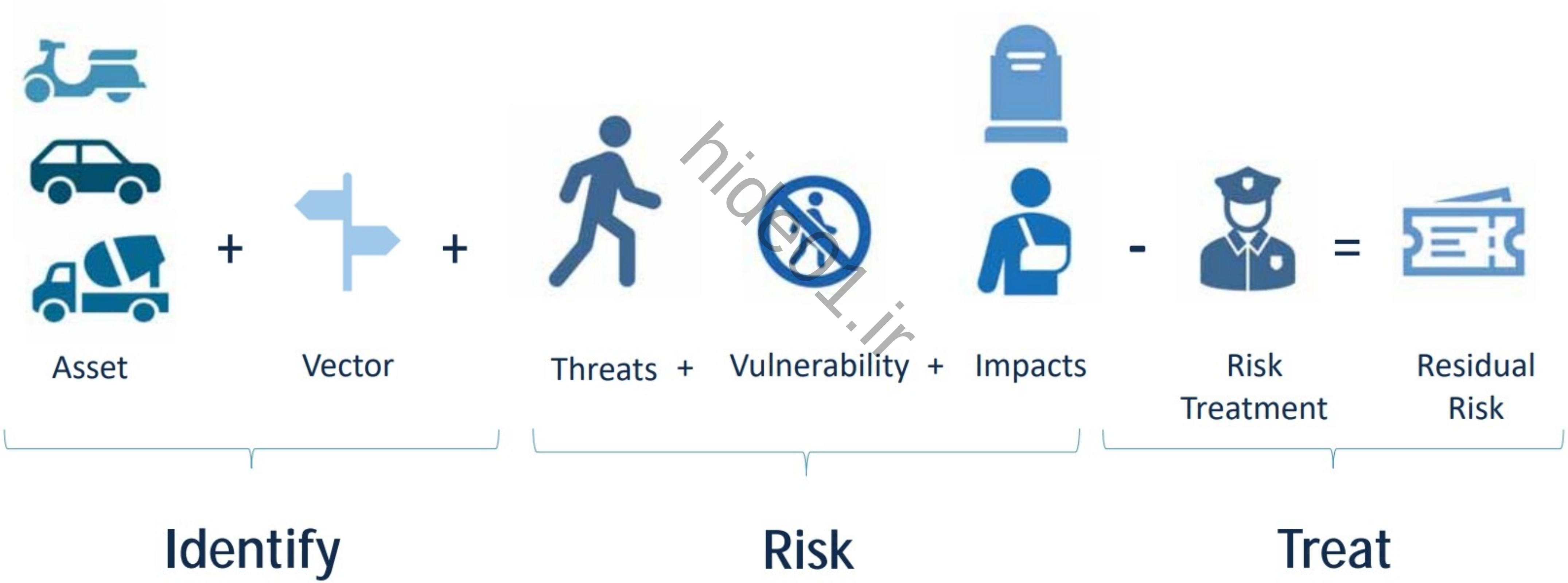
RISK OWNERSHIP

- Risk is owned by asset owners.
  - Systems, data, clusters.
- Assigning ownership can be political.
- CISOs do not generally own risk.
  - Only within their sphere of ownership (the security program).
- CISOs don't have the authority nor responsibility for determining which risks will be treated and which risks will be accepted.
  - Risk must be communicated to those individuals that have the ultimate responsibility for systems and data.
  - They ultimately determine the treatment.
  - The CISO's job is to advise and assist.

RISK ASSESSMENT TYPES

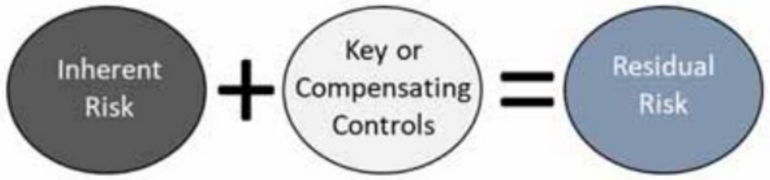
QUANTITATIVE		QUALITATIVE
Objective	PERSPECTIVE	Subjective
Time consuming	DIFFICULTY LEVEL	Quick
Numerical	RESULTS	Ranges/categories
Required	THREAT FREQUENCY CALCULATION	Optional
Recommend a tool	AUTOMATION	Spreadsheet or tool
Substantial data & research	PRE-WORK	Context and scope
Asset value must be known	ASSET	Asset estimates are used

RISK ASSESSMENT PROCESS



RISK MANAGEMENT: CATEGORIES

Two primary categories of risk:



- Inherent Risk

  Inherent risk defines the risk that exists before controls are implemented. The organization must understand the potential impact of a realized risk before controls are implemented. This helps determine the value and effectiveness of a mitigation strategy.

- Residual Risk

  Some quantity of risk always remains after controls are applied, resulting in residual risk. Risk mitigation exists to reduce risk to an acceptable level. Risk acceptance is a common outcome of reducing risk to the lowest acceptable residual level.

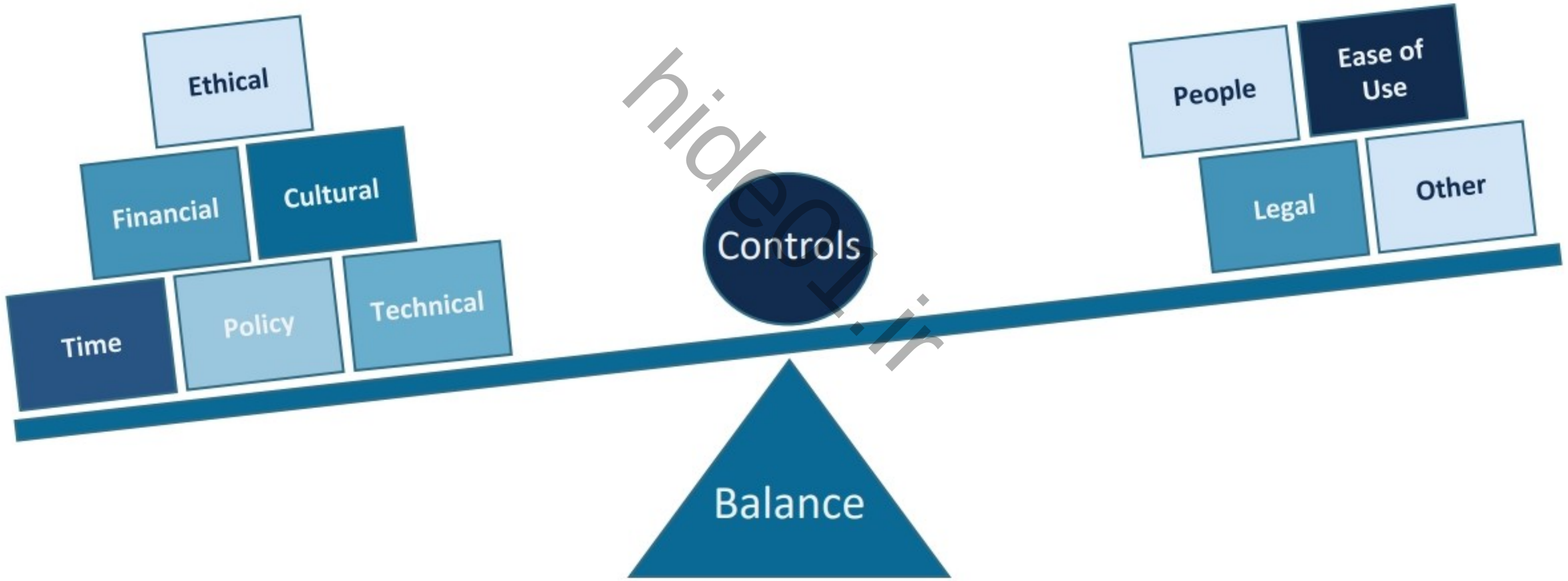
RISK TREATMENT

- Risk treatment is the process of deciding what to do with a risk.
- Risk treatment is how you specifically manage/address risk through an action.
- CISOs support the risk treatment decision-making process by accurately identifying risks and recommending treatment options.
- The CISO may offer support for risk treatment, but **the final decision of risk treatment belongs to the business or asset owner**.
- Risk treatment is a usually determined by balancing criticality and resource constraints.

RISK MODIFICATION

- Applying additional controls to offset or reduce risk.
- Risk identification, ratings and reporting - tradecraft of CISO.
  - Part art, part science.
- There is typically a strong connection between risk management, security operations, and IT operations.
- Multiple controls can be used to manage a risk.

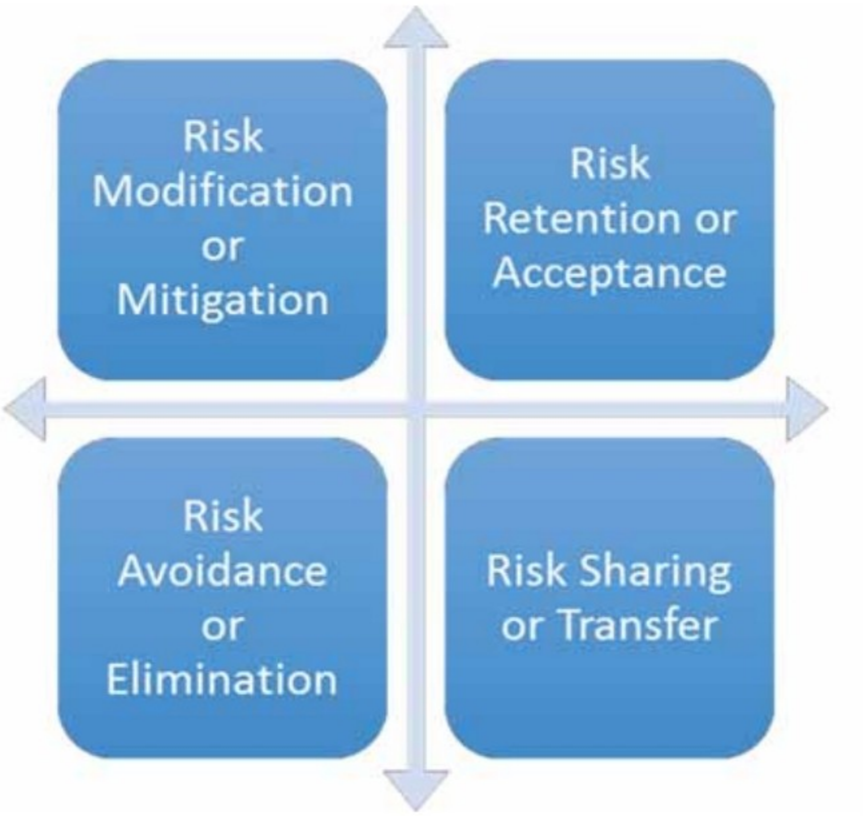
RISK MODIFICATION: CONSTRAINTS



RISK TREATMENT OPTIONS

- Organizations have four options for risk treatment.

Risk Treatment Options


Risk Modification or Mitigation
Risk Retention or Acceptance
Risk Avoidance or Elimination
Risk Sharing or Transfer

RISK TREATMENT: OPTIONS

- **Risk modification or mitigation** is the most common risk treatment option. An organization seeks to change risk exposures or outcomes by applying security controls to a process, system, or environment.

- **Risk retention or acceptance** occurs when an organization acknowledges the existence of a risk and deliberately chooses to not apply controls or management the risk.

- **Risk avoidance or elimination** is the treatment option that occurs when an organization makes changes or avoids an activity by removing the asset to eliminate the risk.

- **Risk sharing or transfer** occurs when assigning accountability for a risk to another entity or organization.

APPLYING COMPENSATING CONTROLS TO REDUCE RISK

- Compensating controls are alternative solutions used instead of applying controls that directly resolve the risk issue.
- This is the next step when key controls cannot be applied due to constraints such as budget, time, technical barriers, business needs, etc.
- Typically requires a clear communication of why alternate solutions have been used.
- Must meet the rigor and intent of key controls.
- In aggregate, compensating controls must provide similar levels of risk reduction.

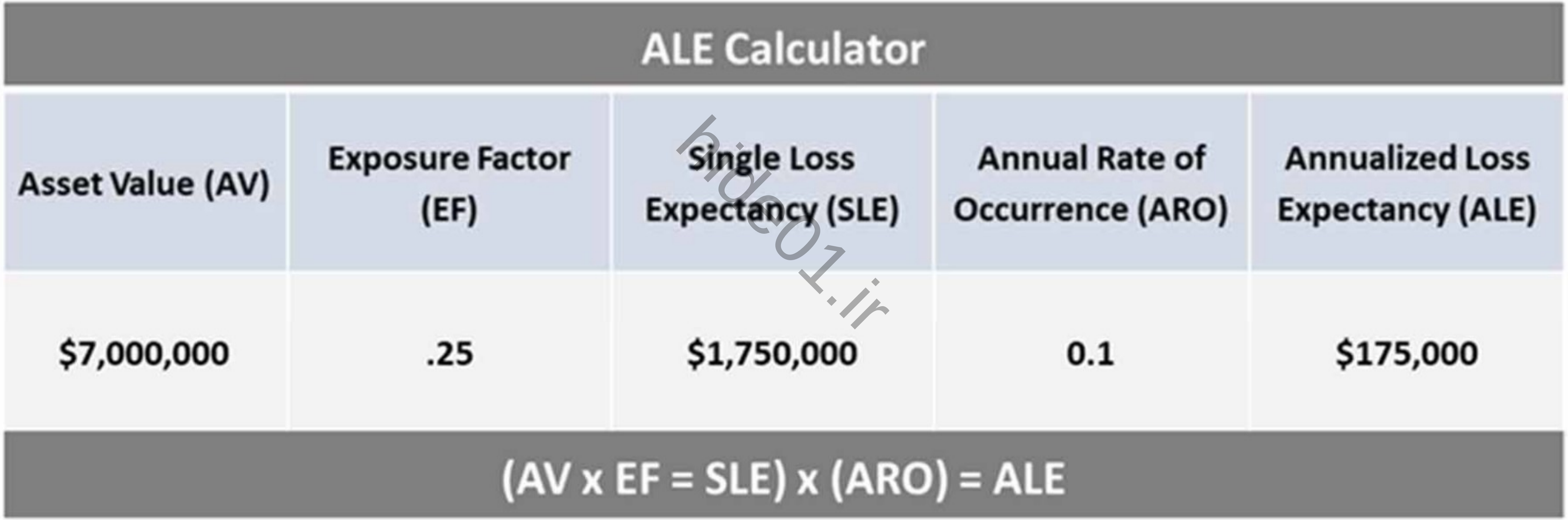
RISK CALCULATION FORMULAS

- There are many risk calculation methodologies and types of calculations that can be applied.
- Calculations are valuable when determining risk treatment.
  - Not every risk should be invested in equally.
- Risk treatments should be commensurate with the value of the asset and potential damage from a realized risk.
- Risk formulas allow CISOs and risk managers to apply effective risk management ranking them within the risk register.

RISK CALCULATION FORMULA

- **Asset Value (AV):** The value of an asset, can be expressed as a monetary value or within a rating schema (such as high, medium, low)
- **Exposure Factor (EF):** The estimated damage or impact that a realized threat would have on an asset.
- **Single Loss Expectancy (SLE):** The projected loss to the business based on an adverse asset event.
- **Annual Rate of Occurrence (ARO):** Estimated number of times the threat could occur within a calenda year.
- **Annualized Loss Expectancy (ALE):** Projected annual business loss of an asset.

RISK CALCULATION FORMULA: EXAMPLE



ALE Calculator

Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Annual Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
$7,000,000	.25	$1,750,000	0.1	$175,000

(AV x EF = SLE) x (ARO) = ALE

RISK MANAGEMENT FRAMEWORKS

- Frameworks provide a broad overview, outline, or guidance for supporting an approach to a specific objective.
- They also serve as a general guide that can be modified as required by adding or deleting items within the framework.
- The CISO should select the risk management framework or approach that best supports the organization.
- Numerous frameworks exist to guide the processes of identifying, treating, and monitoring information security risks in an organization.

RISK MANAGEMENT FRAMEWORKS: CATEGORIES

- Cybersecurity risk management frameworks.
- Enterprise Risk Management (ERM) frameworks.
- General risk management frameworks.
- Risk assessment methodologies.

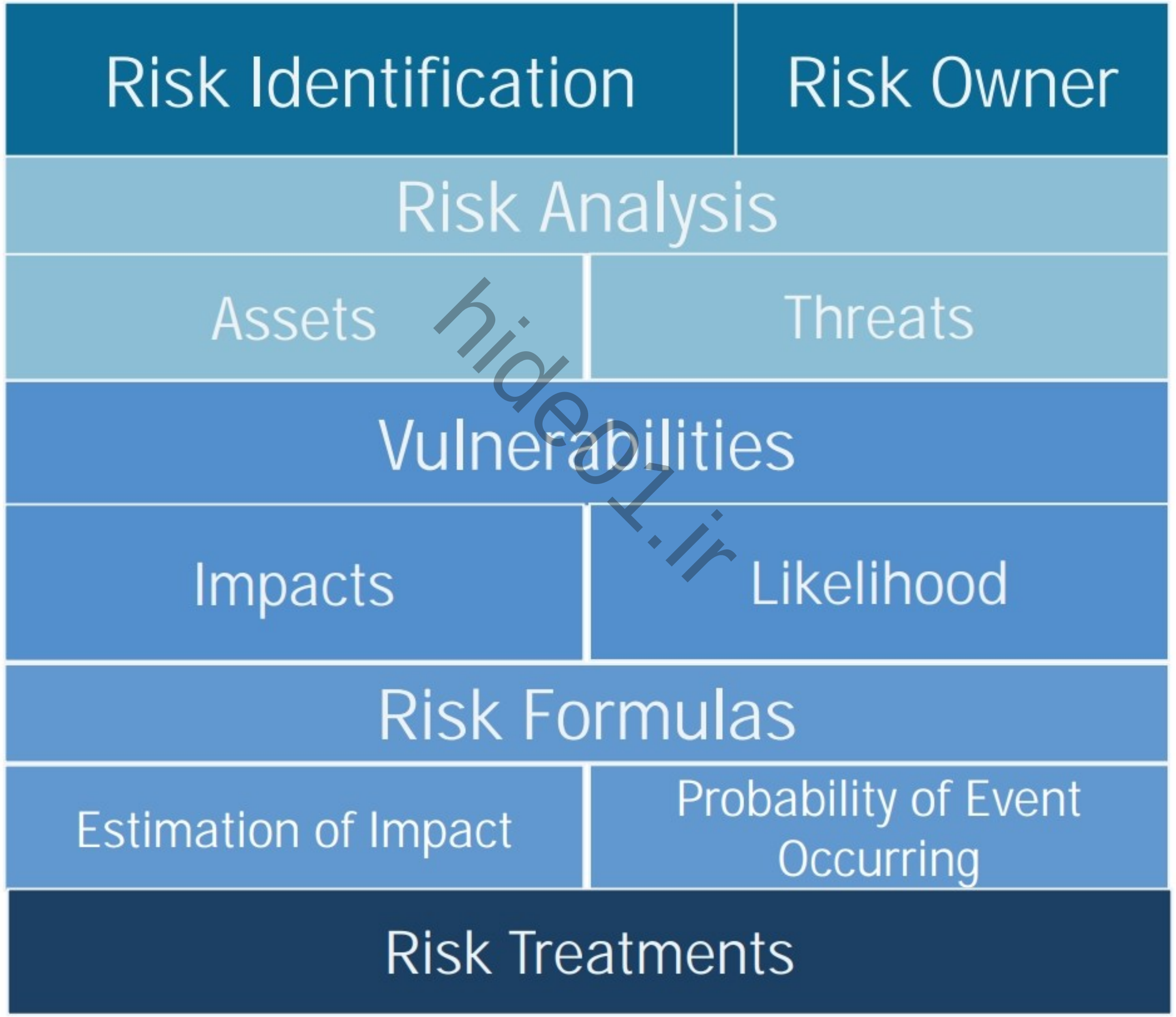
RISK MANAGEMENT FRAMEWORKS: CATEGORIES

Cybersecurity Risk Management Frameworks	Enterprise Risk Management (ERM) Frameworks	Risk Assessment Methodologies	General Risk Management Frameworks
COBIT 5 for Risk (ISACA)	COSO Enterprise Risk Management Framework	Information Risk Assessment Methodology 2 (IRAM2)	IRGC Risk Governance Framework
Factor Analysis of Information Risk (FAIR)	RMA Enterprise Risk Management (ERM)	Facilitated Risk Analysis Process (FRAP)	Operational Risk Management Framework (RMA)
ISO/IEC 27005:2018 Information Security Risk Management	ISO/IEC 31000:2018 Framework and Process for Managing Risk		
NIST SP 800-37 Rev. 2 Risk Management Framework			
TARA (Threat Assessment Risk Analysis) Management Framework			
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)			
The Risk IT Framework - ISACA			

ISO 27005

- International Organization for Standardization (ISO):
  - 27005:2018 - Security Risk Management Guidelines.
  - Systematic approach to Information Security Risk Management (ISRM).
  - Targeted toward CISOs and auditors.
  - Provides for a framework allowing continual risk management and regular risk program reviews.

ISO 27005 FRAMEWORK



Risk Identification

Risk Owner

Risk Analysis

Assets

Threats

Vulnerabilities

Impacts

Likelihood

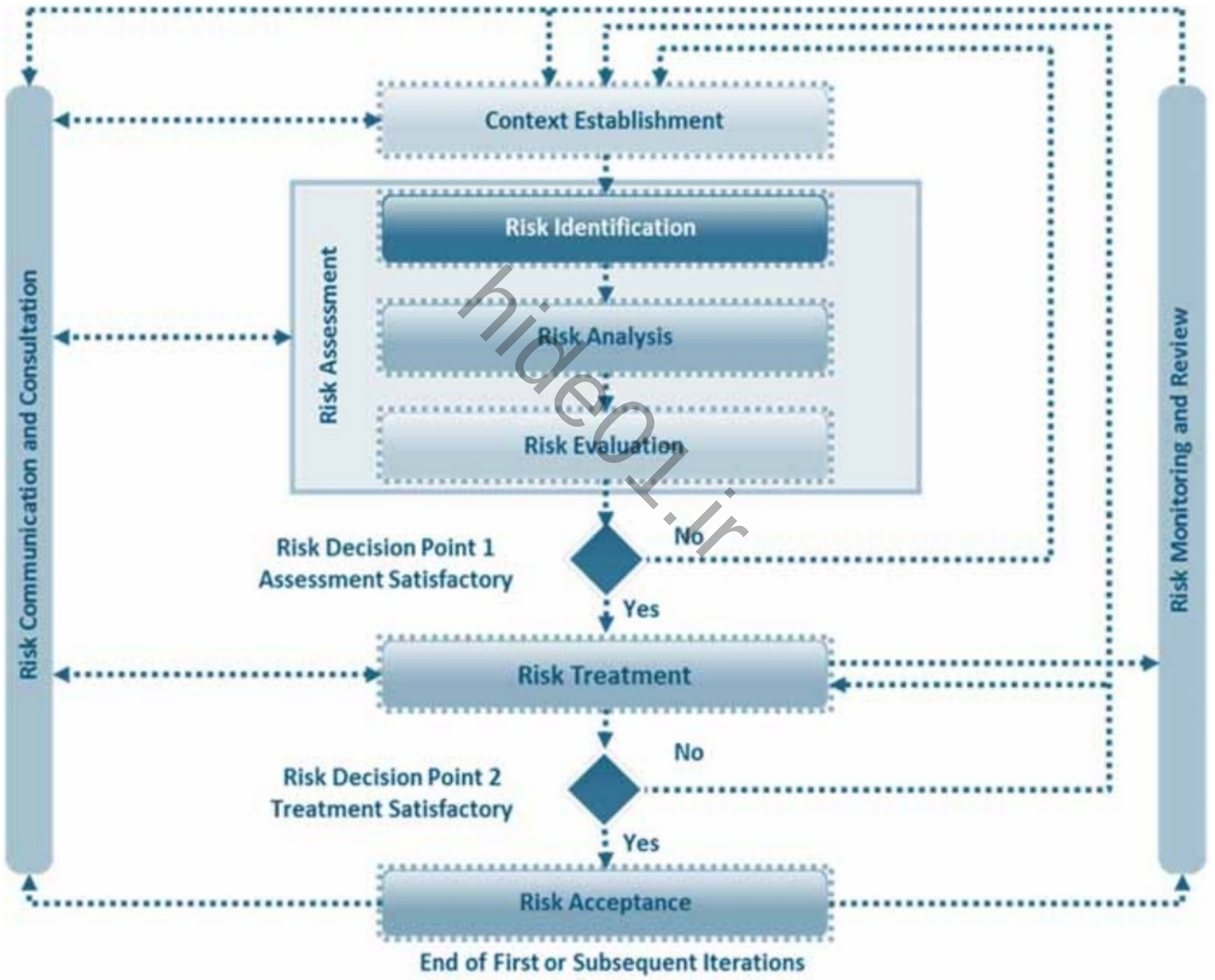
Risk Formulas

Estimation of Impact

Probability of Event Occurring

Risk Treatments

ISO 27005 RISK MANAGEMENT WORKFLOW



(Source: ISO/IEC 27005: 2018, "International Standard Information Technology-Information technology Security techniques -Information security risk management" (3rd ed.), Geneva: ISO Copyright Office. P. (4).)

ISO 27005: CONTEXT ESTABLISHMENT

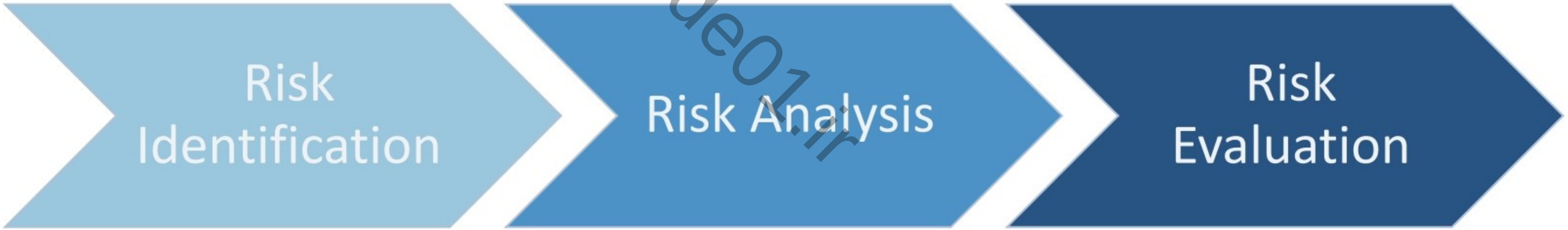
- The requirements to establish context for information security risk management are defined in Section 7 of ISO 27005.
- Inputs are gathered and evaluated when establishing context.
- The process of establishing context identifies the conditions and boundaries of a risk assessment.
- This output includes the scope and boundaries of the risk assessment, and identification of details of the organization's assets on which the risk assessment will be performed.

ISO 27005: RISK ASSESSMENT

- **Input**: Risk assessment context consisting of the scope and boundaries.
- **Action**: Risks should be identified, quantified or qualitatively described and prioritized against the risk evaluation criteria and objectives relevant to the organization.
- **Implementation Guidance:** risk assessments quantitatively or qualitatively describe the risk and enables treatment prioritization.
- **Workflow**: Risk assessments consist of the following activities:
  - Risk identification.
  - Risk analysis.
  - Risk evaluation.
- **Output**: List of identified risks prioritized according to the risk evaluation.

ISO 27005: WORKFLOW

- Risk assessment in ISO 27005 is a sequence of activities that help an organization identify risks and determine their potential impact. Each step builds upon the previous one to produce the prioritized list of risks affecting the organization.



Identification of:

- Assets
- Threats
- Existing controls
- Vulnerabilities
- Consequences

Assessment of:

- Consequences
- Incident likelihood
- Level of risk determination

Develop A Prioritized List of Risks:

- Information security properties - relevance
- Business impact

ISO 27005 Risk Assessment Workflow

ISO 27005: RISK IDENTIFICATION

- Risk identification determines what could happen to potentially cause a loss.
- Identification also helps gain insight into how, where, and why a loss may happen.
- Identification evaluates assets, threats, existing controls, vulnerabilities, and consequences to create a list of scenarios.
- Resulting consequences are mapped to assets and business processes.

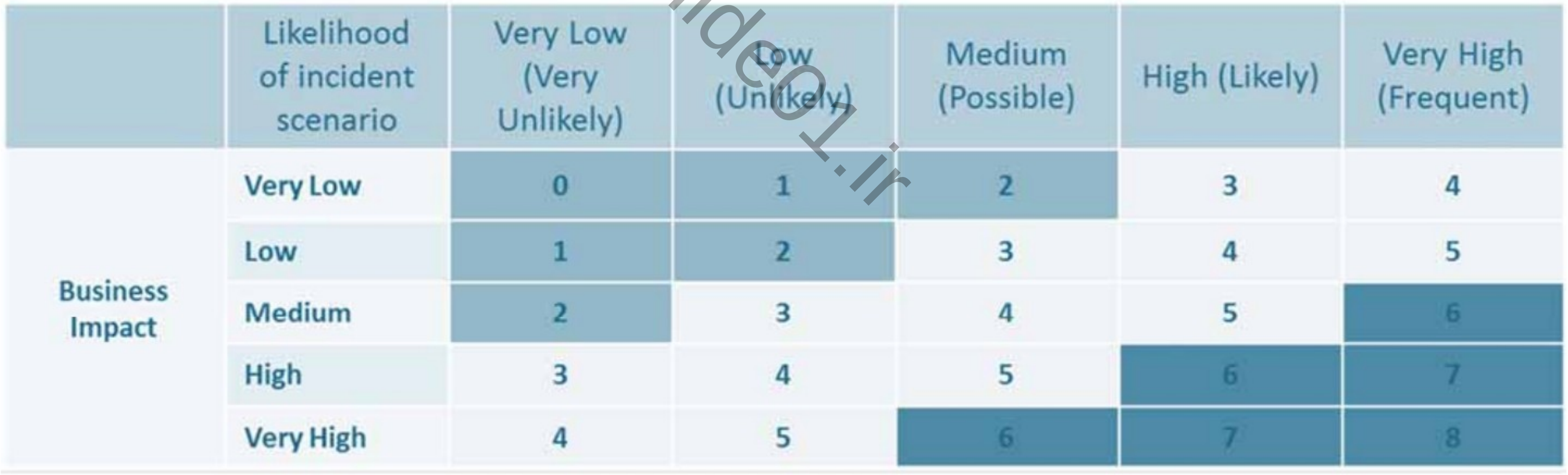
ISO 27005: RISK ANALYSIS

Risk analysis produces a list of risk value levels assigned by taking output from the risk identification and using it as input for the following three assessments:

1. **Consequences:** this primarily evaluates the asset value in relation to the occurrence of a threat.
2. **Incident likelihood:** Potential of occurrence and frequency of a realized risk.
3. **Level of risk determination:** Output from first two steps allow an organization to assign values that communicate the results of the probability and cost of a realized risk.

ISO 27005: RISK SCORE TABLE

The following table provides a sample of a risk scale of 0 to 8 by mapping likelihood to business impact in order to generate the risk score:



	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Generic Level of Risk Determination Chart

27005: RISK EVALUATION

- Risk evaluation combines the list of risks with:
  - Value levels assigned from the risk analysis phase.
  - The risk evaluation criteria from the context establishment phase.
  - The risk acceptance criteria defined by the organization.
- This produces a prioritized list of risks with two important considerations:
  - Information security properties (Confidentiality, Integrity, Availability).
  - The importance of the business process or activity supported by a particular asset or set of assets.

ISO 27005: RISK TREATMENT

The prioritized set of risks produced during the risk assessment supports decisions for the risk treatment plan.

The plan is developed as part of the risk management workflow in ISO 27005. The goal of risk treatment is to manage unacceptable risks within the organization.

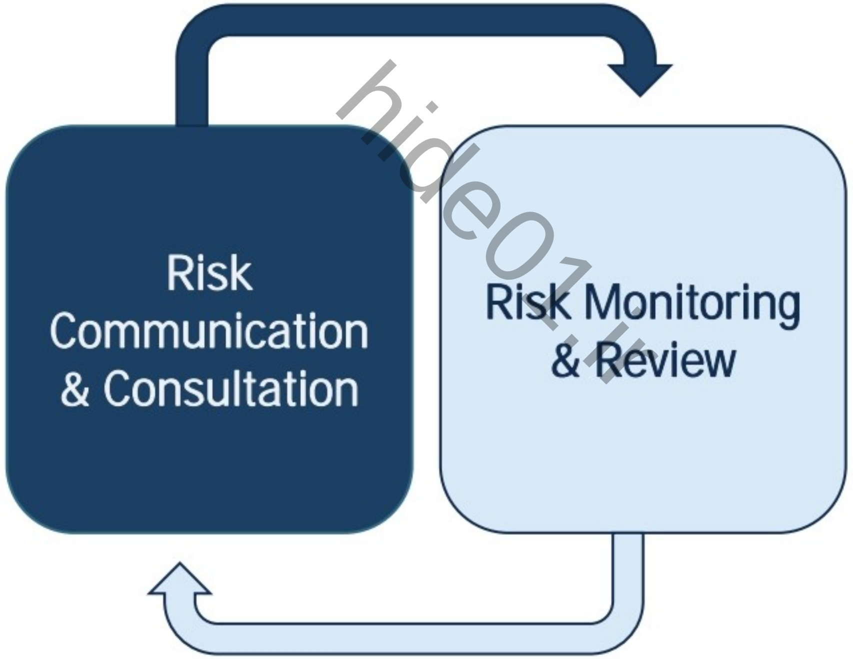
- Review prioritized list from the risk assessment.
- Verify that the risk assessment results are valid.
- Develop recommendations for risk treatment.

ISO 27005: RISK ACCEPTANCE

- High risk items can be accepted by the business owners.
  - CISO responsibility – document acceptance, continue monitoring and reporting.
- Risk acceptance more normally occurs after risk treatment is applied.
  - Residual risk is evaluated after treatment.
  - Risk appetite determines risk acceptance.
- Control effectiveness influences risk acceptance.
- Risk acceptance is a formal process that requires record keeping.
- The CISO is not responsible for risk beyond management of the security program.

ISO 27005: RISK FEEDBACK

Regularly communicate risks and provide advisement to asset or business owners.



Monitor the risks and initiate reassessment when risks change within the environment.

ISO 27005: RISK COMMUNICATION AND CONSULTATION

- Communication is important throughout risk management processes.
- This communication includes:
  - Outcomes of assessments.
  - Status reports.
  - Assessment issues.
  - General concerns.
- Typically, if a critical risk is identified during an assessment, it is *immediately* communicated to the business owner.
- A risk communication plan should include insight about the evolving nature of the risks that will influence risk treatment decisions.

ISO 27005: RISK MONITORING AND REVIEW

Continuous risk management feedback loop

- Monitor risk
  - Continued observation of risks and factor affecting them
- Review risk
  - Internally with the risk team
  - Externally with the business

ISO 27005: RISK MONITORING

Organizations should ensure the following are continually monitored:

- New assets that have been included in the risk management scope.
- Modification of asset values.
- New threats to the organization that have not been assessed.
- Possible new or increased vulnerabilities that could allow threats to exploit those vulnerabilities.
- Old vulnerabilities that could be exposed to new or reemerging threats.
- Increased consequence with assessed threats.
- Information security incidents.

RISK COMMUNICATIONS

Risk Communication Value

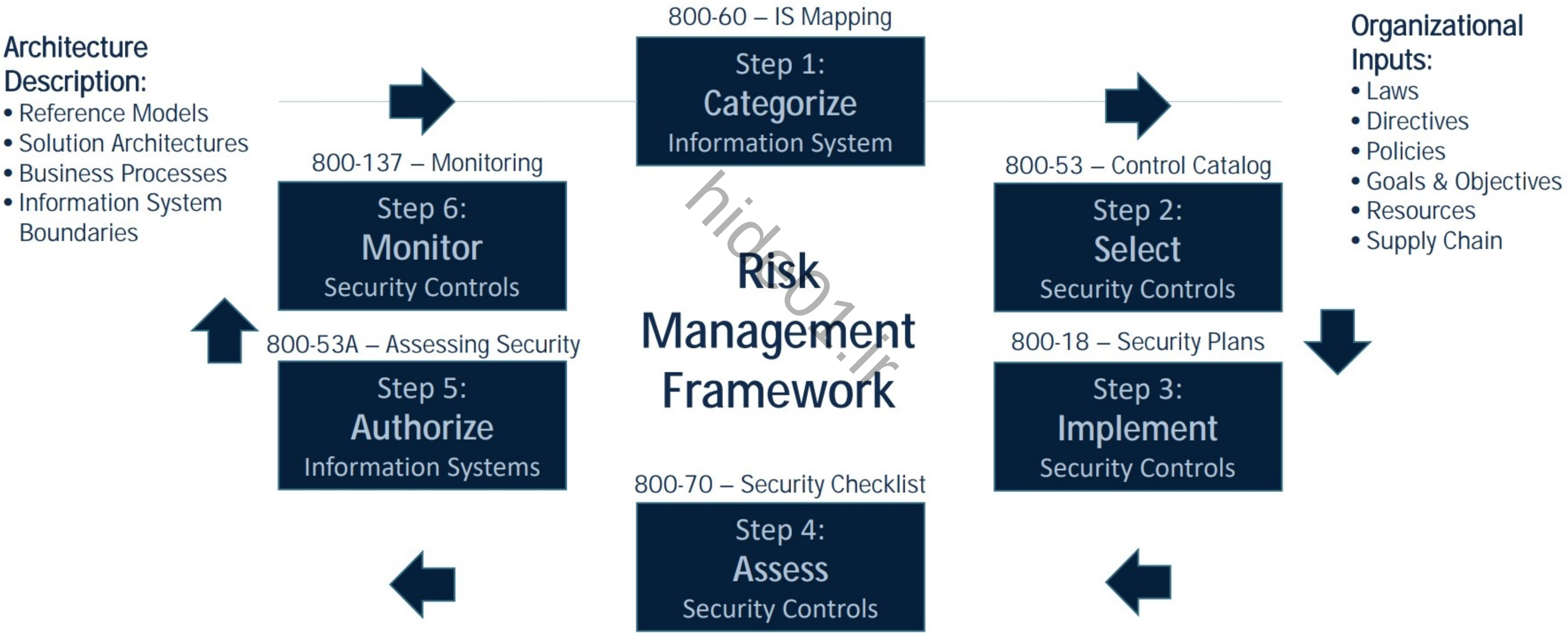
- Provide assurance of outcome.
- Collect additional risk information.
- Share assessment results.
- Avoid occurrence of breach.
- Support decision making.
- Obtain new security knowledge.
- Coordinate response plans.
- Determine shareholder responsibility
- Improve awareness.

NIST SP 800-37: OVERVIEW

National Institute of Standards and Technology (NIST) – Special Publication (SP) 800-37 R2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle:

- Life cycle for risk management.
- Utilizes information from multiple NIST publications to provide guidance on how to manage risk.
  - 800-53 (Security and Privacy Controls for Information Systems and Organizations)
  - 800-30 (Guide for Conducting Risk Assessments)
  - 800-39 (Managing Information Security Risk)
- Applicable to all industries.

NIST RISK MANAGEMENT FRAMEWORK (RMF)



Architecture Description:

- Reference Models
- Solution Architectures
- Business Processes
- Information System Boundaries

800-60 – IS Mapping

Step 1: **Categorize** Information System

800-53 – Control Catalog

Step 2: **Select** Security Controls

800-18 – Security Plans

Step 3: **Implement** Security Controls

800-70 – Security Checklist

Step 4: **Assess** Security Controls

800-53A – Assessing Security

Step 5: **Authorize** Information Systems

800-137 – Monitoring

Step 6: **Monitor** Security Controls

Risk Management Framework

Organizational Inputs:

- Laws
- Directives
- Policies
- Goals & Objectives
- Resources
- Supply Chain

NIST Risk Management Framework (RMF)

NIST SP 800-37: PROCESS OVERVIEW

Step 1: Categorize the Information System – identifies the security rating of the system, process, or service.

Step 2: Select Security Controls – identifies corrective controls according to the security rating defined in the categorization step.

Step 3: Implement Security Controls – defines process for applying controls to the system. It provides a holistic approach to information security and risk management .

Step 4: Assess the Information System – evaluate the effectiveness of controls applied to the environment.

Step 5: Authorize the Information System – create list of weaknesses and the proposed remediation plan – this is the Plan of Actions and Milestones (POAM).

Step 6 : Monitor Security Controls – provides ongoing evaluation of existing controls and processes to assure controls remain effective as the system undergoes life cycle changes and modifications.

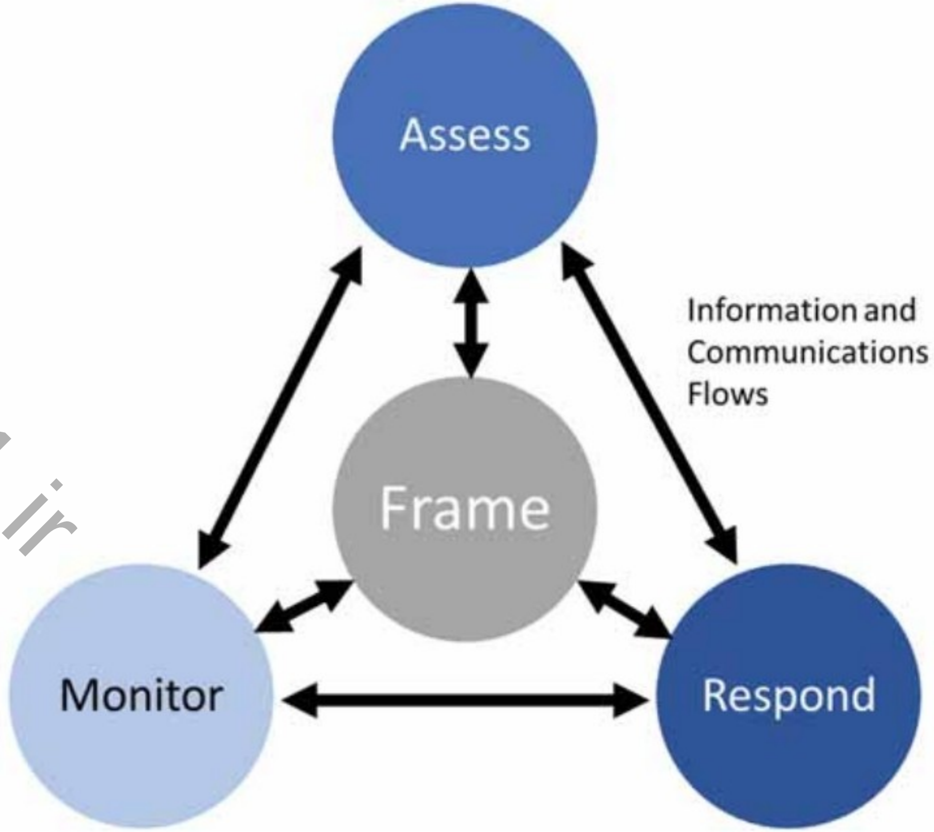
NIST RISK MANAGEMENT & ASSESSMENT

Additional NIST Publications

- Nist SP 800-37 – Risk Management Framework (RMF)
- NIST SP 800-30 – Guide for Conducting Risk Assessments
- NIST SP 800-39 – Managing Information Security Risk

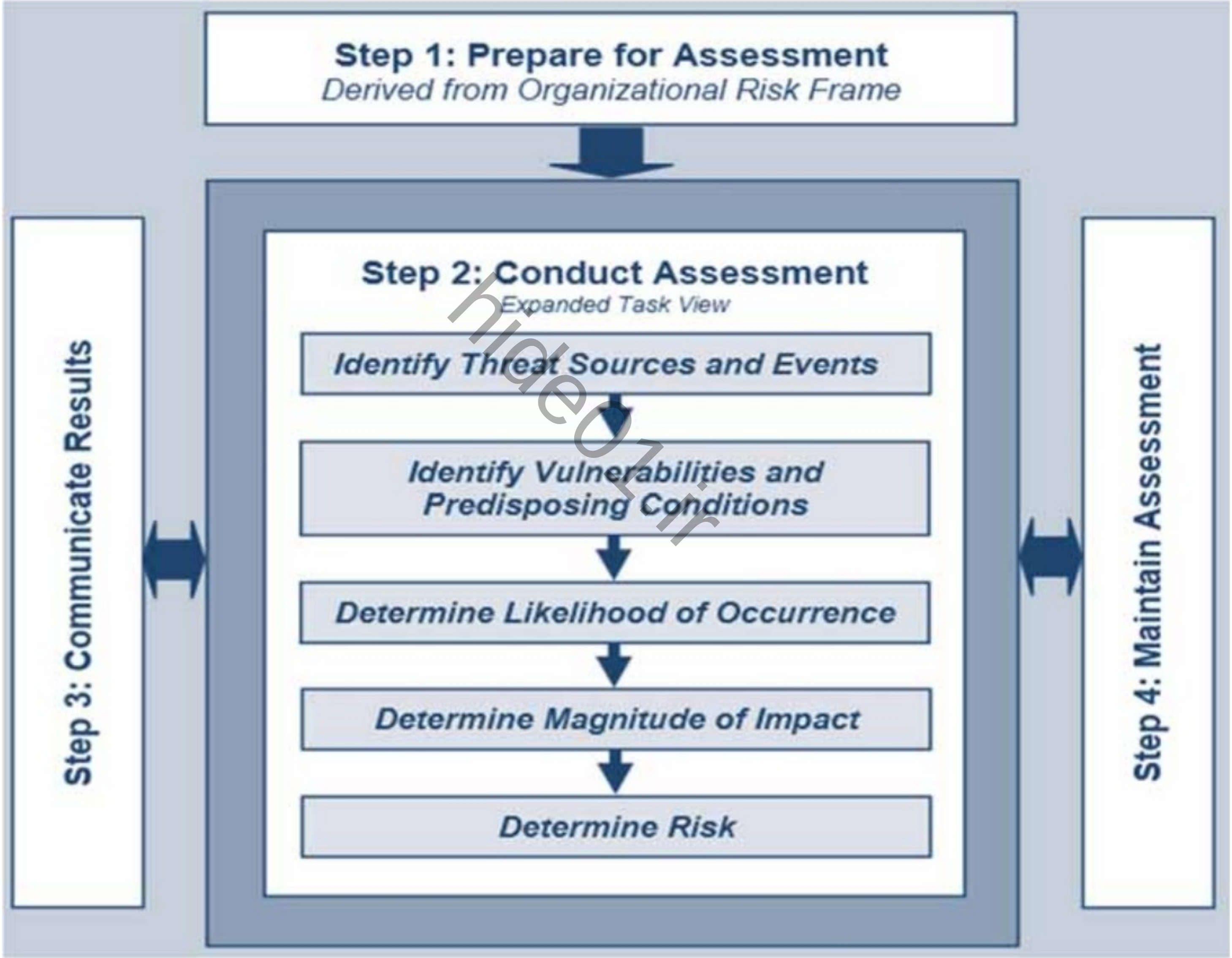
NIST SP 800-37: MANAGEMENT HIERARCHY

- **Frame**: Establish the context of risk by describing the environment and constraints of risk decisions.
- **Assess:** Expose threats and vulnerabilities.
- **Respond**: Risk treatment.
- **Monitor**: Continuous evaluation of risk.



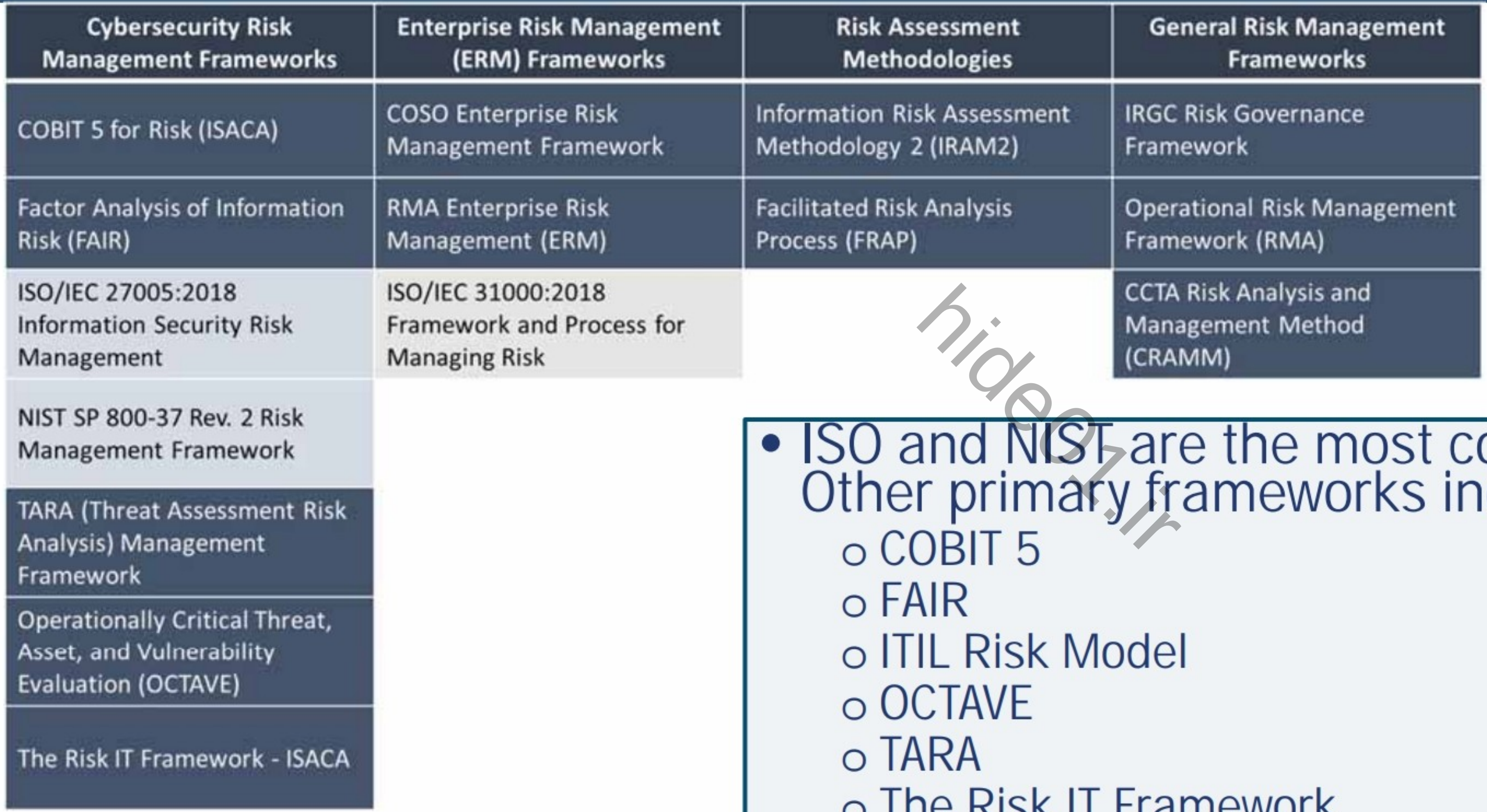
NIST Risk Management Hierarchy

NIST SP 800-37: RISK ASSESSMENT PROCESS



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

OTHER RISK FRAMEWORKS

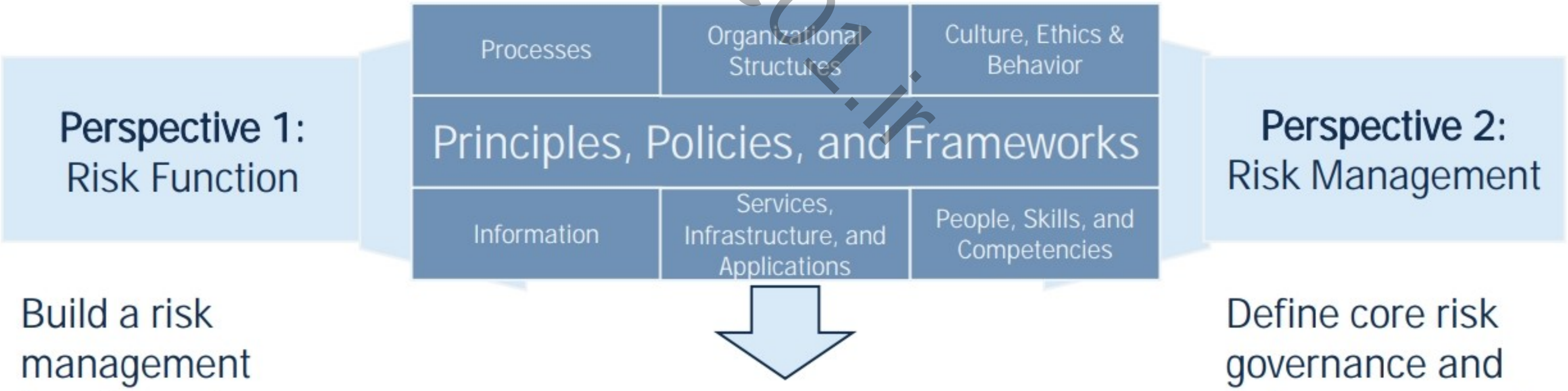


Cybersecurity Risk Management Frameworks	Enterprise Risk Management (ERM) Frameworks	Risk Assessment Methodologies	General Risk Management Frameworks
COBIT 5 for Risk (ISACA)	COSO Enterprise Risk Management Framework	Information Risk Assessment Methodology 2 (IRAM2)	IRGC Risk Governance Framework
Factor Analysis of Information Risk (FAIR)	RMA Enterprise Risk Management (ERM)	Facilitated Risk Analysis Process (FRAP)	Operational Risk Management Framework (RMA)
ISO/IEC 27005:2018 Information Security Risk Management	ISO/IEC 31000:2018 Framework and Process for Managing Risk		CCTA Risk Analysis and Management Method (CRAMM)
NIST SP 800-37 Rev. 2 Risk Management Framework			
TARA (Threat Assessment Risk Analysis) Management Framework			
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)			
The Risk IT Framework - ISACA			

- ISO and NIST are the most common risk frameworks. Other primary frameworks include:
  - COBIT 5
  - FAIR
  - ITIL Risk Model
  - OCTAVE
  - TARA
  - The Risk IT Framework
- Not all frameworks can be covered in course.

COBIT RISK MANAGEMENT

- Control Objectives for Information and Related Technology (COBIT 5).
- Published by ISACA.
- Not specifically designed for risk management.
  - COBIT provides 2 perspectives on risk management.



Processes
Organizational Structures
Culture, Ethics & Behavior
Principles, Policies, and Frameworks
Information
Services, Infrastructure, and Applications
People, Skills, and Competencies

Perspective 1: Risk Function

Build a risk management function using Cobit enablers.

Perspective 2: Risk Management

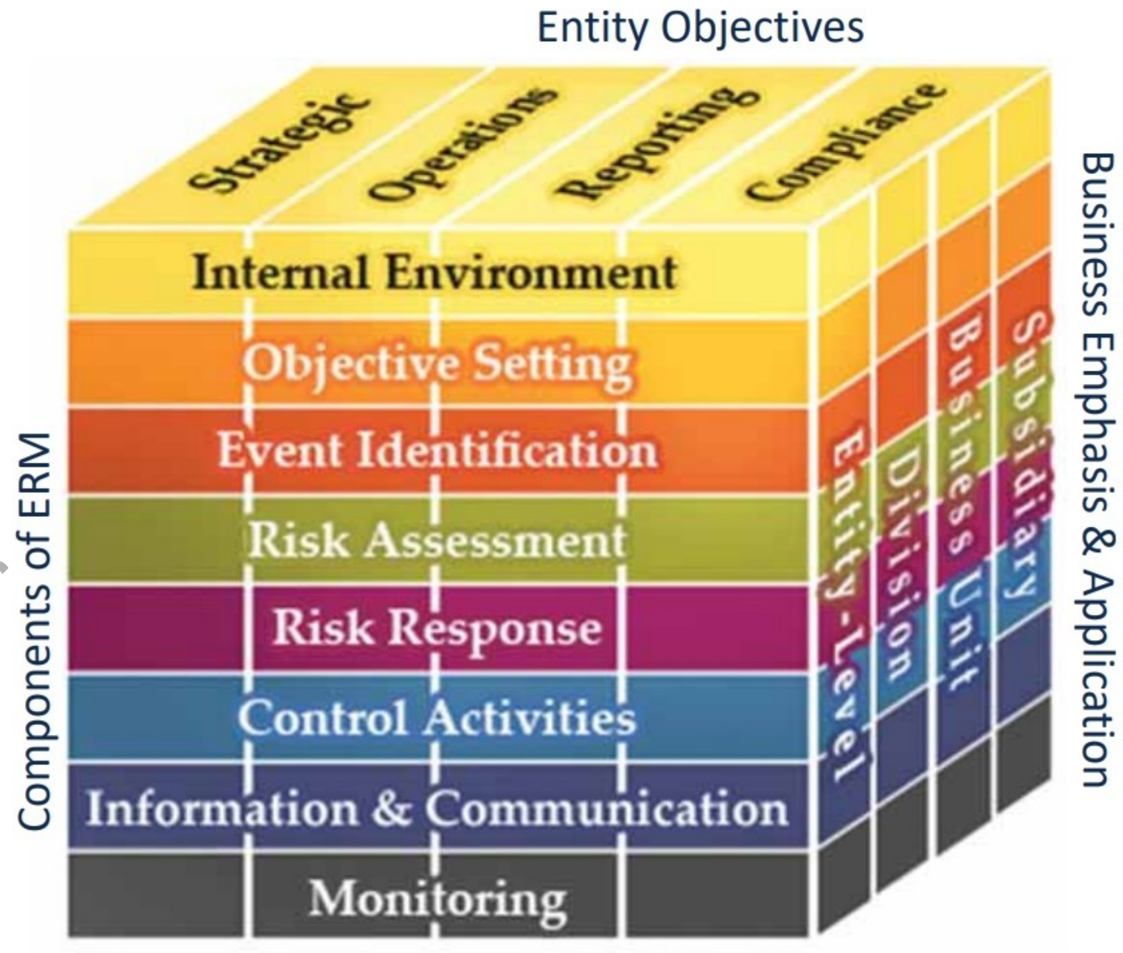
Define core risk governance and risk management processes using Cobit enablers.

Risk Management Program

Source: ISACA, COBIT 5 for Risk

COSO ENTERPRISE RISK MANAGEMENT INTEGRATED FRAMEWORK

- COSO is an Enterprise Risk Management (EM) framework.
- Published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) .
- Defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language.

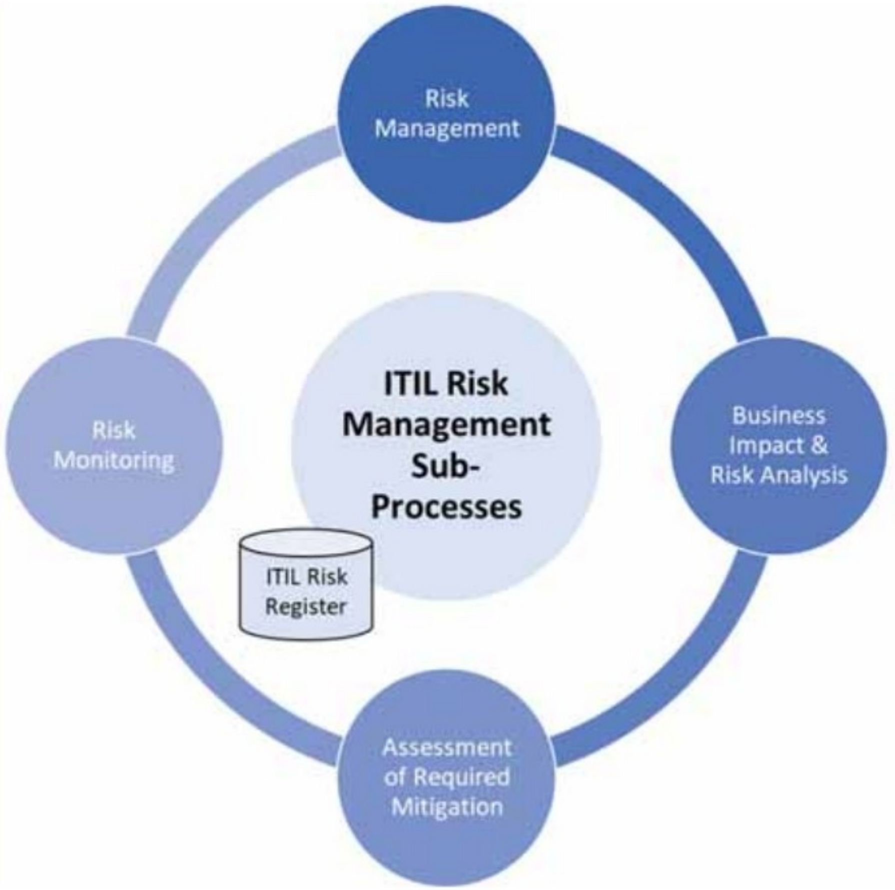


Source: Treadway Commission

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

- Information Technology Infrastructure Library (ITIL):
  - Owned by Axelos, a joint venture of Capita and the UK Cabinet Office.
  - Risk Management is not an officially defined process.
  - ITIL Risk Management is the process of identifying, assessing, and prioritizing potential business risks.
  - Risk Management, in ITIL, is an integral part of the Service Management Lifecycle.

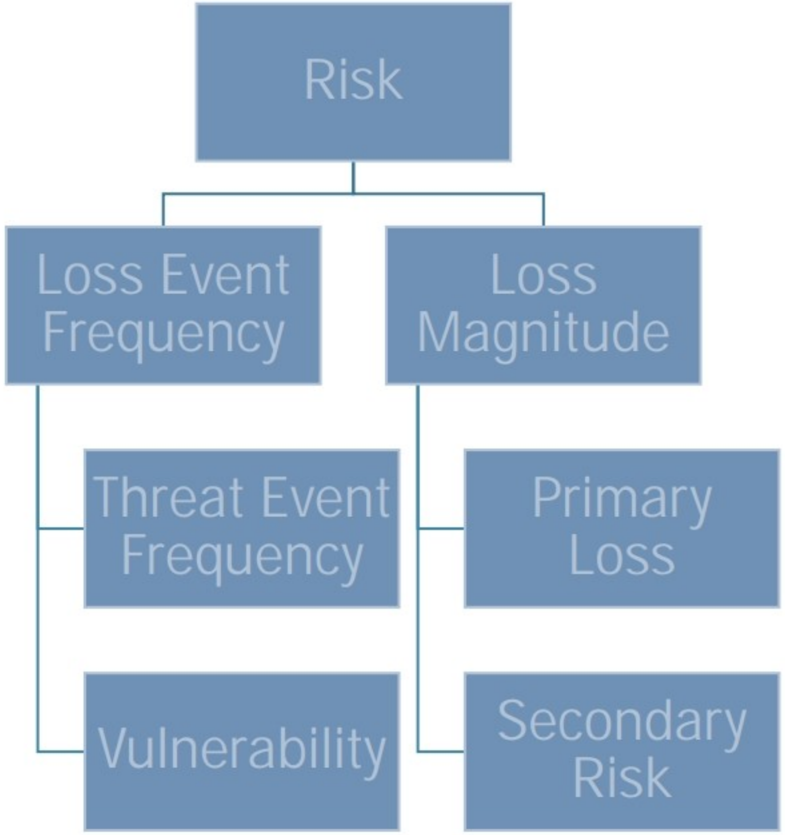
- ITIL Risk Definition: *"A possible event that could cause harm or loss or affect the ability to achieve objectives."*


Risk Management
Business Impact & Risk Analysis
Assessment of Required Mitigation
Risk Monitoring
ITIL Risk Management Sub-Processes
ITIL Risk Register

ITIL Risk Management Model

FACTOR ANALYSIS OF INFORMATION RISK (FAIR)

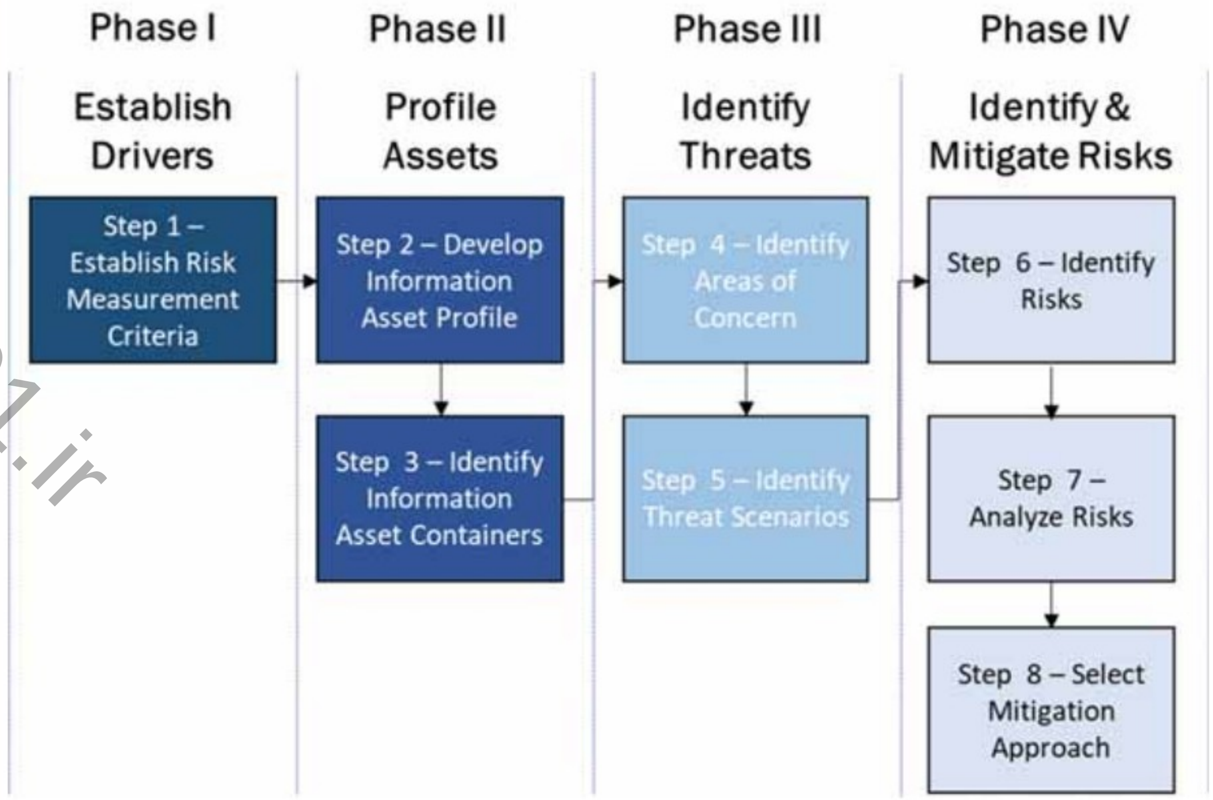
- Factor Analysis of Information Risk (FAIR):
  - Published by FAIR Institute.
  - Quantitative approach.
  - Considered a risk model.
- Value at Risk (VaR) framework for cybersecurity and operational risk.
- International standard.
- Includes a standard taxonomy (classification) and ontology (relationship model) for information and operational risk.
- Modeling construct for analyzing complex risk scenarios.



Source: FAIR Institute, FAIR Model

OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION (OCTAVE)

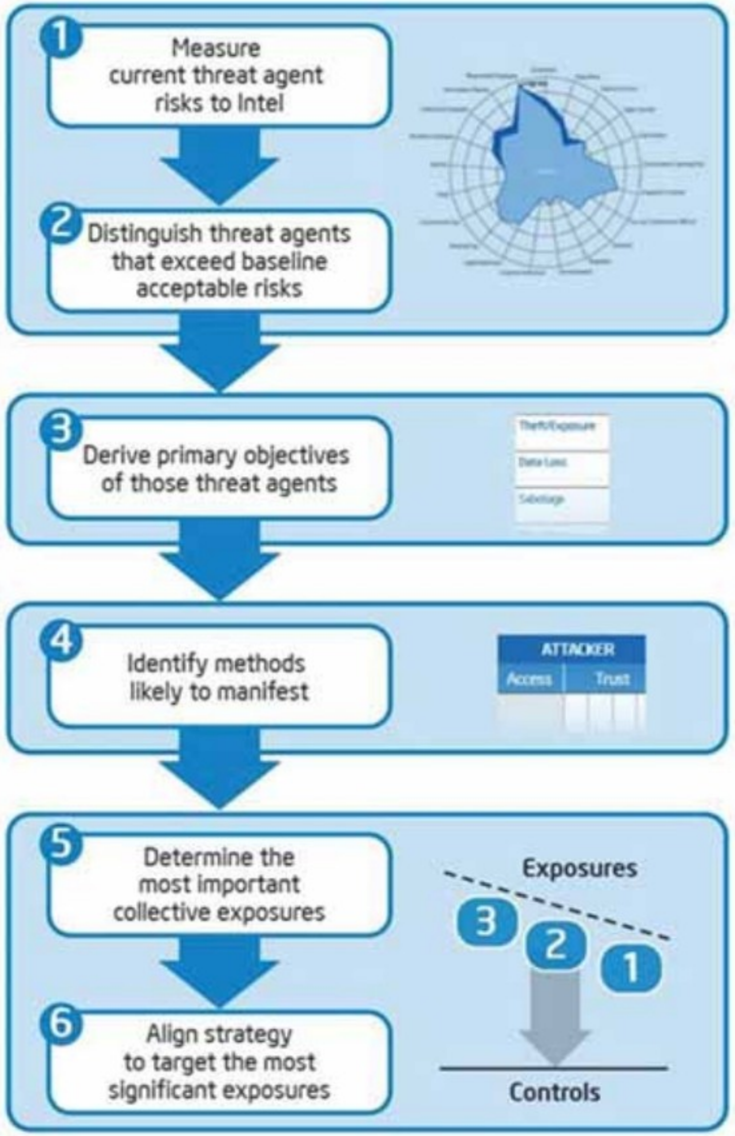
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE):
  - Developed by Carnegie Mellon University CERT Coordination Center
  - Asset centric, uses a lean risk assessment.
- Standardized approach to a risk-driven and practice-based information security evaluation.
- Four phase, eight step process.


Phase I
Establish Drivers
Phase II
Profile Assets
Phase III
Identify Threats
Phase IV
Identify & Mitigate Risks
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Source: Carnegie Mellon University

THREAT ASSESSMENT AND REMEDIATION ANALYSIS (TARA)

- Threat Assessment and Remediation Analysis (TARA):
  - Published by MITRE Corporation.
  - Catalog of attack vector and countermeasure data.
  - Similar to Microsoft's STRIDE threat modeling system.
- Engineering methodology to identify, prioritize, and respond to cyber threats through the application of countermeasures.



1 Measure current threat agent risks to Intel

2 Distinguish threat agents that exceed baseline acceptable risks

3 Derive primary objectives of those threat agents

4 Identify methods likely to manifest

5 Determine the most important collective exposures

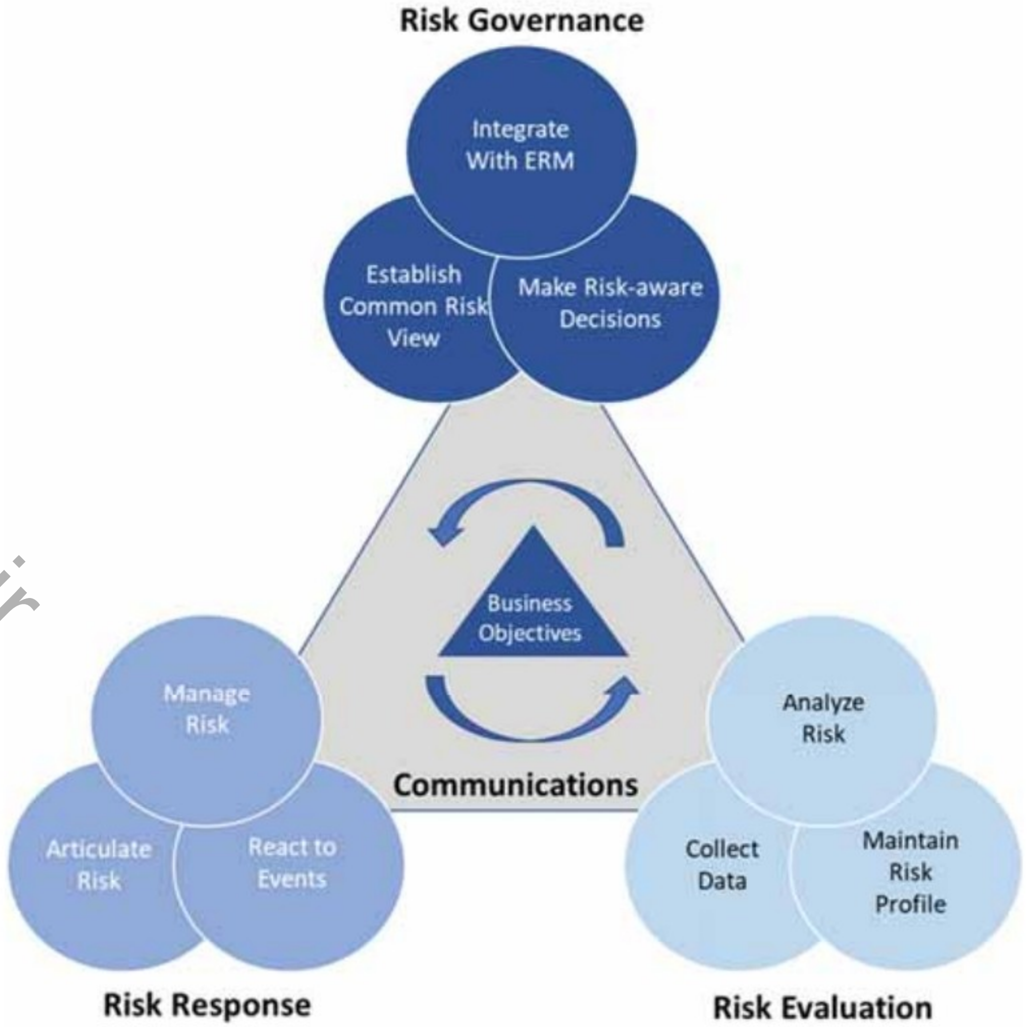
6 Align strategy to target the most significant exposures

Source: TARA Methodology

THE RISK IT FRAMEWORK

- The Risk IT Framework:
  - Published by ISACA.
  - Complements COBIT 5.
- Designed for COBIT clients to implement a risk management program.
- Treats IT risk as a business risk.

Note: Missing in BOK.



Source: ISACA, The Risk IT Framework

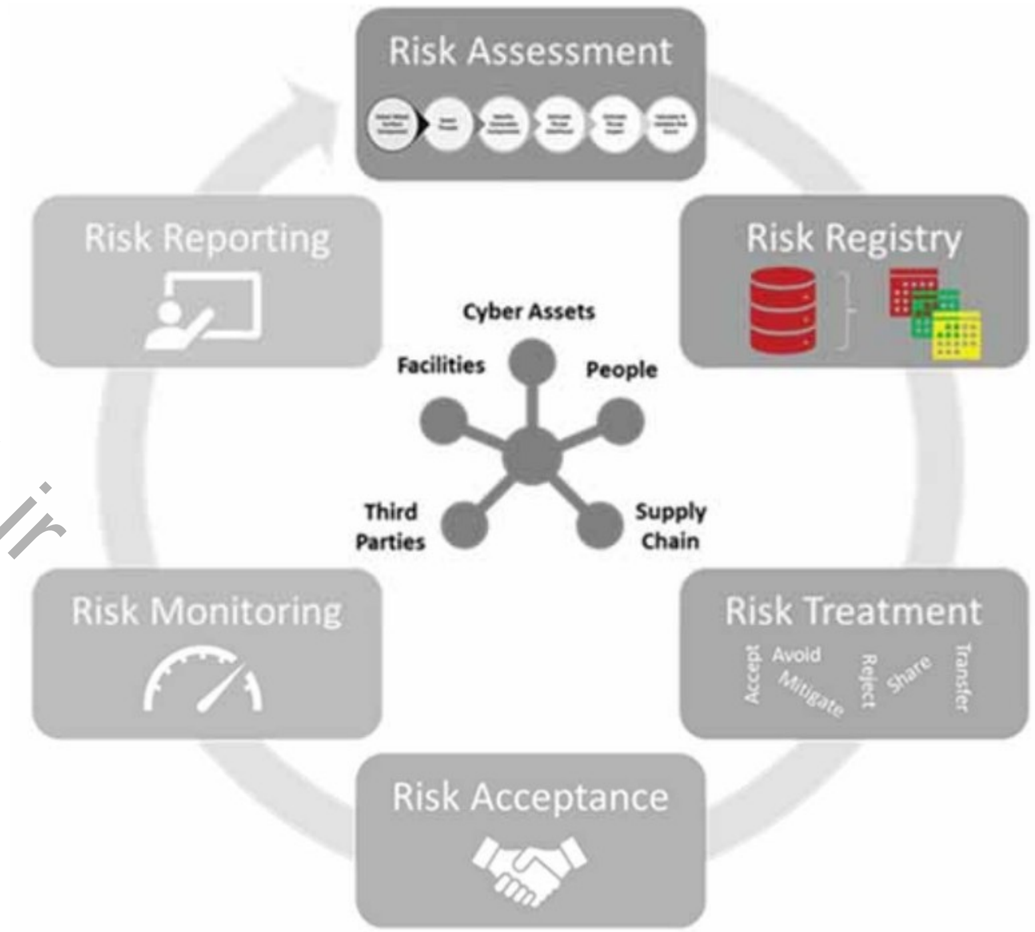
RISK MANAGEMENT POLICIES AND PROCEDURES

- Accurate documentation is critical for consistent and repeatable risk management program. This includes:
  - Policies.
  - Procedures.
  - Processes.

- Unique terms and information in risk management policies:
  - Risk appetite.
  - Risk tolerance.
  - Risk ownership.
  - Risk algorithms.
  - Risk model.

RISK MANAGEMENT LIFECYCLE

- Effective risk management includes an articulated lifecycle.
- Ensures risk is managed in a continuous and methodical manner.
- Closed loop lifecycle.



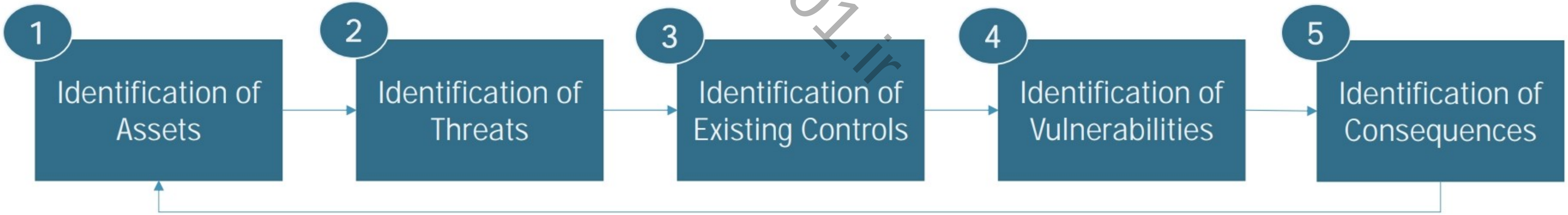
Risk Management Lifecycle. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License)

RISK MANAGEMENT LIFECYCLE

- Risk assessment with three types:
  - Quantitative
  - Qualitative
  - Hybrid
- Risk registry – the ledger of identified risks
  - All risk information – from business thru ratings to management or treatment of the risk.
- Risk treatment – decision as to risk disposition.
- Rik acceptance – initial or resulting risk decision.
- Risk monitoring – continual analysis for changes in the risk.
- Risk reporting – organization, Board visibility.

RISK MANAGEMENT PROGRAM IMPLEMENTATION USE CASE

ISO 27005 example of a risk program implementation.

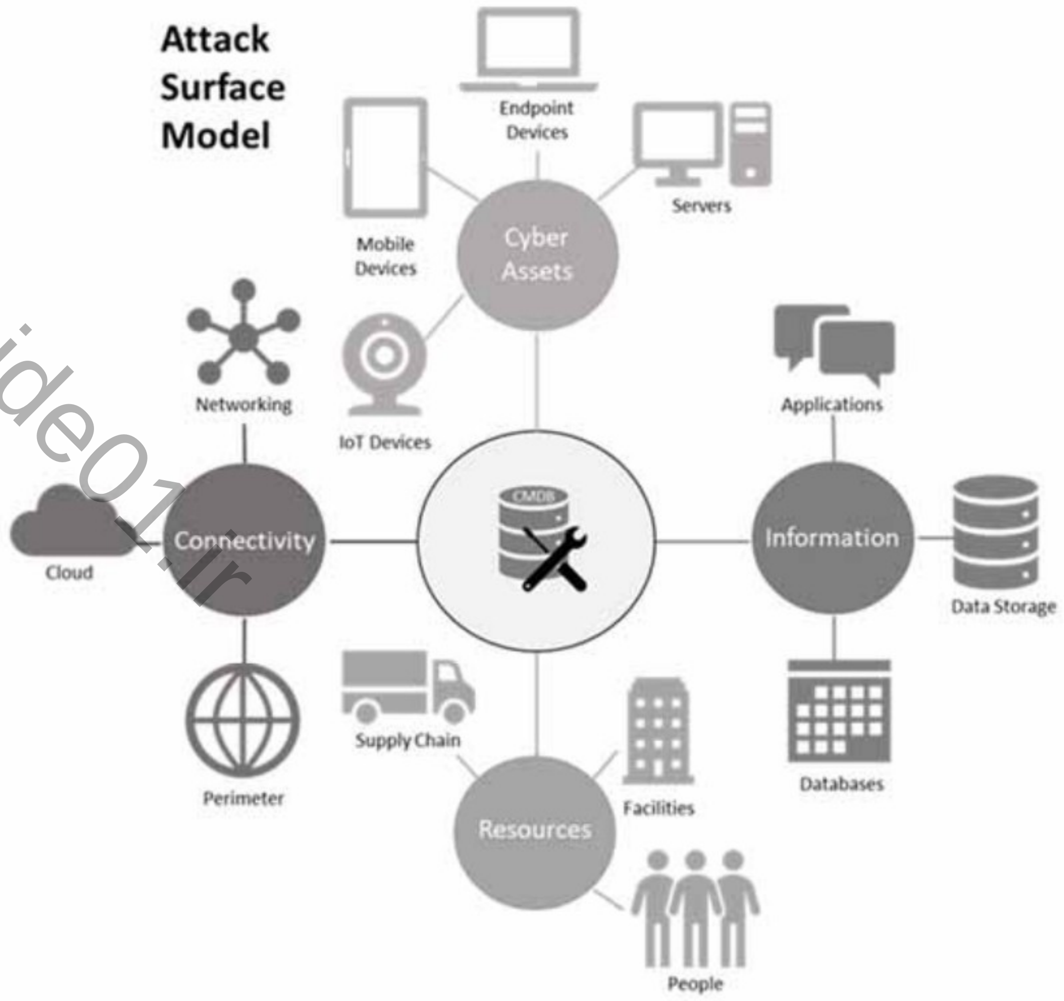

1
Identification of Assets
2
Identification of Threats
3
Identification of Existing Controls
4
Identification of Vulnerabilities
5
Identification of Consequences

STEP 1: IDENTIFICATION OF ASSETS

- Attack surface:
  - Assets – anything of value.
  - Represents where an attacker would focus.
- Asset inventory:
  - Repository of asset information
    - System
    - Owner
    - Data
    - Business process
  - Defines scope of risk management program.
- Asset owners = risk owners.
- Shadow IT assets – unregistered assets causing unknown risk.

STEP 1: IDENTIFICATION OF ASSETS

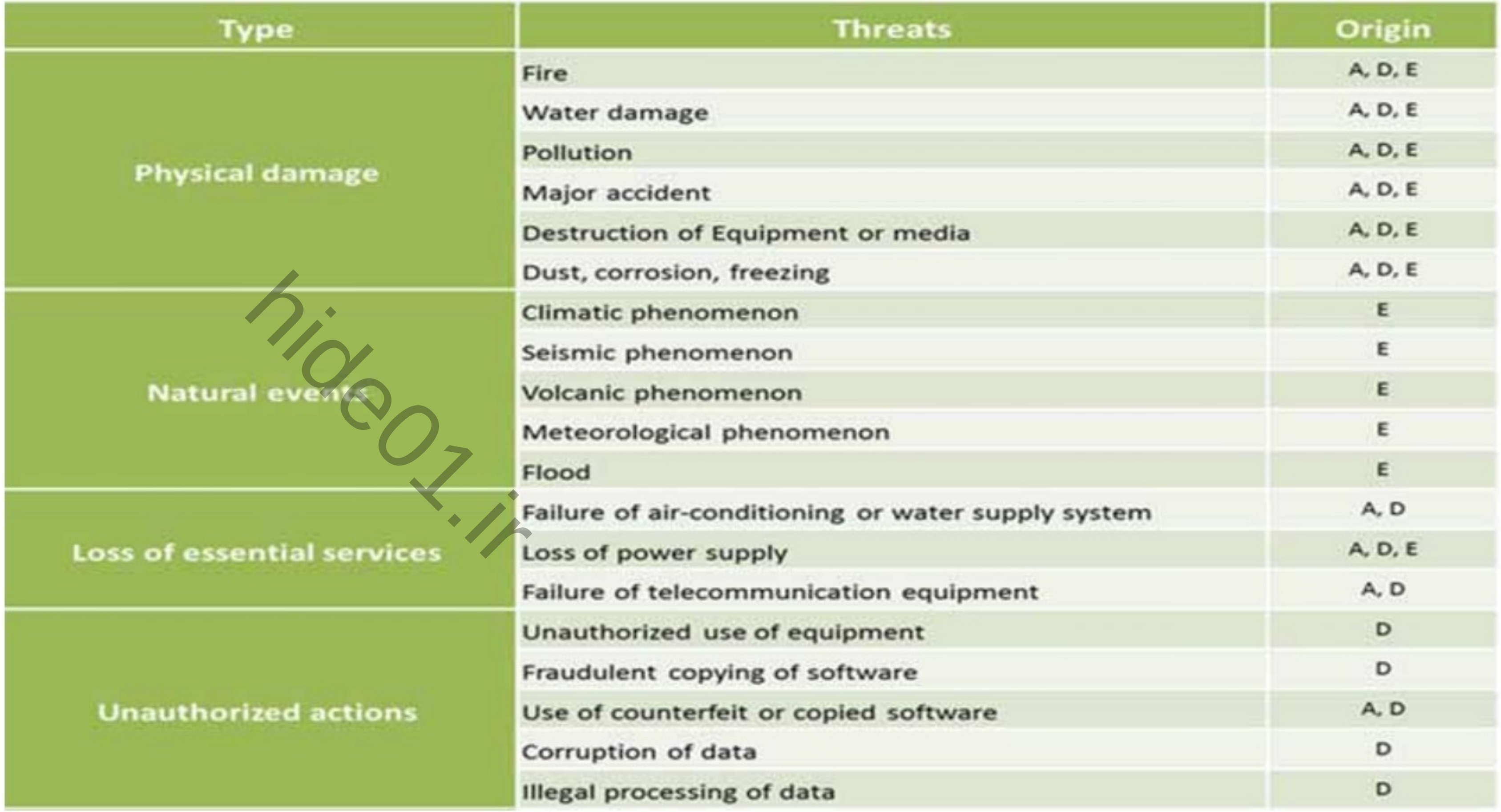
- Hackers look at organizations as something that can be exploited. The systems and data are the attack surface.
- Assets can be tangible and intangible.
- You can't protect what you can't see.



Attack Surface Model™. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License)

STEP 2: IDENTIFICATION OF THREATS

- Threats need to be clearly articulated.
- Threats are detailed in the risk register.
- Discussed further in Domain 3.



Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of Equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Unauthorized actions	Unauthorized use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D

SAMPLE THREATS

Source: ISO 27005 Annex C - Examples of Typical Threats

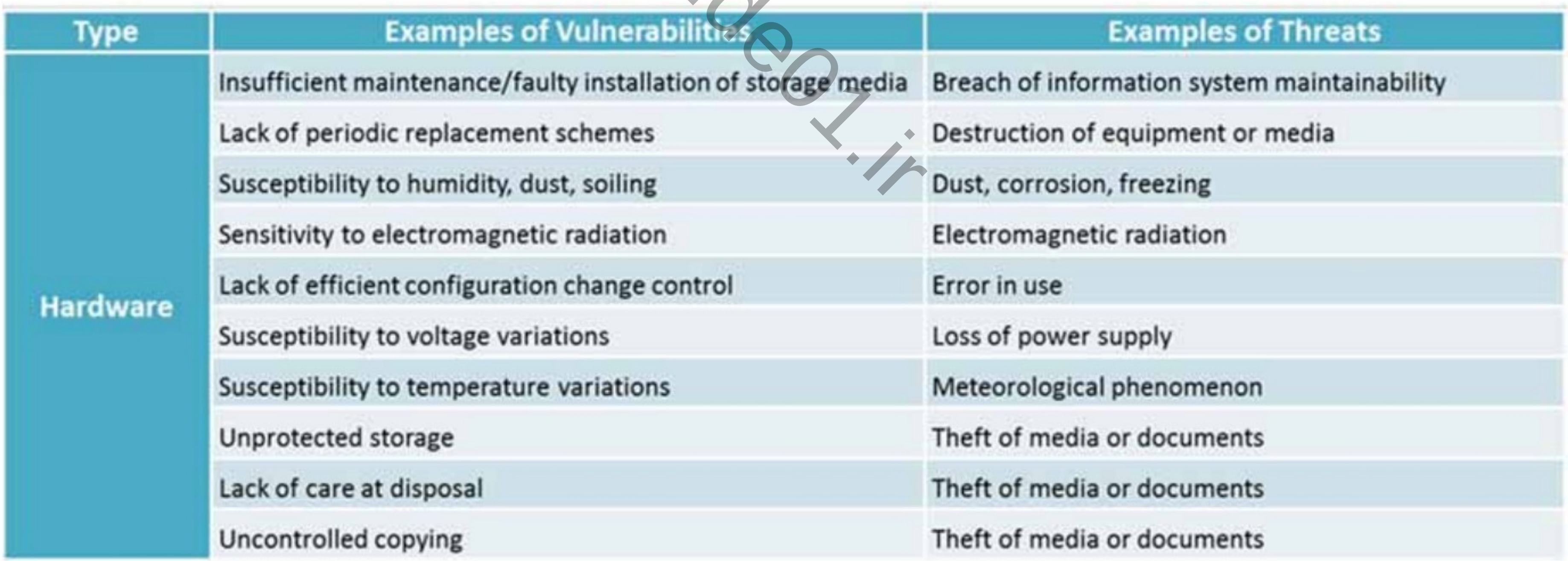
Key; A = Accidental – D = Deliberate – E = Environmental

STEP 3: IDENTIFICATION OF EXISTING CONTROLS

- Catalogue and document existing controls to understand how they provide current levels of protection.
  - Controls are generally located in policies, procedures, standards, etc.
- Eliminate inconsistency and look for disparate technologies, duplicated controls, or other inefficiencies.
- Create a controls inventory and link it to the with risk register.
- Controls are discussed further in Domain 2.

STEP 4: IDENTIFICATION OF VULNERABILITIES

- Vulnerabilities are weaknesses in an attack surface.
- Vulnerabilities represent the potential for exploit.
- Vulnerabilities are usually catalogued and integrated with the risk register.
- Discussed further in Domain 3.



Type	Examples of Vulnerabilities	Examples of Threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents

Source: ISO 27005 Annex D - Examples of Vulnerabilities

STEP 5: IDENTIFICATION OF CONSEQUENCES

- Consequences are the adverse outcomes related to loss of:
  - Confidentiality
  - Integrity.
  - Availability.
- Categorized consequences examples include:
  - Financial loss.
  - Personnel impact.
  - Opportunity loss.
  - Reputation loss.
  - Goodwill loss.
  - Market loss

RISK MANAGEMENT PROGRAM REVIEW

- Risk management programs are messy!
- They are never perfect and can become political battle points within an organization.
- Constraints typically get inserted into the risk decision process and can often be overstated.
- CISOs need a tough outer shell to accept program criticisms.
  - You WILL get pushback during risk communication and when you provide remediation counsel.
  - Find executive support throughout the organization in order to add pressure to reduce risk.
- Adopt a continuous improvement process to evolve the risk management program – engage with both supporters and antagonists.

RISK CONCLUSION

- A CISOs primary role is to reduce organizational IT risk to an acceptable level.
- Select the proper framework to manage risk.
  - Make sure it is readily understood
  - Modify as needed.
  - Try to choose a framework that best aligns to the organization.
- Understanding and effectively communicating organizational risk is critical to your program's success.
- Risk management, control selection, and continuous assessment are fundamental for protecting organizational assets.
- Risk treatment must be commensurate with the value of the assessed asset.

DOMAIN 1
END

DOMAIN 1 SUMMARY

DOMAIN 1: GENERAL

- This domain discussed the identification, reduction, and management of risk to an organization.
- Aligning an information security program to an organization's business model is crucial for effectiveness and adoption by the organization.
- The CISO is the voice of reason that helps an organization balance risk and reward to achieve business goals.
- The CISO must understand the weaknesses of an organization's technology infrastructure and act as the advisor to senior leadership.
- To promote a professional risk program, CISOs use a standardized and consistent risk assessment and scoring methodology.

DOMAIN 1: BUSINESS DRIVERS

- Information security programs are heavily influenced by business drivers.
- A business driver is a condition, process, requirement or other concern that influences the way in which an organization directs or manages activities.
- Key business drivers include organizational structure, industry, and maturity.
- It is difficult for a security program to evolve beyond the maturity of the organization it protects.
- IS programs need to achieve at least a maturity level of 3 before real improvements can be made.

DOMAIN 1: INFORMATION SECURITY DRIVERS

- Information security drivers are like business drivers because of their effect on the management and operation of the security program.
- Who a CISO reports to can heavily affect the success of the security program.
- Compliance requirements heavily affect the focus and investment in security programs.

DOMAIN 1: POLICIES

- CISOs can benefit greatly by adopting a pre-existing security framework.
- Developing security policies is one of the first program development steps.
- Policies should be tailored to the organization rather than copied from other organizations.
- Most industry regulations and standards require the development, dissemination, and acknowledgement of security policies.
- A security policy must be supported by the organization's senior management team to be successful.

DOMAIN 1: ETHICS

- Ethics defines the moral principles that govern the behavior of a person or group.
- Ethical behavior is crucial for the CISO.
    - CISO actions are closely scrutinized.
    - You will be judged on how you conduct business or direct activities within the organization.
- Follow the “would my parents be proud of me” rule when making an ethical-based decision.
- EC-Council Code of Ethics codifies the expectations for ethical behavior by CCISO certification holders.

DOMAIN 1: RISK MANAGEMENT

- Risk management is the identification, assessment, and prioritization of risks.
- Risk is a product of the impact that threats can have on vulnerabilities within the IT infrastructure and business processes.
- CISOs help define and communicate the organization's risk appetite and risk tolerance.
- CISOs do not own risk! Asset owners are responsible for risk within their systems and supported business processes.

DOMAIN 1: RISK MANAGEMENT - CONTINUED

- Quantitative risk assessments are based on numerical equations.
- Qualitative risk assessments use ranges or categories.
- Hybrid risk assessments are generally used.
- CISOs should understand the difference between inherent and treated risk.
- Residual risk is what is left after the application of risk treatment.

DOMAIN 1: RISK TREATMENT

- Once a risk is identified it must be addressed.
  - Risk modification or mitigation
  - Risk retention or acceptance
  - Risk sharing or transfer (insurance)
  - Risk avoidance or elimination
- Risk treatments are driven by constraints that typically include cost, time, and level of overall effort to remediate.

DOMAIN 1: CALCULATION FORMULAS

- Risk calculations have common aspects for scoring and ranking risk:
  - Asset Value (AV): The value or worth of an asset.
  - Exposure Factor (EF): The estimated percentage of damage or impact that a realized threat would have on the asset or organization.
  - Single Loss Expectancy (SLE): The projected loss of a single realized risk or event.
  - Annual Rate if Occurrence (ARO): Estimated number of times the risk would be realized within a calendar year.
  - Annualized Loss Expectancy (ALE): Projected loss to the business based on the asset value and annual rate of occurrence.

DOMAIN 1: RISK MANAGEMENT FRAMEWORKS

- The CISO should select the risk management framework or methodology that best supports the organization.
- Numerous frameworks exist to guide the processes of identifying, treating, and monitoring information security risks in an organization. They include:
  - Cybersecurity risk management frameworks.
  - Enterprise Risk Management (ERM) frameworks.
  - Risk assessment methodologies.
  - General risk management frameworks.

DOMAIN 1: RISK MANAGEMENT FRAMEWORKS - CONTINUED

- The most widely used risk frameworks include:
  - ISO/IEC 27005.
  - NIST SP 800-37.
  - Factor Analysis of Information Risk (FAIR)
- Second tier risk frameworks include:
  - COSO ERM Integrated Framework.
  - Threat Assessment and Remediation Analysis (TARA).
  - ISACA Risk IT Framework.

DOMAIN 1: RISK MANAGEMENT PROGRAM IMPLEMENTATION

- Example risk program implementation (ISO/IEC 27005):
  1. Identification of assets.
  2. Identification of threats.
  3. Identification of existing controls.
  4. Identifications of vulnerabilities.
  5. Identification of consequences.

DOMAIN 1: RISK MANAGEMENT LIFECYCLE

- Effective risk management includes an articulated lifecycle.
  1. Risk assessment.
  2. Risk registry entries.
  3. Risk treatment decisions.
  4. Risk acceptance.
  5. Risk monitoring.
  6. Risk reporting.

DOMAIN 1 PRACTICE QUESTIONS

PRACTICE QUESTIONS

1. What is the Annual Rate of Occurrence?

A. The times per year that an asset is evaluated for quantitative value purposes.

B. A qualitative measurement of annual events.

C. The number of times per year that a risk could be realized.

D. The impact of an event happening with a calendar year.

PRACTICE QUESTIONS

2. An organization recently implemented a risk management program to measure the risk of IT projects. Which of the following cases would this organization be **MORE** willing to accept vs. mitigate risk?

A. The organization uses a quantitative process to measure risk.

B. The organization uses a qualitative process to measure risk.

C. The organization's risk tolerance is high.

D. The organization's risk tolerance is low.

PRACTICE QUESTIONS

3. A global healthcare company is concerned about protecting confidential information.

Which of the following is of **MOST** concern to this organization?

A. Compliance to Payment Card Industry (PCI) Data Security Standard.

B. Compliance to privacy laws and regulations for each country where they operate.

C. Conformance to local employment laws for each country where they operate.

D. Alignment to International Organization for Standardization (ISO).

PRACTICE QUESTIONS

4. A retail company is working on defining a compliance management process.

Which of the following are **MOST** likely to be included?

A. Payment Card Industry Data Security Standards (PCI-DSS).

B. Information Technology Infrastructure Library (ITIL).

C. International Organization for Standardization (ISO) standards.

D. National Institute for Standards and Technology (NIST) standards.

PRACTICE QUESTIONS

5. To achieve effective strategic alignment of the Cybersecurity initiatives in an organization what should a CISO consider as most important ?

A. A steering committee is formed, and leadership alternates between members

B. Major business functions provide input and reach consensus.

C. Business strategy is updated periodically

D. Standards and procedures are approved by all business functions

C|CISO

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

DOMAIN 2

INTRODUCTION

This domain provides training on how to:

- Adopt an information security framework.
- Define and assign control attributes to deploy effective and efficient control schemas.
- Create an information security control catalog.
- Build an information security service catalog.
- Understand the most common information security regulations and statutes.
- Respond to an internal or external audit.

KNOWLEDGE ASSUMPTIONS

- Students are expected to have:
  - Five years of domain experience.
  - A familiarity of information security controls vocabulary.
  - A working knowledge of ISO 27001 or NIST 800-53 standards.
  - A working knowledge of the CIA triad.
  - An understanding of defense-in-depth concepts.
  - An understanding of information security compliance.
  - A working knowledge of one or more industry-specific regulations.
  - A basic understanding of auditing processes.

IS CONTROLS, COMPLIANCE, AND AUDIT MANAGEMENT

DOMAIN 2

INFORMATION SECURITY CONTROLS, COMPLIANCE, AND AUDIT MANAGEMENT

DOMAIN OUTLINE

1. Information Security Controls
2. Compliance Management
3. Guidelines, Good and Best Practices
4. Audit Management

Summary and Practice Questions

1. INFORMATION SECURITY CONTROLS

INFORMATION SECURITY CONTROLS

- A successful information security program relies on controls to protect information and assets from attack by external threat actors and insider threats.
- Controls may be automated or manual processes.
- These actions and technologies are used to prevent, detect, or correct malicious (or even accidental) activities against an organization.

IDENTIFYING THE ORGANIZATION'S INFORMATION SECURITY NEEDS

Identifying the organization's information security needs is critical for selecting the controls to protect your organization's information and assets.

This is part of that all-important alignment to the business and allows a higher probability of security program success.

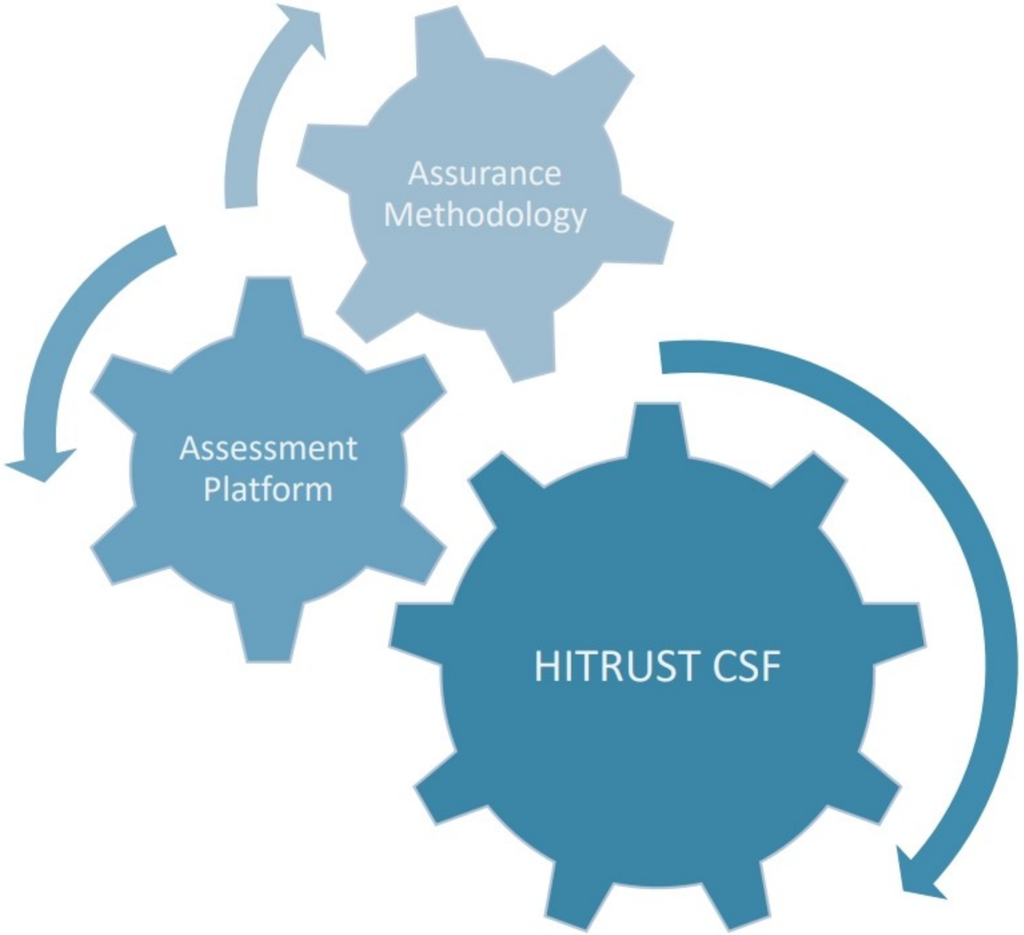
Controls should be reasonable, effective, and provide efficiency within resource constraints (money, time and people).

IDENTIFYING THE OPTIMUM INFORMATION SECURITY FRAMEWORK

- When reviewing cybersecurity frameworks and models, many popular frameworks originate from either ISO or NIST:
  - ISO/IEC 27001/27002 Information Security Management System (ISMS).
  - NIST SP 800-37 Cybersecurity Framework.
- Both frameworks are mature, well-documented, and referenced by a variety of regulations, standards, and IT frameworks:
  - Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).
  - Information Security Forum Framework (ISF).
  - Information Technology Infrastructure Library (ITIL).

HEALTH INFORMATION TRUST ALLIANCE (HITRUST) COMMON SECURITY FRAMEWORK (CSF)

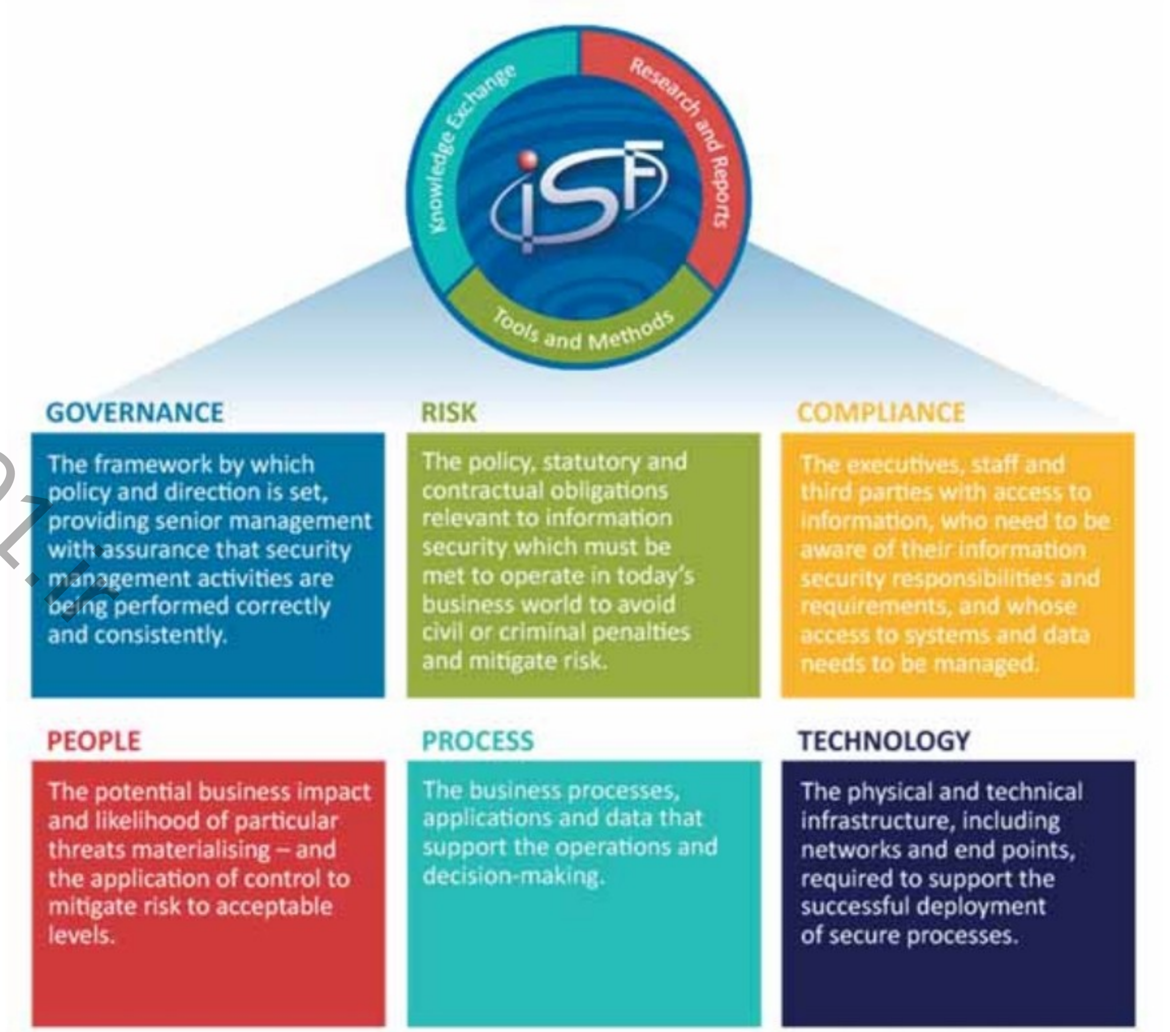
- The HITRUST CSF is a comprehensive cybersecurity and privacy framework originally intended for healthcare organizations.
- HITRUST CSF has been the most widely-adopted security framework in the US healthcare industry since 2010.
- Thirty-five standards are used within the framework.



HITRUST Framework

INFORMATION SECURITY FORUM (ISF) FRAMEWORK

- Independent, not-for-profit association founded in 1989.
- Based on ISO/IEC 27001.
- Each control consists of up to 3 levels of implementation.
- Focused on audit and risk management, BCP, change management, operational monitoring, and trusted access.



GOVERNANCE

The framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently.

RISK

The policy, statutory and contractual obligations relevant to information security which must be met to operate in today's business world to avoid civil or criminal penalties and mitigate risk.

COMPLIANCE

The executives, staff and third parties with access to information, who need to be aware of their information security responsibilities and requirements, and whose access to systems and data needs to be managed.

PEOPLE

The potential business impact and likelihood of particular threats materialising – and the application of control to mitigate risk to acceptable levels.

PROCESS

The business processes, applications and data that support the operations and decision-making.

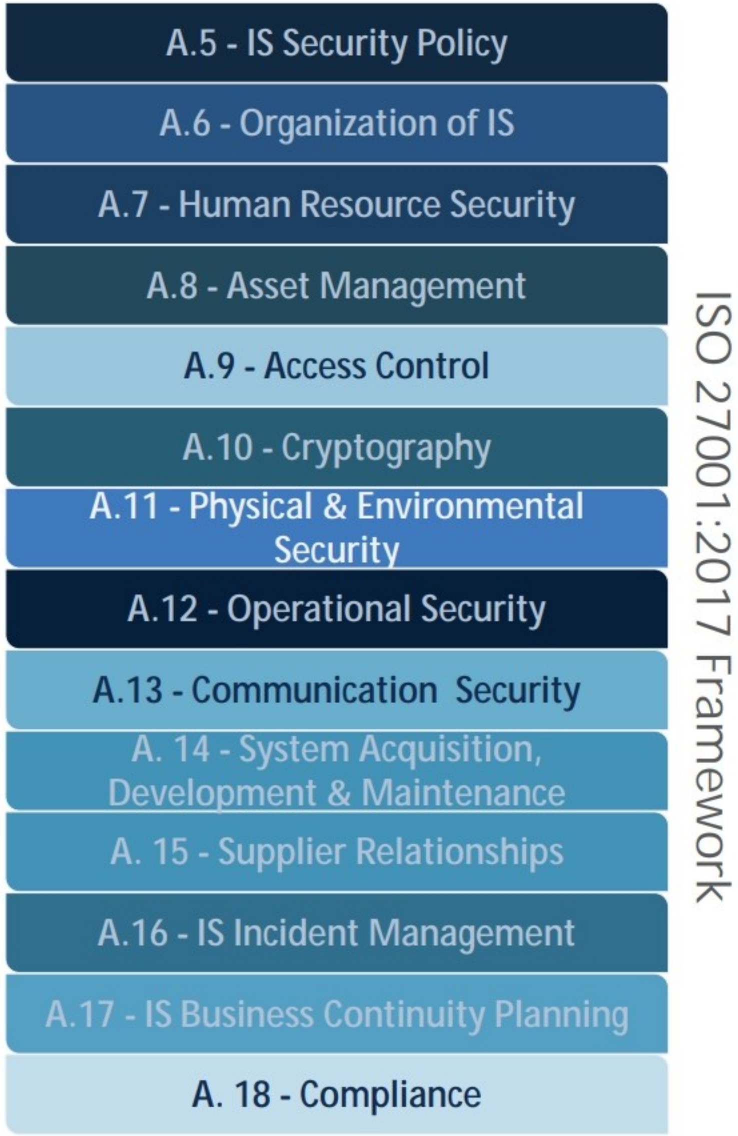
TECHNOLOGY

The physical and technical infrastructure, including networks and end points, required to support the successful deployment of secure processes.

Source: International Security Forum

ISO/IEC 27001/27002 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

- A global information security standard, part of the ISO/IEC 27000 family of standards.
- Contains fourteen clauses and 114 controls.
- Allows for certification within the standard.
- Supported by ISO/IEC 27002.
- Applies to all industries, technologies, or operations.
- ISO/IEC information is copyrighted.
- There is a cost for using the standard.



A.5 - IS Security Policy

A.6 - Organization of IS

A.7 - Human Resource Security

A.8 - Asset Management

A.9 - Access Control

A.10 - Cryptography

A.11 - Physical & Environmental Security

A.12 - Operational Security

A.13 - Communication Security

A. 14 - System Acquisition, Development & Maintenance

A. 15 - Supplier Relationships

A.16 - IS Incident Management

A.17 - IS Business Continuity Planning

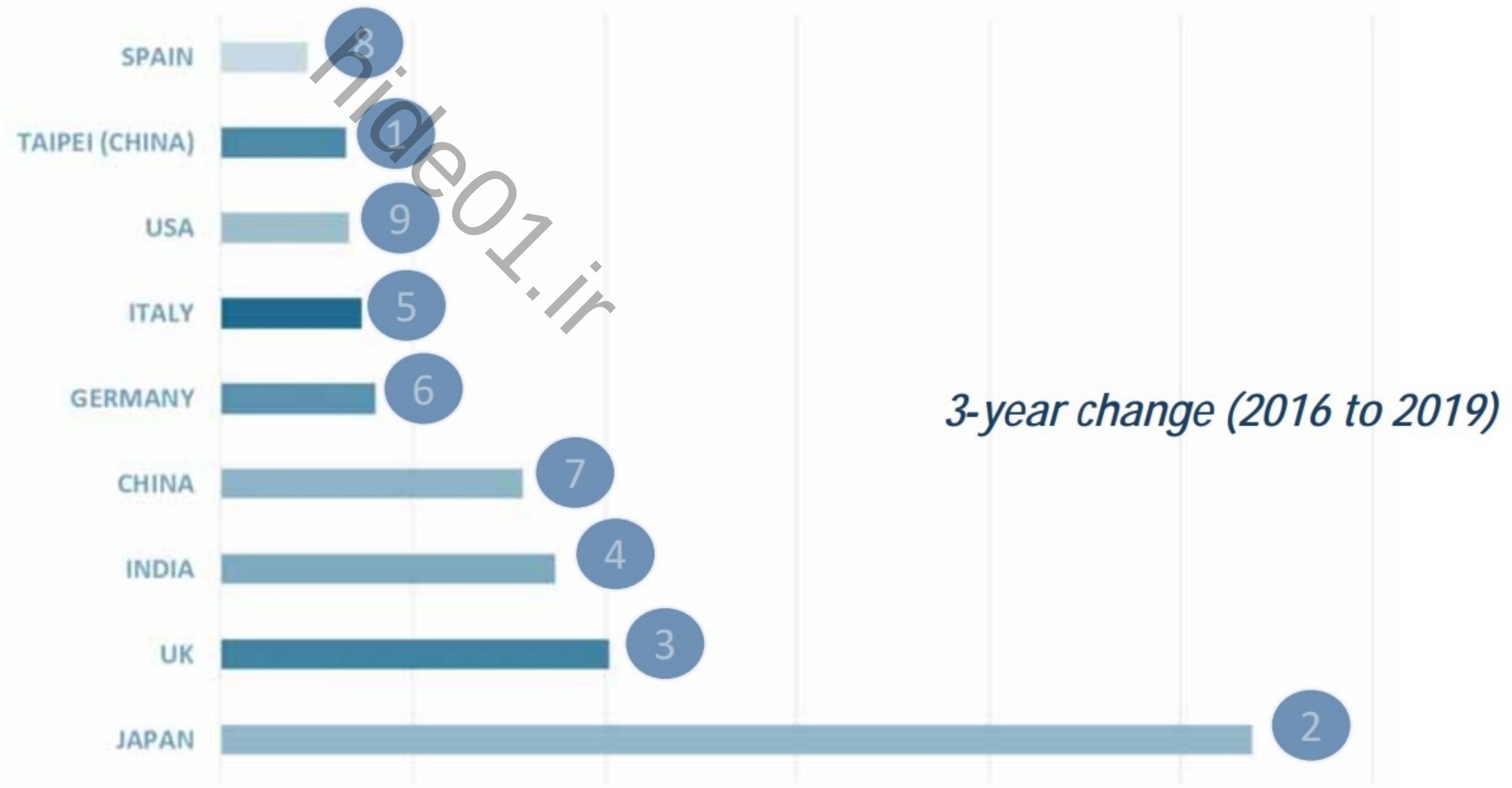
A. 18 - Compliance

ISO 27001:2017 Framework

ISO/IEC 27001/27002 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

ISO (IEC) standards 27001 and 27002 are widely seen as the primary international information security standards.

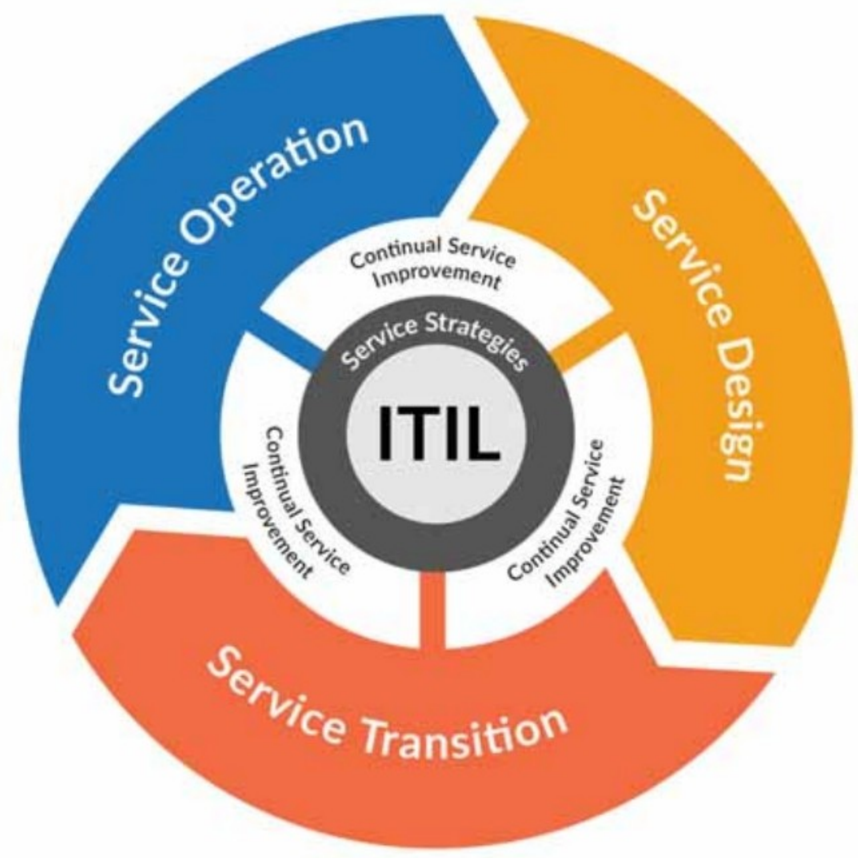
Top 10 ISO 27001 certifications by country.



3-year change (2016 to 2019)

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

- Ideally suited for operationalization of information security solutions.
- Provides a service management framework for the information security portfolio.
- ISO 27001 was adopted for security process.


Service Operation
Service Design
Service Transition
Continual Service Improvement
Continual Service Improvement
Continual Service Improvement
Service Strategies
ITIL

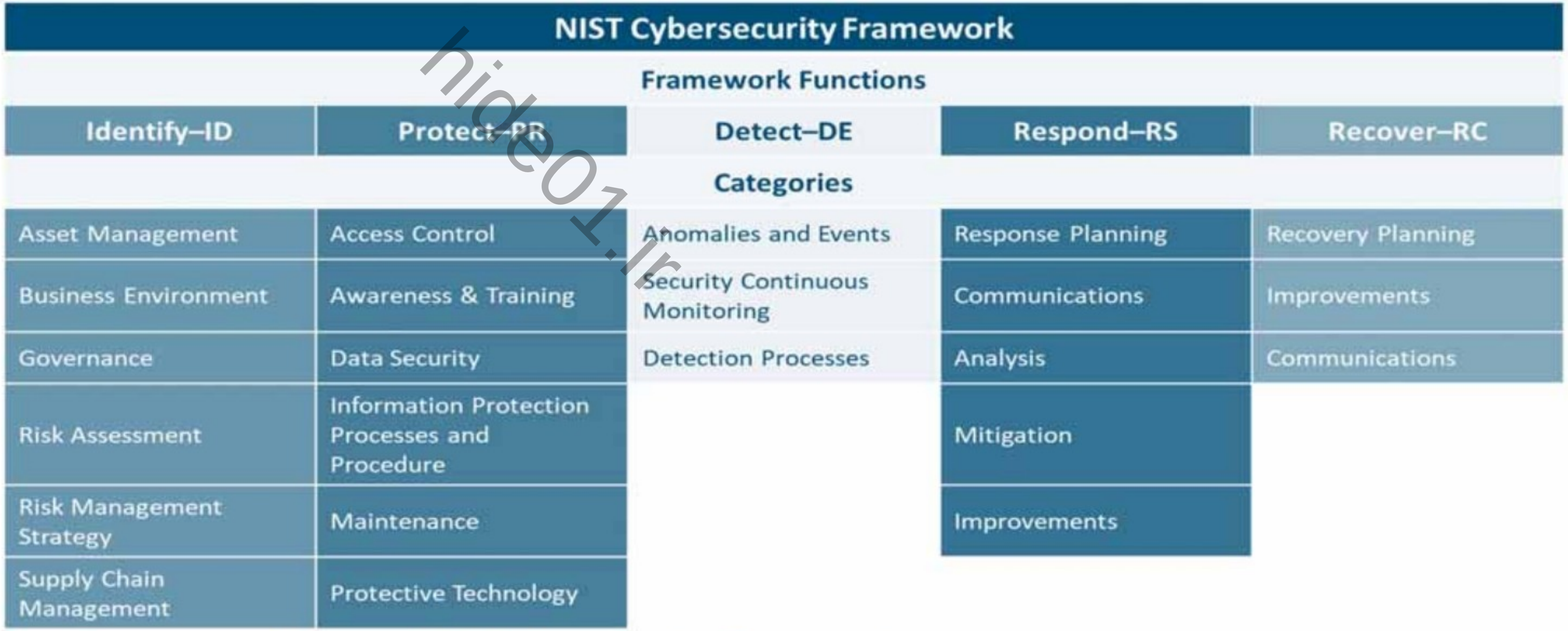
Source: ITIL v3 - Helpsystems

NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework (CSF) originates from Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued February 12, 2013 (Executive Order, 2013).

CSF IS COMPRISED OF THREE PARTS:

1. Framework Core
2. Framework Profile
3. Framework Implementation Tiers



NIST Cybersecurity Framework

Framework Functions

Identify–ID	Protect–PR	Detect–DE	Respond–RS	Recover–RC
Categories				
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedure		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Management	Protective Technology			

Figure : NIST Cybersecurity Framework

DESIGNING SECURITY CONTROLS

- Designing an IS control requires a balance between effectiveness and cost.
- Part of the design process includes mapping controls to standards and regulations.
- CISOs should have strong understanding of available controls and the corresponding control objectives.
- Controls mitigate risk or achieve compliance and have three attributes:
  1) What the control is.
  2) What the control does.
  3) How the control performs its objective.

DESIGNING SECURITY CONTROLS

- Manual Controls
  - Require human intervention to perform the control.
  - Examples include activities such as checking badges for authorized entry or manually reviewing audit logs.
  - Manual controls are important, but they are subject to human error.
  - Can inadvertently enable forgetfulness, negligence, or misunderstanding processes or requirements.

DESIGNING SECURITY CONTROLS

Automated Controls

- Apply logical intervention using technology to perform the control.
- Many logical controls exist as automated controls because they perform without human interaction.
- Automated controls are preferred because of the accuracy, speed, and scalability with which they perform.
- Automated controls are not infallible - they require proper configuration and monitoring to assure maximum effectiveness.

CONTROL LIFECYCLE MANAGEMENT

Controls are assets to an information security program. Like any asset, they should be managed based on their lifecycle.

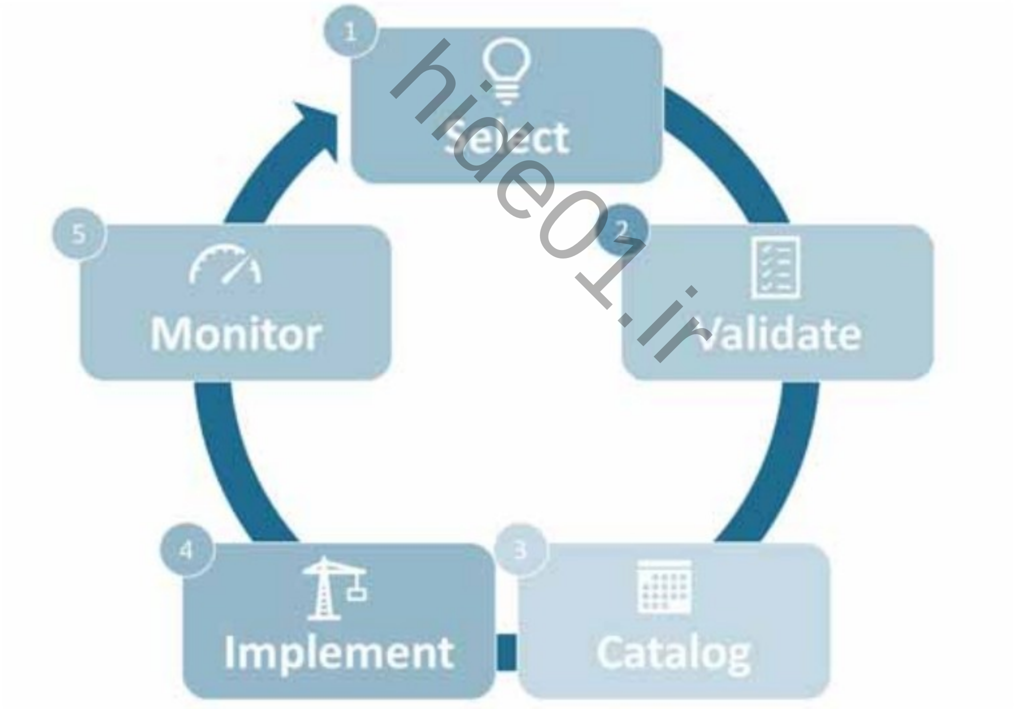


Figure: Control Lifecycle Management

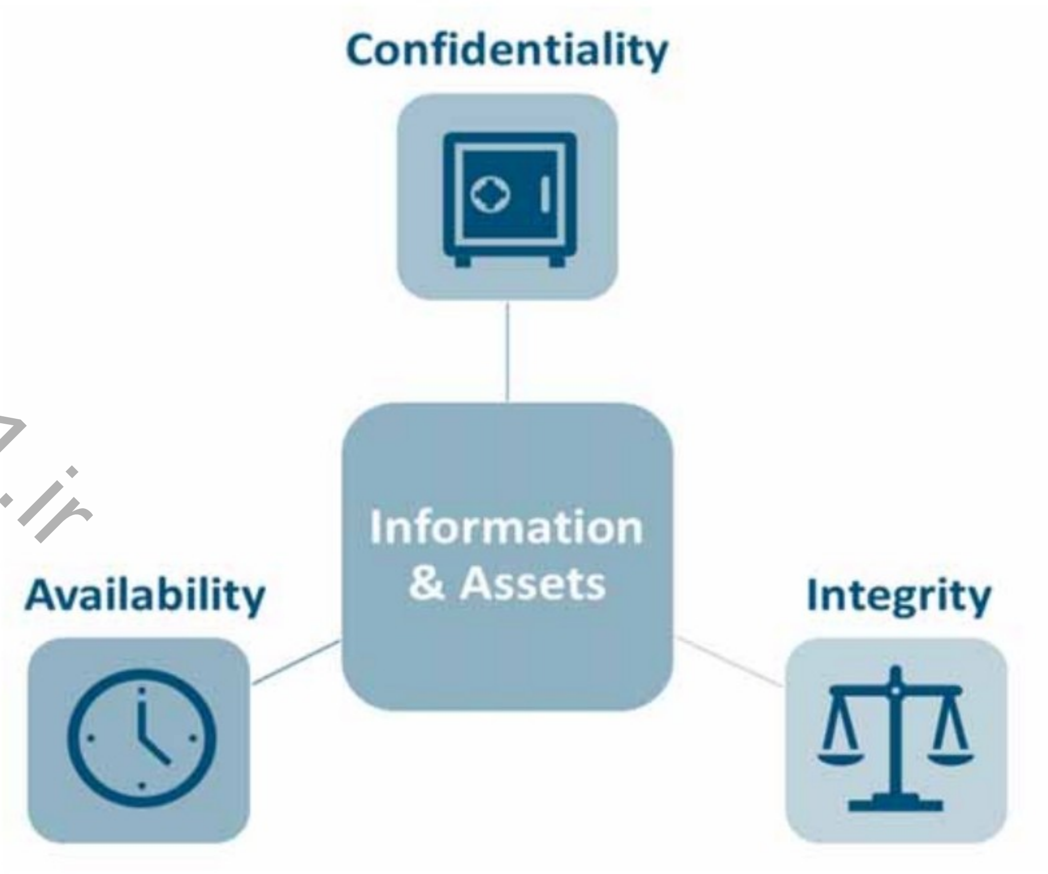
CONTROL CLASSIFICATION

- Control classification allows a CISO to select a control for a specific purpose.
- Classification examples include:
  - Protection of information and assets.
  - Compliance with legal or regulatory requirements.
  - Supporting security tenets.

Control Classification Schema Examples
CIA Triad. COSO PDC Defense-in-Depth Model. NIST Security Control Classes. NIST Minimum Security Controls.

CIA TRIAD

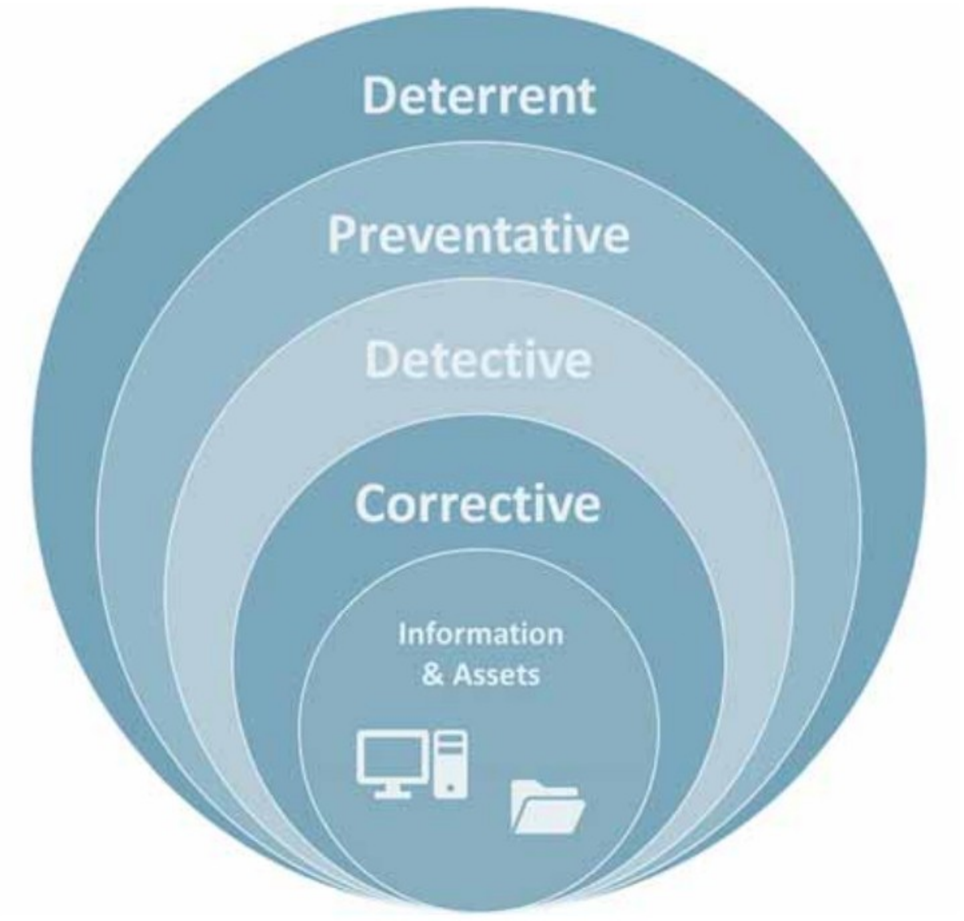
- The CIA Triad formed over time as wisdom passed among information security professionals rather than by a single proponent.
- The formalization of confidentiality can be traced back to a 1976 U.S. Air Force study.
- Represents the 3 primary tenets of information protection.



CIA Triad Model

COSO DEFENSE-IN-DEPTH MODEL

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework defines internal control as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance.



COSO Defense-in-Depth Model

COSO DEFENSE-IN-DEPTH MODEL

4 Types of Controls

- **Preventive Controls** protect the organization by precluding a threat from exploiting a vulnerability. This type of control proactively prevents a risk from being manifested.
- **Detective Controls** form the second line of defense. Detective controls identify the existence of anomalous or improper activity.
- **Corrective Controls** modify an environment and take action to restore the environment to its correct operating state.
- **Deterrent Controls** discourage the exploitation of a vulnerability or system.

NIST SECURITY CONTROL CLASSES

- NIST Special Publication 800-53-R5 provides guidance for Information Security Program Assessments and Reporting Form, described three classes of security control types:
  - Management.
  - Operational.
  - Technical.

Management Controls	Operational Controls	Technical Controls
(CA) Security Assessment and Authorization	(AT) Awareness and Training	(AC) Access Control
(PL) Planning	(CM) Configuration Management	(AU) Audit and Accountability
(RA) Risk Assessment	(CP) Contingency Planning	(IA) Identification and Authorization
(SA) System and Service Acquisition	(IR) Incident Response	(SC) System and Communications Protection
(PM) Program Management	(MA) Maintenance	
	(MP) Media Protection	
	(PE) Physical and Environmental Security	
	(PS) Personnel Security	
	(SI) System and Information Integrity	

Table: NIST Security Controls Classes Chart

NIST SECURITY CONTROL CLASSES

Control Classes		
Management or Administrative Control	Operations or Physical Control	Technical or Logical Controls
Designed to address the management of risk and information security.	Designed to be implemented and executed by people.	Designed to be executed by systems (hardware, software, firmware).

NIST MINIMUM SECURITY CONTROLS

To assist organizations in making the selection of security controls for their information systems, NIST introduced the concept of applying baseline controls based on criticality.

- **High-impact baseline** - severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate-impact baseline** - serious adverse effects could include significant operational damage to assets, financial loss, or individual harm that is not loss of life or physical.
- **Low-impact baseline** - limited adverse effects of confidentiality, integrity, and availability.

CONTROL SELECTION AND IMPLEMENTATION

- CISOs should consider the entire cost of controls in terms of the three critical resources – people, time and money.
- Expenditure analysis includes lifecycle costs throughout acquisition, implementation, maintenance, operational support, and monitoring.
- A common approach for selecting and implementing controls is to follow trends set by similar organizations (also known as best practices).

CONTROL SELECTION AND CLASSIFICATION

Types of Controls

- **Key Controls** are high-impact baseline control that mitigate significant risk for an organization.

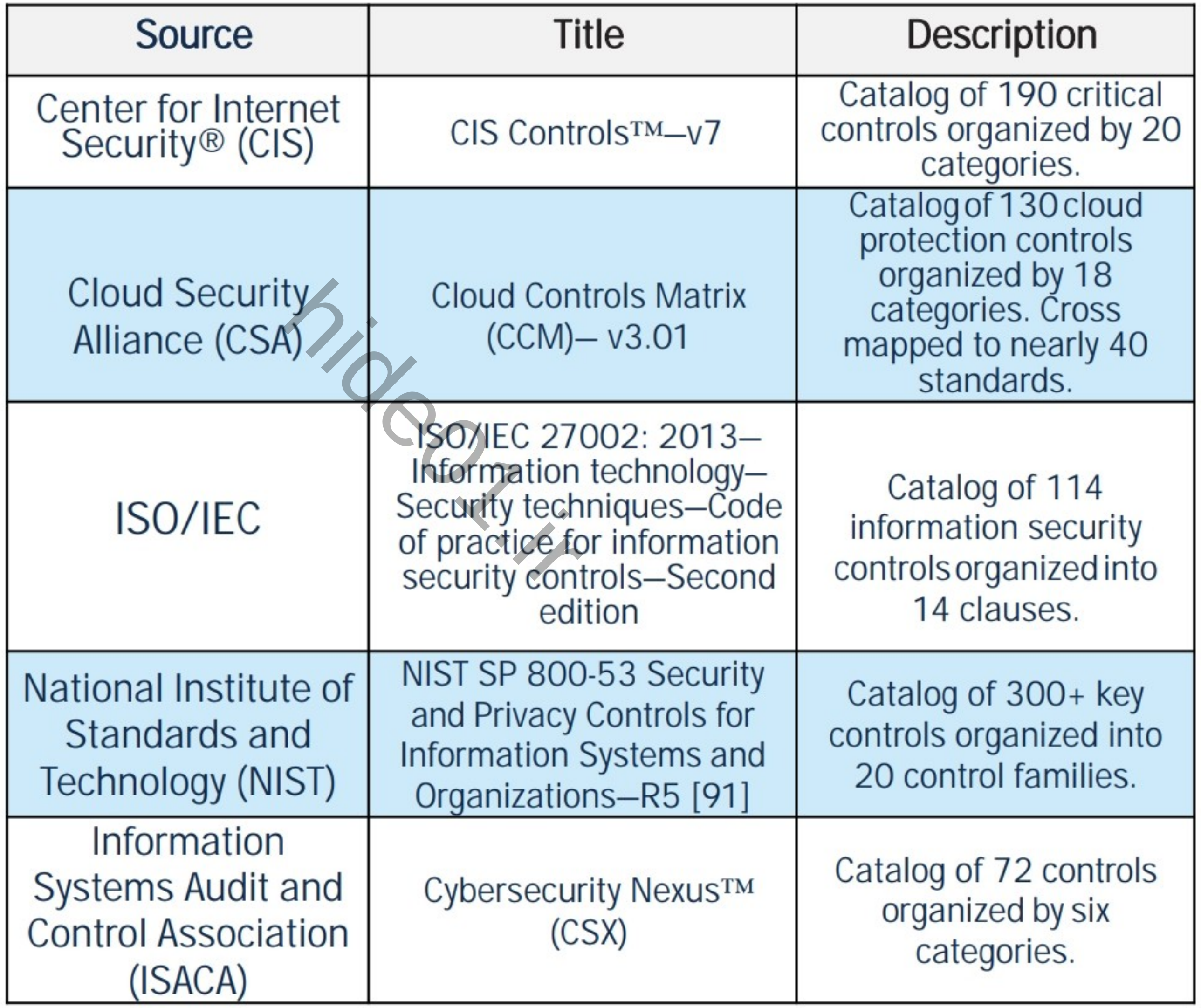
- **Compensating Controls** are used when the recommended approach to implement a control is too expensive, too impractical, or too difficult.

CONTROL CATALOG

- Control catalogs are used to identify the family or category of controls and the objective of each control.
- Catalogs provide guidance or recommendations for implementing controls.
- The two dominant catalogs of information security controls are:
  - ISO 27002.
  - NIST SP 800-53.

CONTROL CATALOGS: SOURCES

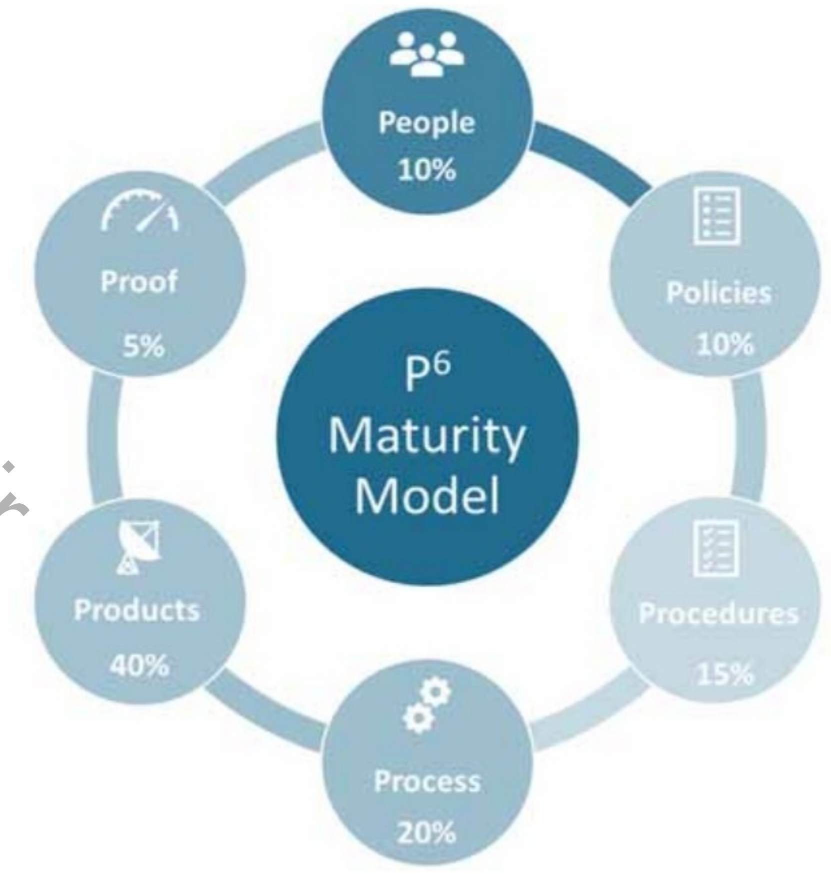
Information Security Control Catalog Sources



Source	Title	Description
Center for Internet Security® (CIS)	CIS Controls™—v7	Catalog of 190 critical controls organized by 20 categories.
Cloud Security Alliance (CSA)	Cloud Controls Matrix (CCM)– v3.01	Catalog of 130 cloud protection controls organized by 18 categories. Cross mapped to nearly 40 standards.
ISO/IEC	ISO/IEC 27002: 2013—Information technology—Security techniques—Code of practice for information security controls—Second edition	Catalog of 114 information security controls organized into 14 clauses.
National Institute of Standards and Technology (NIST)	NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations—R5 [91]	Catalog of 300+ key controls organized into 20 control families.
Information Systems Audit and Control Association (ISACA)	Cybersecurity Nexus™ (CSX)	Catalog of 72 controls organized by six categories.

CONTROL MATURITY

The maturity of an information security control can be evaluated according to the number of properties associated with the control that has been deployed.



P6 Control Maturity Model

MONITORING SECURITY CONTROLS

- Once controls have been identified, categorized, and cataloged they need to be monitored.
- Monitoring consists of reviews:
  - Include date and time.
  - Changes since last review.
  - Control mapping changes.
  - Control changes.

REMEDIATING CONTROL DEFICIENCIES

- Ineffective and missing controls can expose an organization to more risk than expected because of a false sense of security.
- Never assume controls exist and are effective without verifying them.
- When applying controls there are two primary methods to prioritize the program of work:
    - According to potential risk impact.
    - According to what can most easily be accomplished.

MAINTAINING SECURITY CONTROLS

- Properly managing controls within their lifecycle requires the inclusion of change management processes.
- Each time a control property or attribute is added, changed, or deleted, it should be tracked and documented by a change control process.
- Consider using version numbers for controls for historical information.

REPORTING CONTROLS

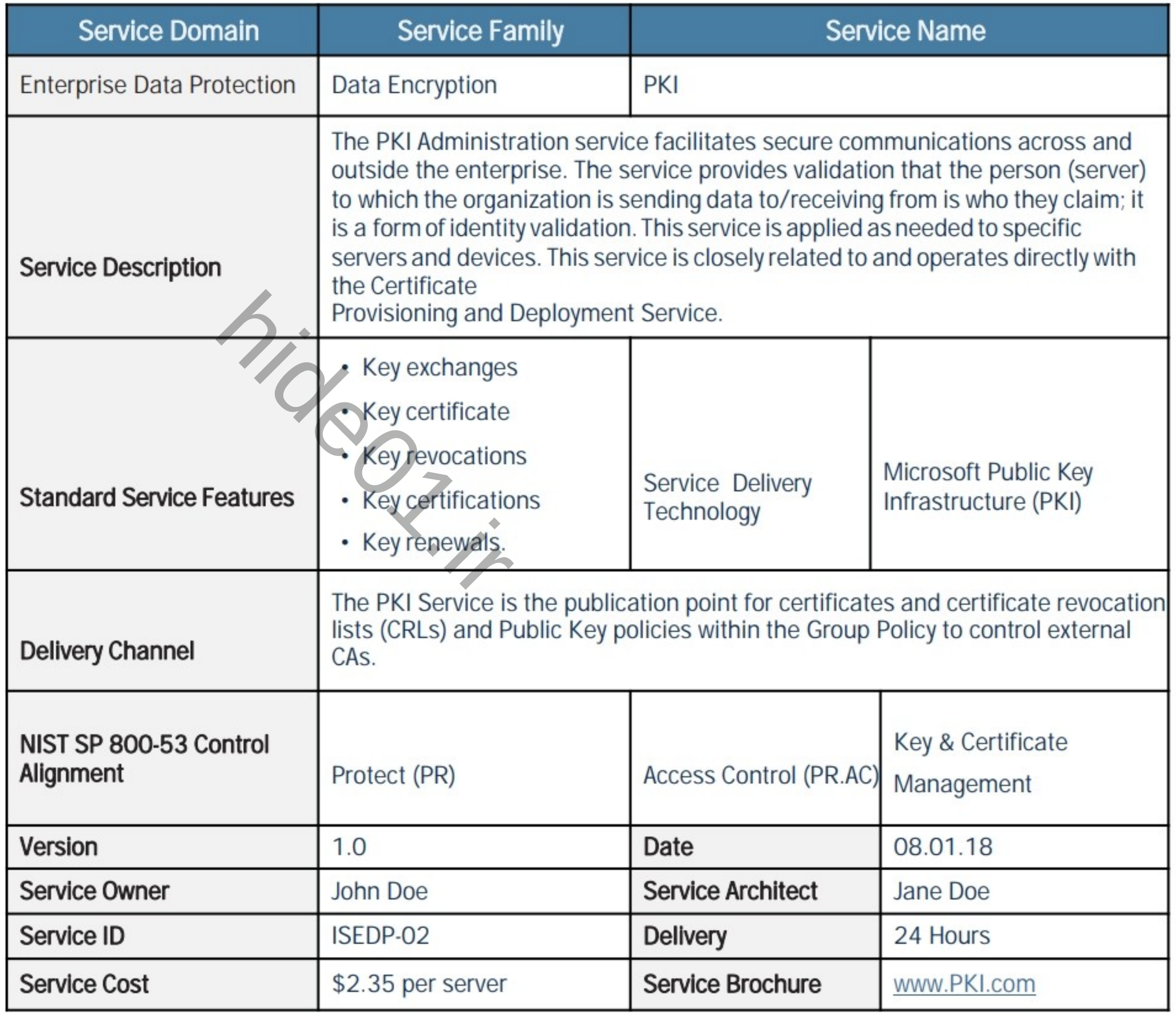
- Control reports should be prepared and provided to the asset owners:
  - On an annual basis.
  - To reemphasize the controls for which they are accountable.
  - To have them verify the controls are still valid and current.
- The control catalogue can be used for creating compliance reports.
- CISOs often assign a resource as manager of the control library to monitor and report on the state of security controls.

INFORMATION SECURITY SERVICE CATALOG

- A service catalog is an organized repository of security services available to the organization.
- Services can be:
  - Repaid through chargeback to a business unit.
  - Budgeted as value-add to departments or business units within the organization.
  - Considered an overall support cost to the organization.
- This depends on the operational financial model within the organization.

INFORMATION SECURITY SERVICE CATALOG

Service Catalog Example

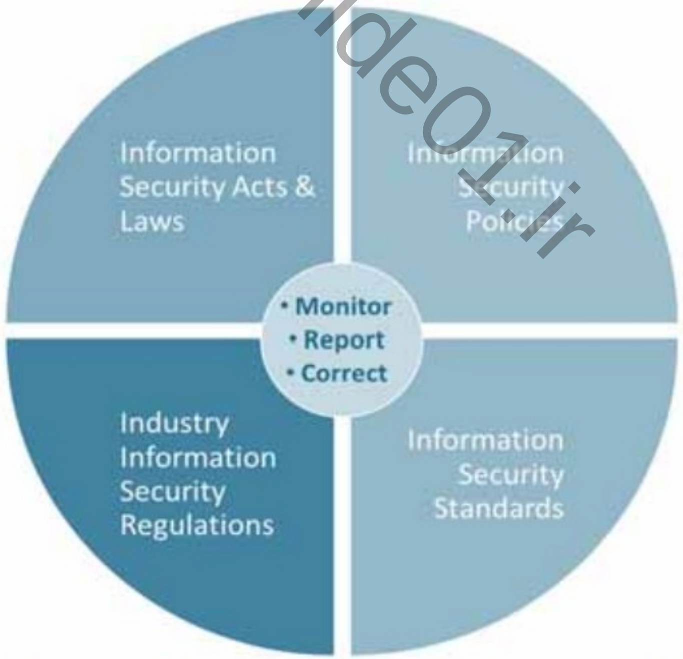


Service Domain	Service Family	Service Name	
Enterprise Data Protection	Data Encryption	PKI	
Service Description	The PKI Administration service facilitates secure communications across and outside the enterprise. The service provides validation that the person (server) to which the organization is sending data to/receiving from is who they claim; it is a form of identity validation. This service is applied as needed to specific servers and devices. This service is closely related to and operates directly with the Certificate Provisioning and Deployment Service.		
Standard Service Features	• Key exchanges • Key certificate • Key revocations • Key certifications • Key renewals.	Service Delivery Technology	Microsoft Public Key Infrastructure (PKI)
Delivery Channel	The PKI Service is the publication point for certificates and certificate revocation lists (CRLs) and Public Key policies within the Group Policy to control external CAs.		
NIST SP 800-53 Control Alignment	Protect (PR)	Access Control (PR.AC)	Key & Certificate Management
Version	1.0	**Date**	08.01.18
Service Owner	John Doe	**Service Architect**	Jane Doe
Service ID	ISEDP-02	**Delivery**	24 Hours
Service Cost	$2.35 per server	**Service Brochure**	www.PKI.com

2. COMPLIANCE MANAGEMENT

COMPLIANCE MANAGEMENT

Compliance management defines how an organization adheres to legal and regulatory requirements. This function monitors and reports on the organizational alignment to applicable laws, regulations, or standards.



Information Security Acts & Laws
Information Security Policies
• Monitor
• Report
• Correct
Industry Information Security Regulations
Information Security Standards

Compliance Management Reference Model

COMPLIANCE MANAGEMENT

Legally or Regulatorily Binding

Acts	Executive Orders	Laws	Regulations	Statutes	Presidential Policy Directive
The Health Insurance Portability and Accountability Act (HIPAA)	Executive Order 13587– Structural Reforms to Improve the Security	State Breach Notification Laws	General Data Protection Regulation (GDPR)	Computer Fraud and Abuse Act (CFAA)	Presidential Policy Directive 21 (PDD-21) (TVA)

Voluntary or Self Enforcing

Frameworks	Guidelines	Standards	Regulations	Presidential Policy Directive
NIST Cybersecurity Framework (CSF)	Open Web Application Security Project (OWASP)	Payment Card Industry Data Security Standard (PCI DSS)	General Data Protection Regulation (GDPR)	Presidential Policy Directive 21 (PDD-21) (Industry)

Compliance Matrix

ACTS, LAWS, AND STATUTES

- Acts are typically passed by legislative bodies on their way to becoming laws.
- Statutes are also passed by a legislative body and are similar to acts.
- Laws are sets of rules and regulations that are enforced by a government.

ACTS: EXAMPLES

- California Consumer Privacy Act (CCPA).
- The Cybersecurity Information Sharing Act (CISA).
- The Cybersecurity Enhancement Act of 2014.
- National Cybersecurity Protection Advancement Act of 2015.
- Cybersecurity and Infrastructure Security Agency Act of 2018.
- New York Stop Hacks and Improve Electronic Data Security Act (SHIELD).

THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

FISMA standardizes the process for risk management and information security practices for all federal agencies and contractors.

- Important FISMA features:
  - Periodic risk assessments.
  - Policies and procedures based on assessments.
  - Quantitative risk rating—data-driven security model.
  - Subordinate plans for information security for networks, facilities, and other sub- systems.
  - Security awareness training for personnel.
  - Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls at least annually.
  - A process to address deficiencies in information security policies (plan of action and milestones—POAM).
  - Procedures for detecting, reporting, and responding to security incidents.
  - Procedures and plans to ensure continuity of operations for information systems that support the organization's operations and assets.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Consists of 2 Primary Rules

The **Privacy Rule** provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

The **Security Rule** specifies administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

Primary HITECH Features

- Provides requirements concerning privacy and security for Patient Health Information (PHI).
- Expands the scope of privacy and security protections available under HIPAA.
- Increases the potential legal liability for noncompliance and expands enforcement.
  - Increased civil penalties for willful neglect.
- Requires data breach notification for unauthorized uses and disclosures of unsecured PHI.
- Creates stronger individual rights to access electronic medical records and restrict the disclosure of certain information.

REGULATIONS

- Regulations are rules or directives that are created, maintained, and in many cases enforced by a central authority.
- They are usually written by government entities.
- Top cybersecurity regulations include:
  - EU General Data Protection Regulation (GDPR).
  - New York's Cybersecurity Regulation (23 NYCR Part 500).
  - Privacy of Consumer Financial Information (Regulation S-P).

GENERAL DATA PROTECTION REGULATION (GDPR)

Scope:

- Replaced EU Data Protection Directive 95/46/etc.
- Applies to all companies processing the personal data of data subjects residing in the European Union, regardless of the company's location.
- Applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.

Penalties (Article 79):

- Fines up to 4% of annual global turnover or €20 Million (whichever is greater).
- Fines of 2% for not having records in order, not notifying the supervising authority and data subject about a breach or not conducting impact assessment.

GDPR - CONTINUED

Critical articles with GDPR include:

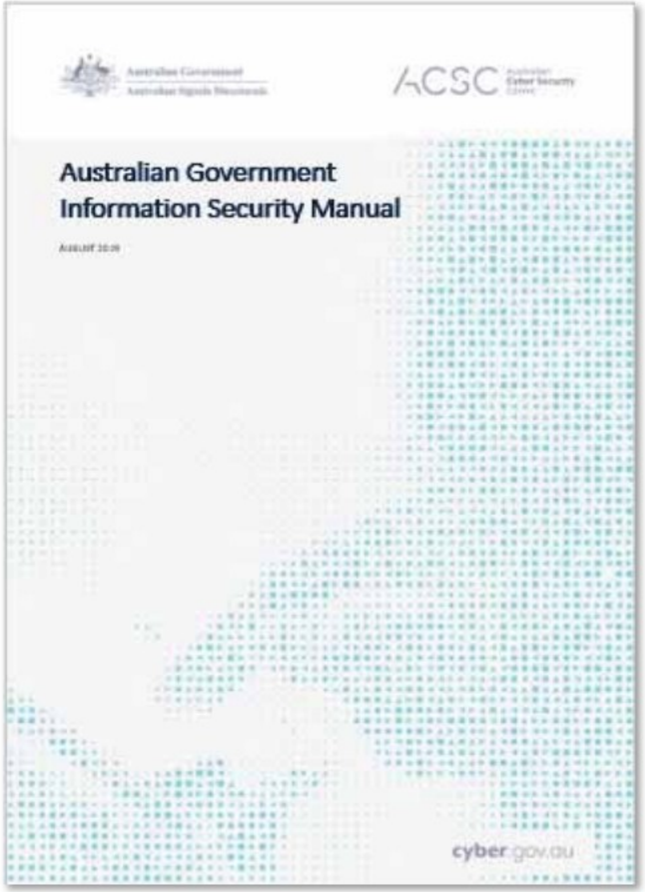
- 17 & 18: Right to portability and right to erasure.
- 23 & 30: Implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure.
- 31 & 32: Data breach notifications.
- 33 & 33a: Perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.
- 35: Appoint data protection officers.
- 36 & 37: Outline the data protection officer position and its responsibilities in ensuring GDPR compliance.

STANDARDS

- A standard is a measurement or metric agreed upon by the group or participants.
- Examples include:
  - Basel III.
  - FFIEC.
  - ISO 27000 Family of Standards.
  - NERC-CIP.
  - PCI DSS.
  - NIST Special Publications.
  - Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

ASD – INFORMATION SECURITY MANUAL

- The Australian Signals Directorate (ASD) produces the Australian Government Information Security Manual (ISM).
  - Outlines a cyber security framework using a risk management framework.
  - The ISM comprises three documents targeting different levels of the organization:
    - 22 cybersecurity guidelines.
    - 800+ cybersecurity controls.
    - Supporting materials.
    - Cybersecurity principles.



Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

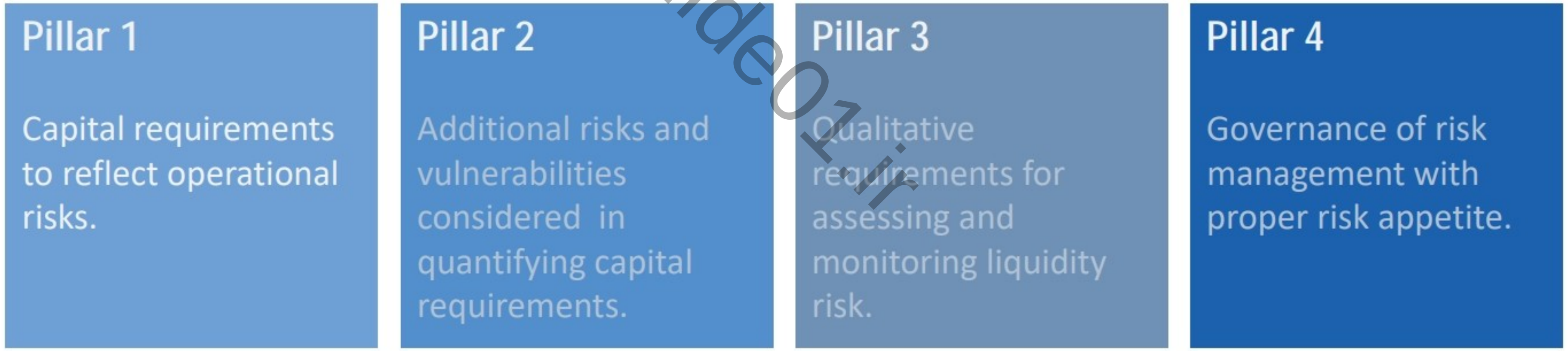
Australian Government Information Security Manual

August 2020

cyber.gov.au

BASEL III

Basel III (the Third Basel Accord) is a global, voluntary regulatory framework focused on bank capital adequacy, stress testing, and market liquidity risk.



Pillar 1

Capital requirements to reflect operational risks.

Pillar 2

Additional risks and vulnerabilities considered in quantifying capital requirements.

Pillar 3

Qualitative requirements for assessing and monitoring liquidity risk.

Pillar 4

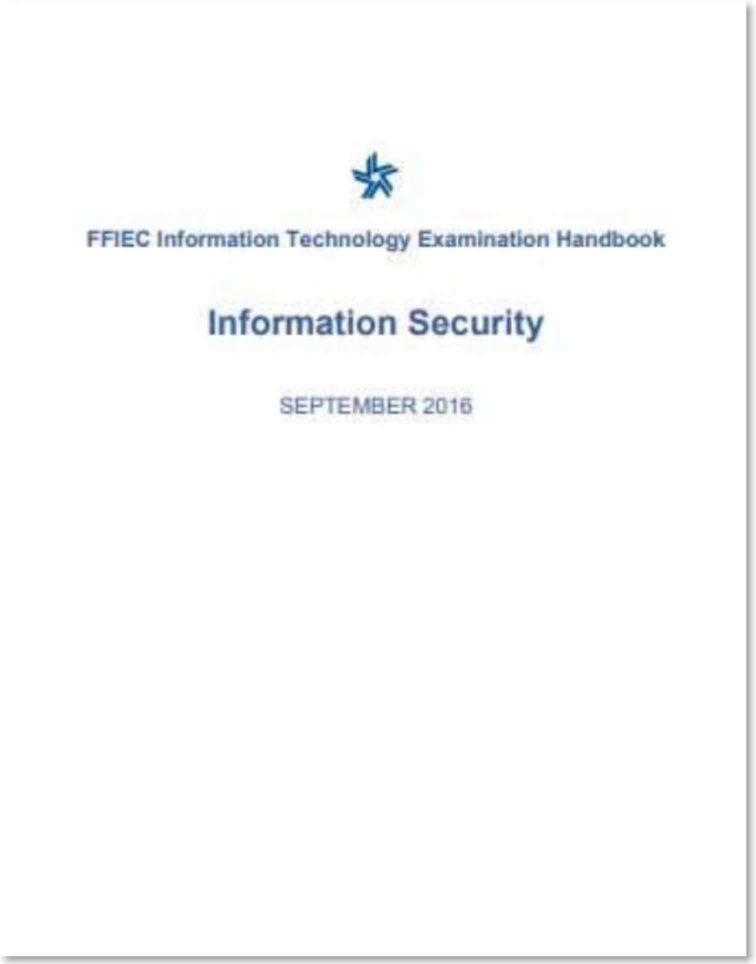
Governance of risk management with proper risk appetite.

Basel III Pillars

Requires the development, implementation and maintenance of enhanced data information technology to accurately assess and aggregate a variety of potential financial, legal and other operational risks.

THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC)

- The FFIEC is a U.S. government interagency body composed of five banking regulators empowered to prescribe uniform principles and standards.
- It directs user to the cybersecurity resource portal.
- It includes a Cybersecurity Assessment Tool (CAT).
- It is also referred to as The FFIEC Information Security Booklet.
- It provides auditor guidelines for assessing financial institution cybersecurity readiness.



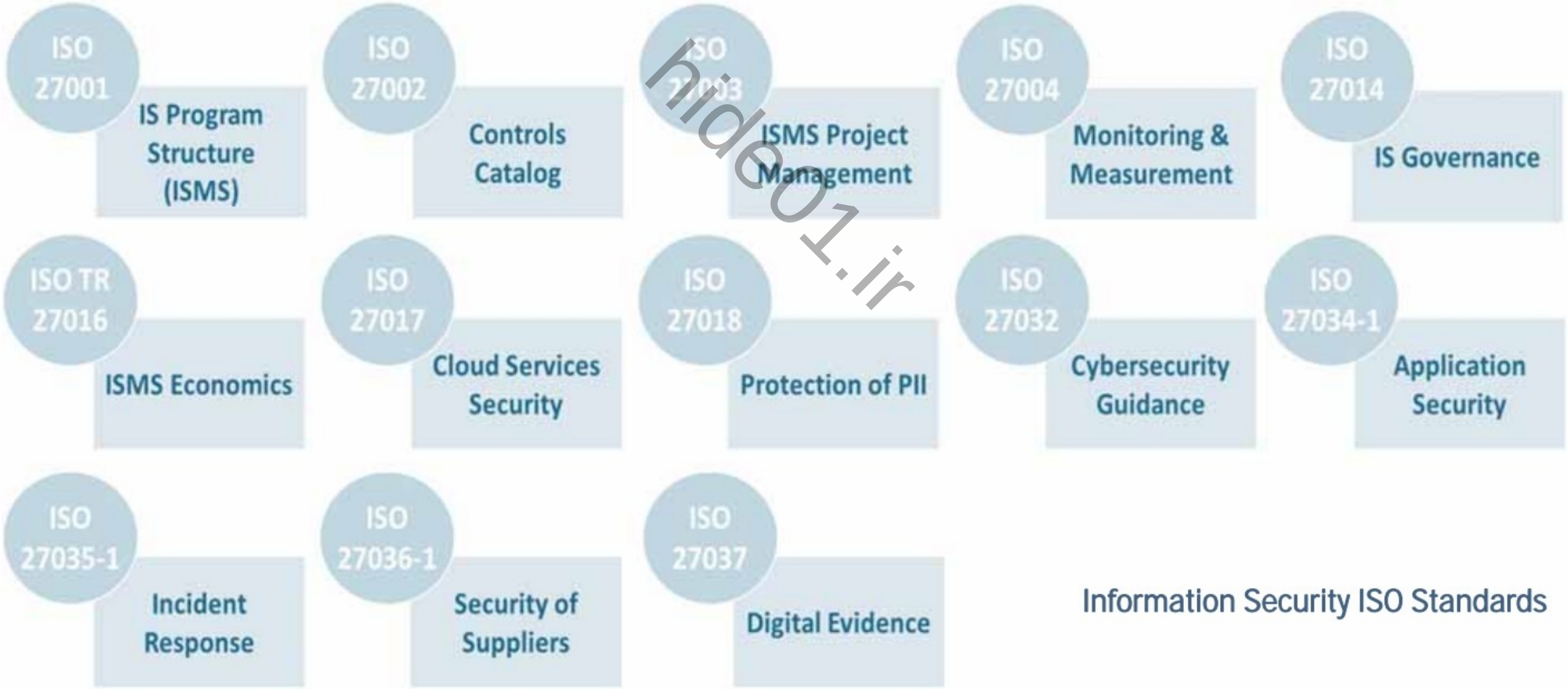
FFIEC Information Technology Examination Handbook

Information Security

SEPTEMBER 2016

ISO 2700 FAMILY OF STANDARDS

One of the most commonly information security standards is published by the International Organization for Standardization (ISO).



ISO 27001 IS Program Structure (ISMS)

ISO 27002 Controls Catalog

ISO 27003 ISMS Project Management

ISO 27004 Monitoring & Measurement

ISO 27014 IS Governance

ISO TR 27016 ISMS Economics

ISO 27017 Cloud Services Security

ISO 27018 Protection of PII

ISO 27032 Cybersecurity Guidance

ISO 27034-1 Application Security

ISO 27035-1 Incident Response

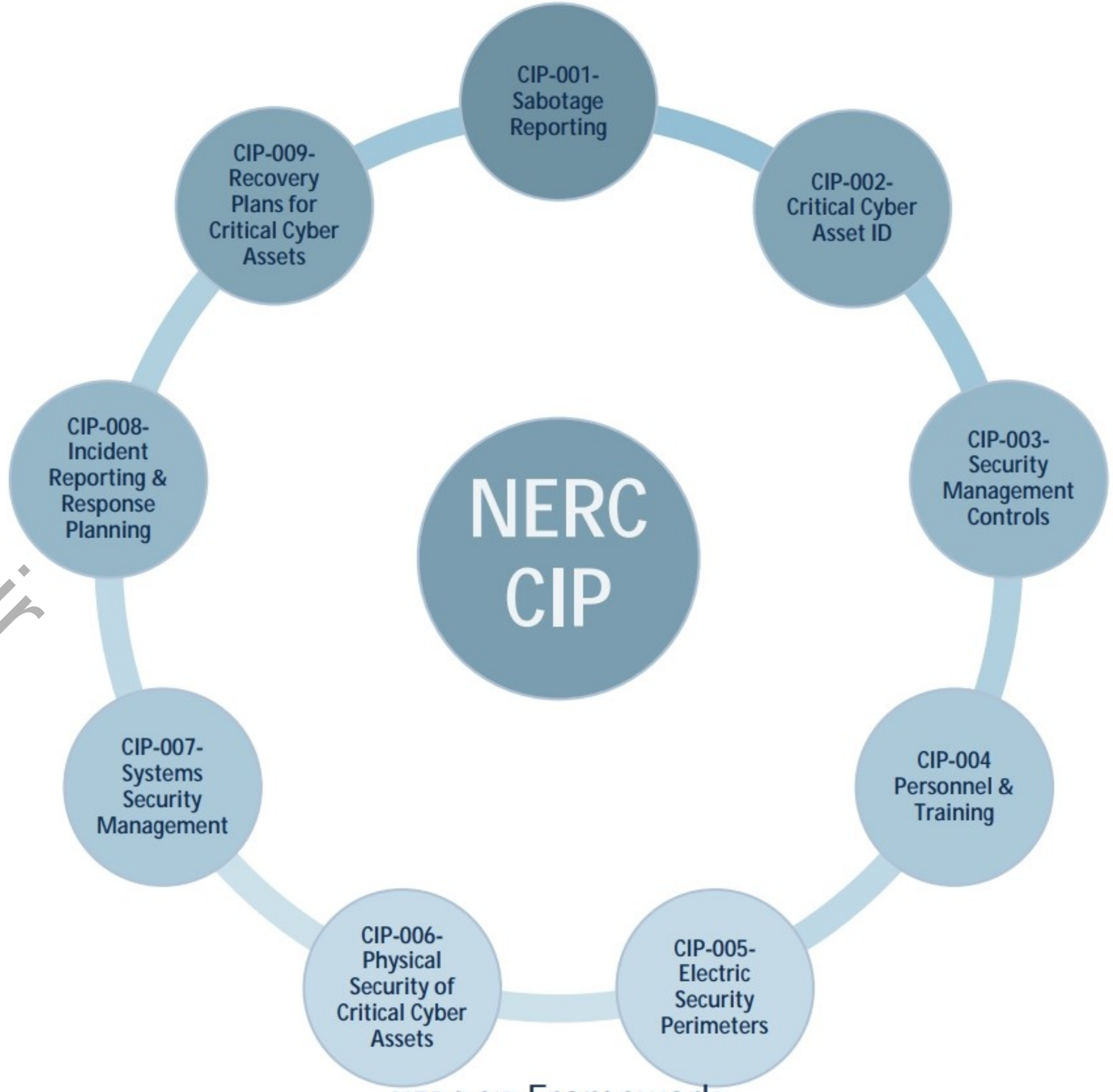
ISO 27036-1 Security of Suppliers

ISO 27037 Digital Evidence

Information Security ISO Standards

THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC) CRITICAL INFRASTRUCTURE PROTECTION (CIP)

- Require utilities to establish a baseline set of security measures.
- Only mandatory requirement electric utilities must comply when it comes to cyber-security.
  - Interconnected power systems of the contiguous United States, Canada and Mexico.



NERC CIP

CIP-001- Sabotage Reporting

CIP-002- Critical Cyber Asset ID

CIP-003- Security Management Controls

CIP-004 Personnel & Training

CIP-005- Electric Security Perimeters

CIP-006- Physical Security of Critical Cyber Assets

CIP-007- Systems Security Management

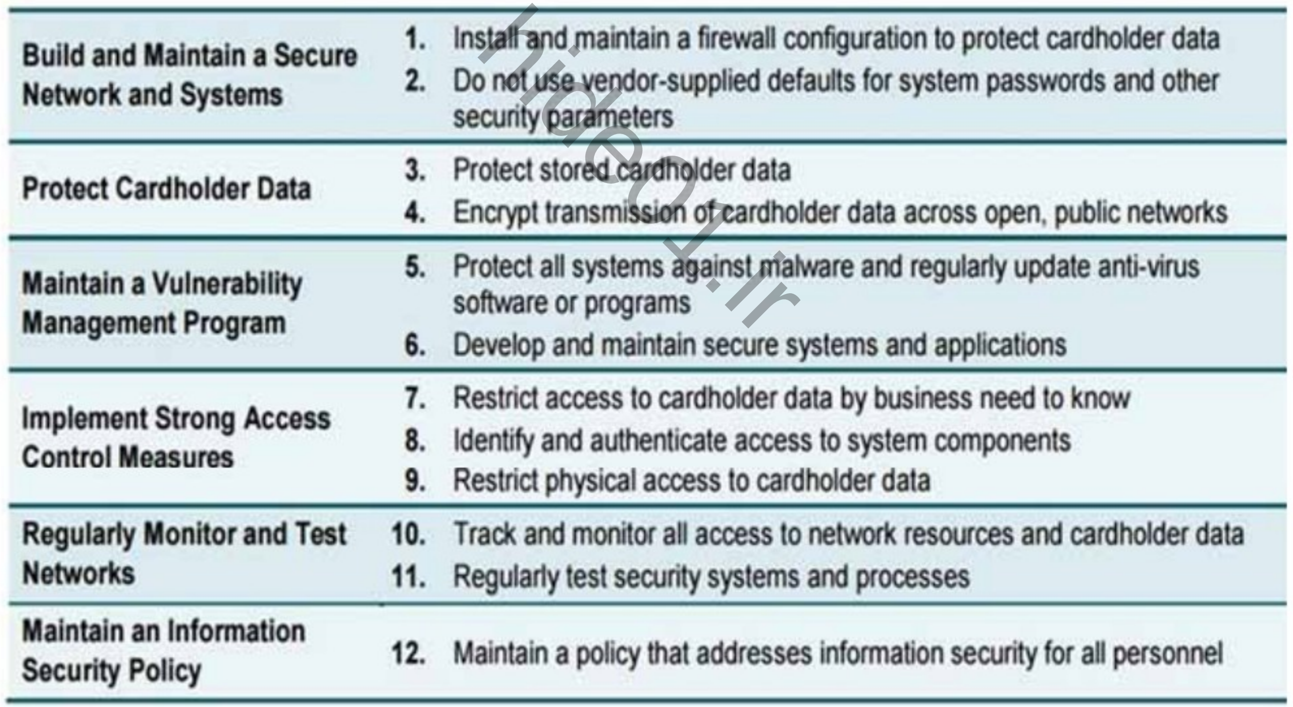
CIP-008- Incident Reporting & Response Planning

CIP-009- Recovery Plans for Critical Cyber Assets

NERC CIP Framework

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS VERSION 4.0)

PCI DSS was developed to encourage and enhance credit card security measures globally.

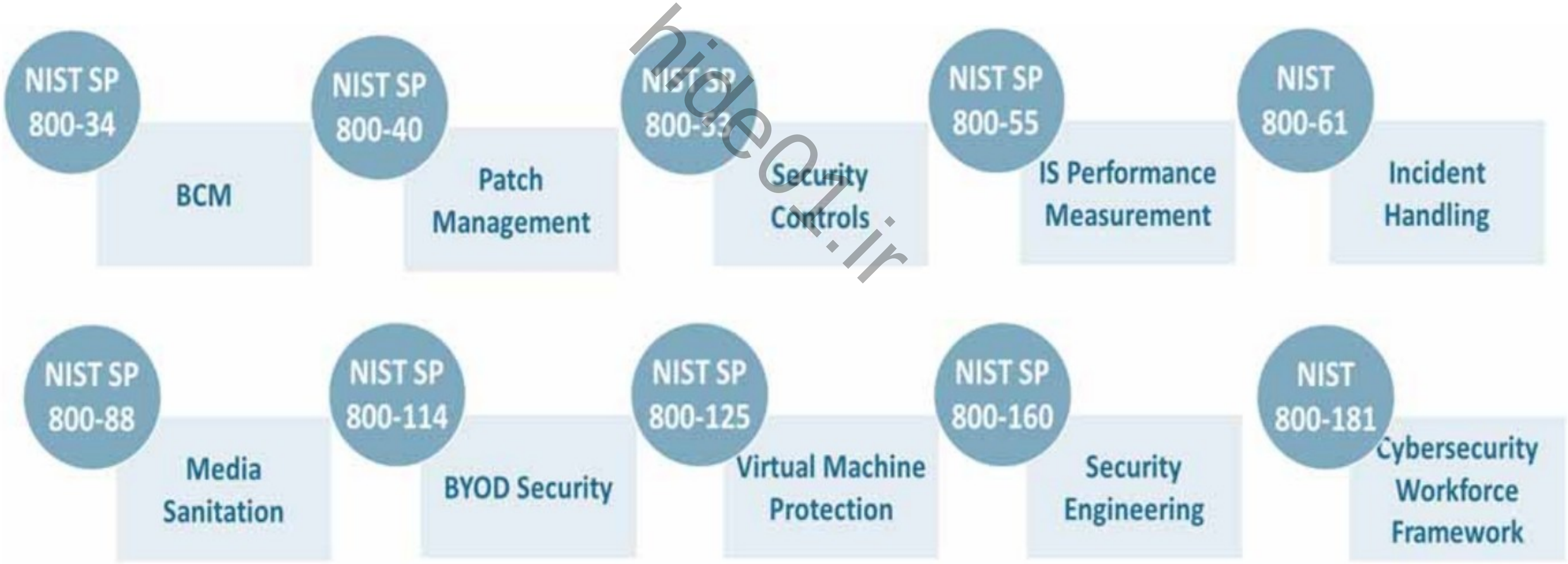


Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

PCI DSS Security Requirements

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATIONS

NIST publishes standards, guidelines, recommendations, and research on computers, cyber operations, information security, and privacy.



- NIST SP 800-34 BCM
- NIST SP 800-40 Patch Management
- NIST SP 800-53 Security Controls
- NIST SP 800-55 IS Performance Measurement
- NIST 800-61 Incident Handling
- NIST SP 800-88 Media Sanitation
- NIST SP 800-114 BYOD Security
- NIST SP 800-125 Virtual Machine Protection
- NIST SP 800-160 Security Engineering
- NIST 800-181 Cybersecurity Workforce Framework

NIST Information Security-Related Special Publications

THE STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS NUMBER 16 (SSAE 16)

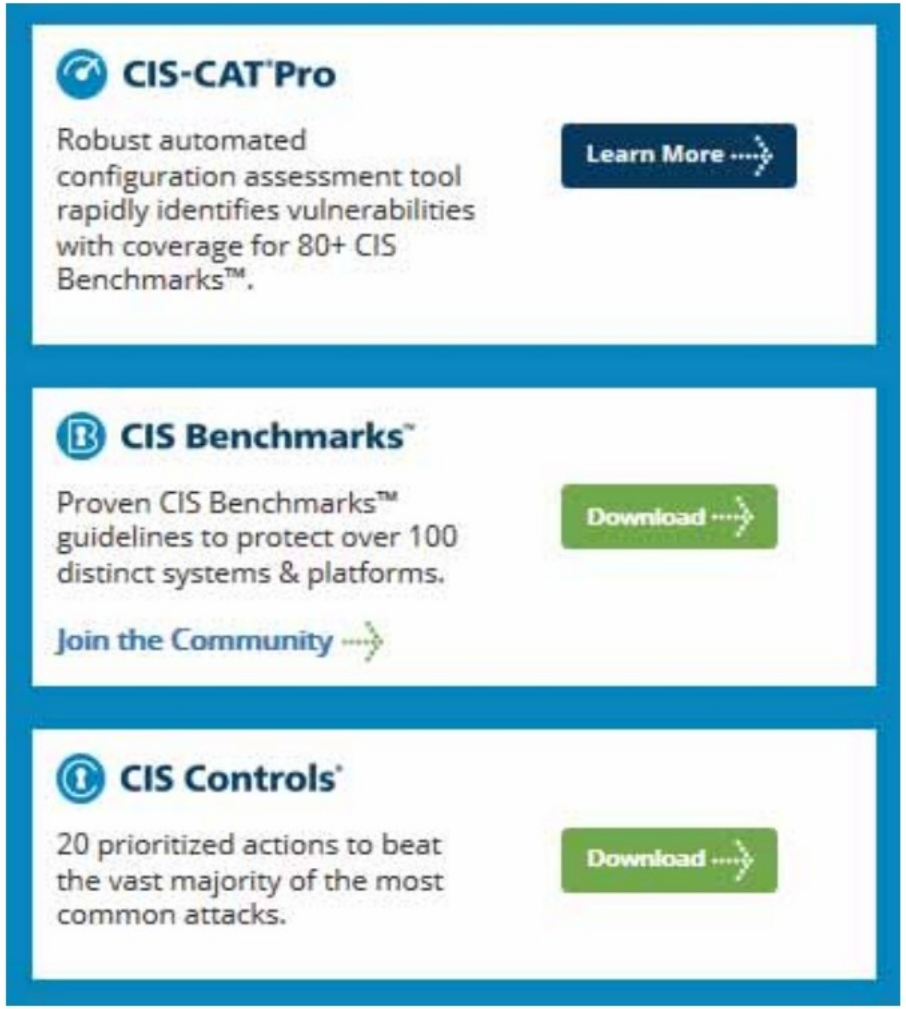
SSAE 16 is an auditing standard for service organizations. It replaced Statement on Auditing Standards number 70 (SAS 70).

- SSAE became effective in 2011 and was developed by the American Institute of Certified Public Accountants (AICPA).
- Largely an American standard.
- Two reports types:
  - SOC 1 Type 1 report is an independent snapshot of the organization's control landscape on a given day.
  - SOC 1 Type 2 report adds a historical element, showing how controls were managed over time (usually a minimum of 6 months).

3. GUIDELINES, GOOD, AND BEST PRACTICES

THE CENTER FOR INTERNET SECURITY (CIS)

- CIS is a nonprofit organization, formed in October 2000.
- Its mission is to identify, develop, validate, promote, and sustain best practice solutions for cyber defense.
- It is also chartered to build and lead communities to enable an environment of trust in cyberspace.



CIS-CAT Pro

Robust automated configuration assessment tool rapidly identifies vulnerabilities with coverage for 80+ CIS Benchmarks™.

CIS Benchmarks™

Proven CIS Benchmarks™ guidelines to protect over 100 distinct systems & platforms.

Join the Community

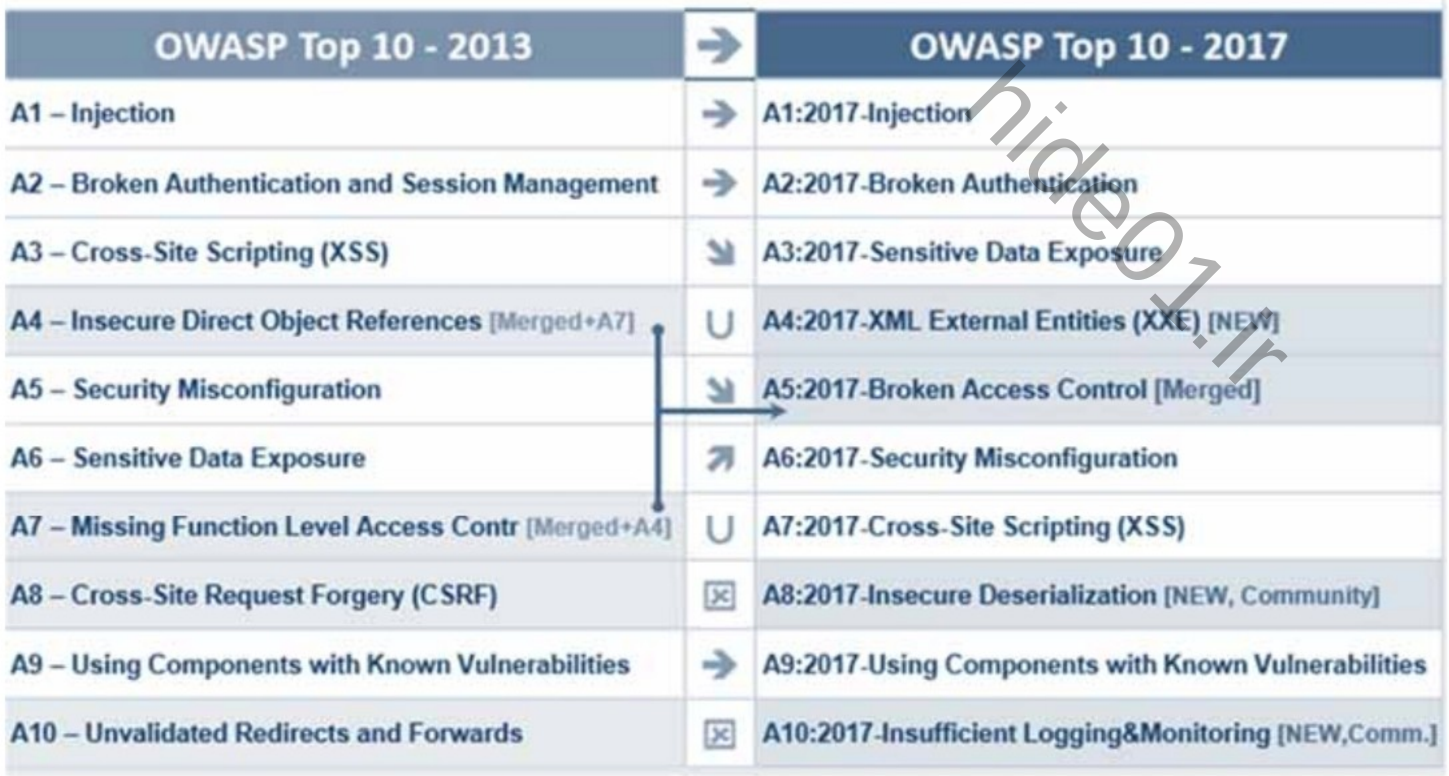
CIS Controls™

20 prioritized actions to beat the vast majority of the most common attacks.

CIS Cybersecurity Tools

THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

The OWASP Top Ten is a powerful awareness document for web application security that represents broad consensus about the most critical web application security flaws.



OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

OWASP Top-10 (2020)

1. Injection
2. Broken Authentication
3. Sensitive Date Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

OWASP Top-10 Seven-Year View

4. AUDIT MANAGEMENT

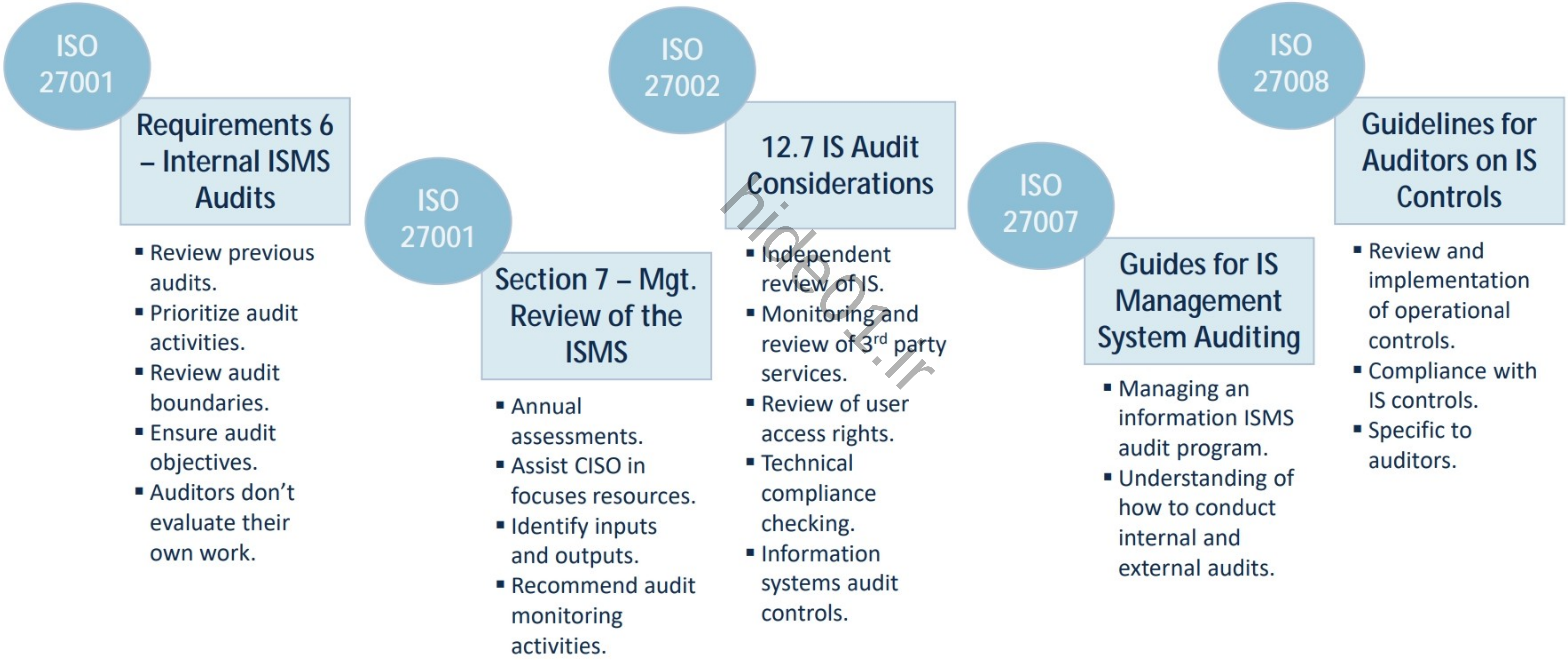
AUDIT EXPECTATIONS AND OUTCOMES

- Audits determine if the organization is keeping its commitment to comply with legal, regulatory, and internal requirements.
- They can identify potential problems or shortfalls in the organization's implementation of a risk management framework.
- Auditors examine the controls applied to protect information assets and verify they perform as documented and designed.

INFORMATION SECURITY AUDIT PRACTICES

- Information security audits are designed to:
  - Confirm that information technology is adequately safeguarded to prevent compromises or interruptions affecting an organization's goals.
  - Highlight violations of legal and regulatory requirements.
- The more frequently used and referenced IS audit practices include:
  - ISO/IEC.
  - NIST.
  - COBIT.

ISO/IEC AUDIT GUIDANCE



ISO 27001 – Requirements 6 – Internal ISMS Audits

- Review previous audits.
- Prioritize audit activities.
- Review audit boundaries.
- Ensure audit objectives.
- Auditors don’t evaluate their own work.

ISO 27001 – Section 7 – Mgt. Review of the ISMS

- Annual assessments.
- Assist CISO in focuses resources.
- Identify inputs and outputs.
- Recommend audit monitoring activities.

ISO 27002 – 12.7 IS Audit Considerations

- Independent review of IS.
- Monitoring and review of 3rd party services.
- Review of user access rights.
- Technical compliance checking.
- Information systems audit controls.

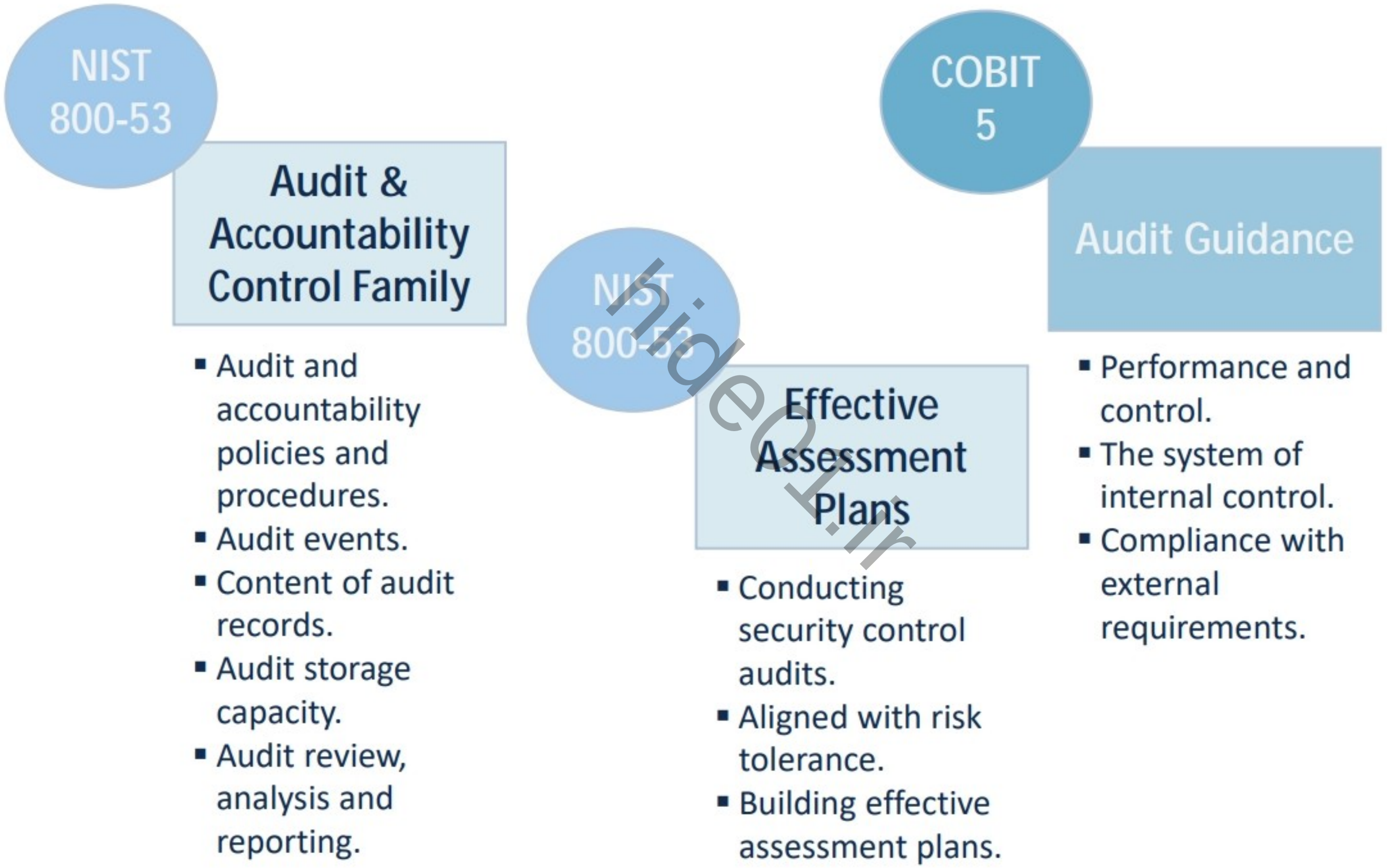
ISO 27007 – Guides for IS Management System Auditing

- Managing an information ISMS audit program.
- Understanding of how to conduct internal and external audits.

ISO 27008 – Guidelines for Auditors on IS Controls

- Review and implementation of operational controls.
- Compliance with IS controls.
- Specific to auditors.

NIST AND COBIT AUDIT GUIDANCE



NIST 800-53

Audit & Accountability Control Family

- Audit and accountability policies and procedures.
- Audit events.
- Content of audit records.
- Audit storage capacity.
- Audit review, analysis and reporting.

NIST 800-53

Effective Assessment Plans

- Conducting security control audits.
- Aligned with risk tolerance.
- Building effective assessment plans.

COBIT 5

Audit Guidance

- Performance and control.
- The system of internal control.
- Compliance with external requirements.

INTERNAL VERSUS EXTERNAL AUDITS

There are two types of audits:

- **Internal** – primarily focus on financial controls. Teams consist of individuals having experience in information technology and information security controls.
- **External** - focus on verifying financial statements and risk to the organization. They are typically performed by third parties or regulatory agencies.

Function	Internal Audit	External Audit
Independence	Internal department	External company
Reporting of Findings	Audit committee	Audit committee
Audit performance	Employees	Public accounting firm
Approach	Review controls	Test controls
Role	Consultant	Accountant
Focus	Risk management	Financial stability
Emphasis	Improve processes	Find faults and failures
Selection	Hired by organization	Shareholder vote
Allegiance	Management	Shareholders
Schedule	Ongoing process	Annually

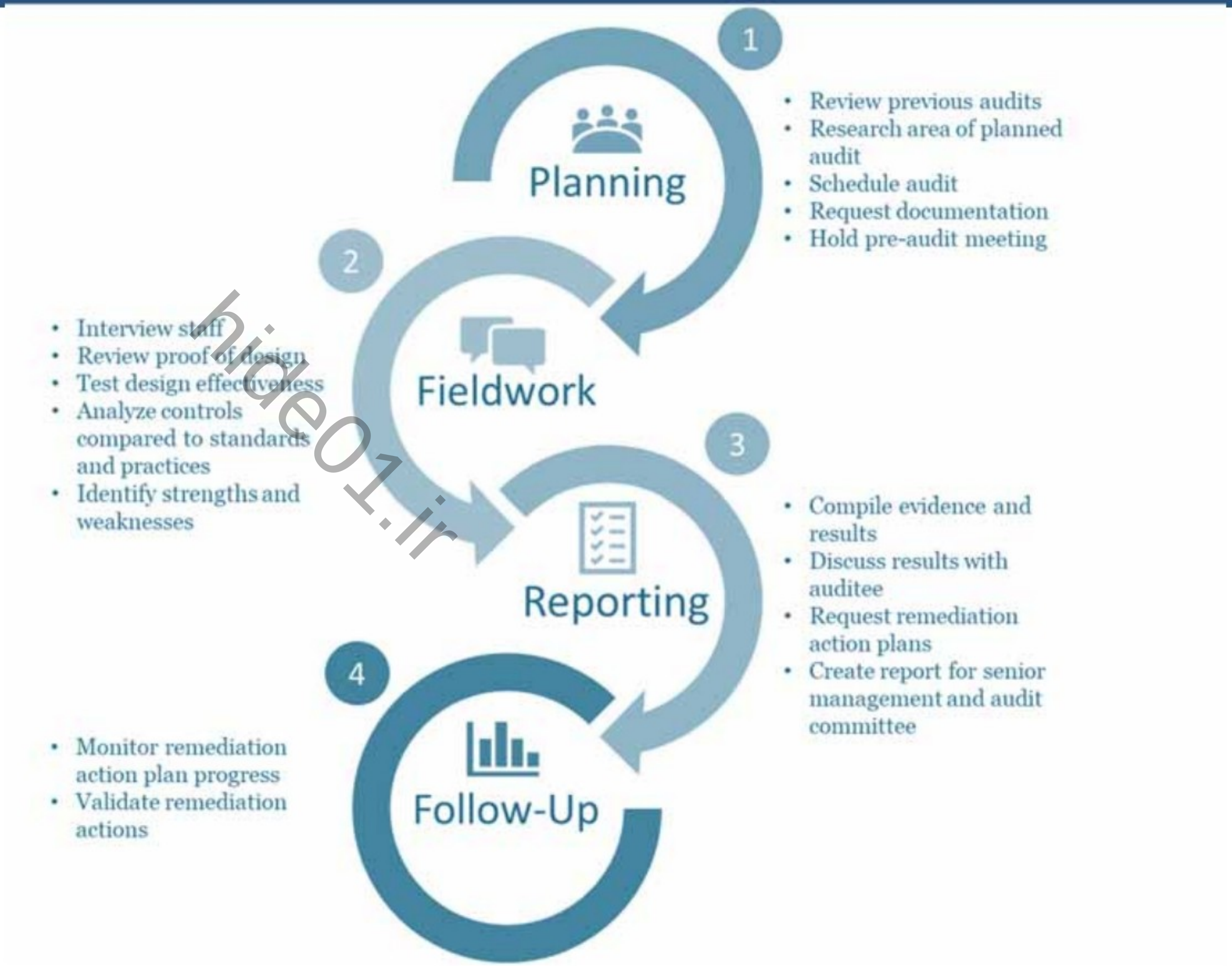
Internal vs. External Audit Function Comparison Chart

PARTNERING WITH THE AUDIT ORGANIZATION

- Senior management and the audit committee should create an environment to ensure the auditor–auditee relationship is not adversarial or compromised.
- CISOs should foster a partnership with internal and external auditors to help improve the effectiveness of the information security program.

AUDIT PROCESS

Typical audit workflow or process



1 Planning

- Review previous audits
- Research area of planned audit
- Schedule audit
- Request documentation
- Hold pre-audit meeting

2 Fieldwork

- Interview staff
- Review proof of design
- Test design effectiveness
- Analyze controls compared to standards and practices
- Identify strengths and weaknesses

3 Reporting

- Compile evidence and results
- Discuss results with auditee
- Request remediation action plans
- Create report for senior management and audit committee

4 Follow-Up

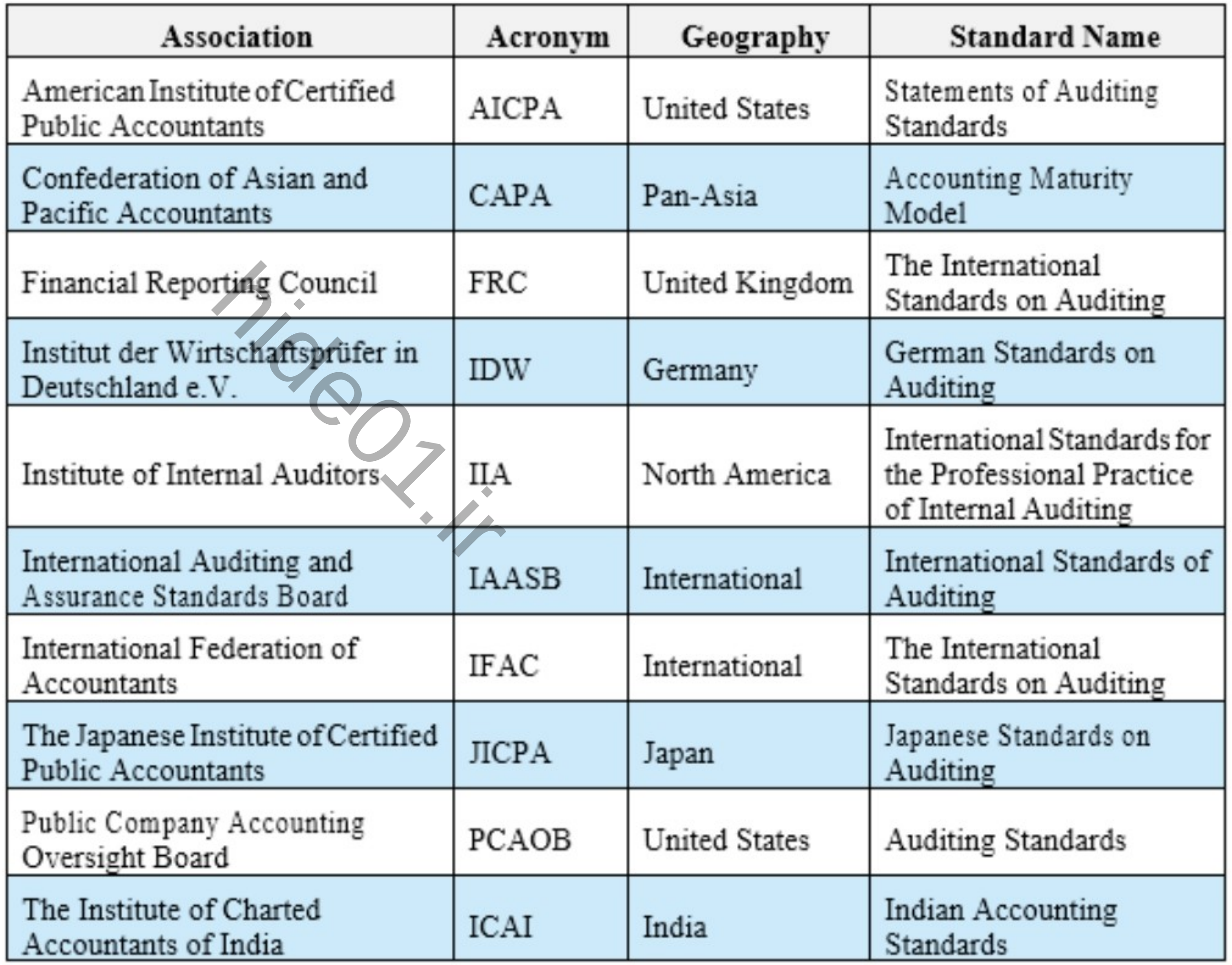
- Monitor remediation action plan progress
- Validate remediation actions

GENERAL AUDIT STANDARDS

- Audits are performed according to auditing standards.
- There are several widely followed international auditing standards.
- Security standards define not only the ethics, rigor, and integrity of an audit, but also the mandatory requirements of information assurance and security.

GENERAL AUDIT STANDARDS

Sample Worldwide Audit Standards



Association	Acronym	Geography	Standard Name
American Institute of Certified Public Accountants	AICPA	United States	Statements of Auditing Standards
Confederation of Asian and Pacific Accountants	CAPA	Pan-Asia	Accounting Maturity Model
Financial Reporting Council	FRC	United Kingdom	The International Standards on Auditing
Institut der Wirtschaftsprüfer in Deutschland e.V.	IDW	Germany	German Standards on Auditing
Institute of Internal Auditors	IIA	North America	International Standards for the Professional Practice of Internal Auditing
International Auditing and Assurance Standards Board	IAASB	International	International Standards of Auditing
International Federation of Accountants	IFAC	International	The International Standards on Auditing
The Japanese Institute of Certified Public Accountants	JICPA	Japan	Japanese Standards on Auditing
Public Company Accounting Oversight Board	PCAOB	United States	Auditing Standards
The Institute of Charted Accountants of India	ICAI	India	Indian Accounting Standards

GENERAL AUDIT STANDARDS

Information Security Audit Standards

COBIT 5: Framework for Information Technology and Governance

COSO 2013 Integrated-Integrated Framework

COMPLIANCE-BASED AUDITS

Compliance-based auditing (CBA) is a check for alignment to stated requirements

These audits determine whether an organization complies with policies, regulations, standards, or legal statutes.

RISK-BASED AUDITS

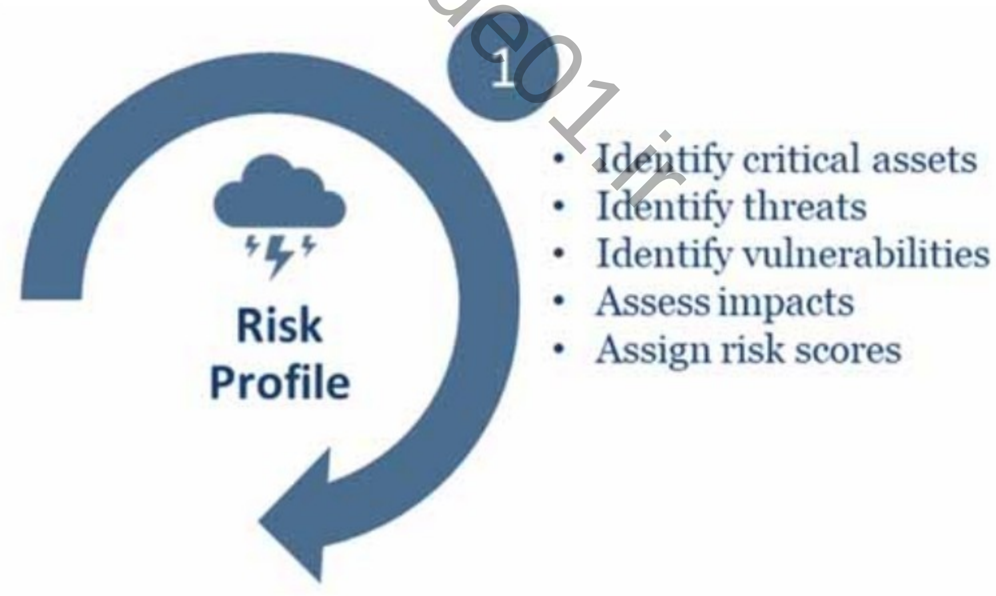
Risk-Based Auditing (RBA) focuses on the identification and management of risk.

Risk management processes are analyzed to determine what risks were managed, how they were managed, and the effectiveness of risk management.

RISK-BASED INTERNAL AUDIT

Risk-based Internal Audit (RBIA) is a widely accepted practice by internal auditors.

The audit process changes by simply inserting a Risk Profile phase ahead of the planning phase.



- Identify critical assets
- Identify threats
- Identify vulnerabilities
- Assess impacts
- Assign risk scores

RBIA Diagram

MANAGING AND PROTECTING AUDIT DOCUMENTATION

- Audit documentation can be subject to discovery in a legal investigation (such as during a data breach).
- It is in the organization's interest to establish client attorney privilege for the most sensitive security assessment and audit information.

PERFORMING AN AUDIT

These steps represent the general process typically used by internal and external auditors prior to conducting an audit.

1: Identify areas requiring auditing.

2: Determine how often auditing is required.

3: Establish an audit calendar.

4: Notify departments of the audits.

5: Prepare for the audit.

EVALUATING AUDIT RESULTS AND REPORT

- Audit findings provide feedback and opportunities for continuous improvement.
- The report typically starts with an executive summary defining the scope of the audit and a concise summary of findings.
- The body of the report contains:
  - A detailed review of the controls audited.
  - The methodology used to conduct the audit.
  - Specific findings.
  - Evidence used to support the findings.

REMEDIATING AUDIT FINDINGS

Responding to audit findings is a fundamental responsibility of a CISO and a core part of cybersecurity program governance.

- Analysis and interpretation of audit results:
  - Audit findings provide feedback and opportunities for continuous improvement. They allow identification and comparison of effective and ineffective controls.
- Outcomes for ineffective or missing controls:
  - If the audit determines that controls are ineffective or don't exist, this information should be incorporated into the risk register for further treatment planning.

LEVERAGE GRC SOFTWARE TO SUPPORT AUDITS

- Governance, Risk and Compliance (GRC) software can be used to automate audit management, simplifying the process for auditors and auditees.
- GRC tools are particularly helpful when risk-based audits are performed.
- Risk audit results can be mapped to implemented controls.

# DOMAIN 2
END

DOMAIN 2 SUMMARY

DOMAIN 2: SUMMARY - GENERAL

- This domain examined the treatment of risk through the application of key or compensating controls.
- CISOs need to manage controls as they would any other safeguard to ensure they are properly deployed and performing according to their intended purpose.
- Compliance requirements should be integrated with risk mitigation treatments to provide long-term value of effort.
- CISOs always participate in audits.
  - Cooperate with auditors.
  - Try to build strong relationships with them.
  - Leverage findings to improve the security program.

DOMAIN 2: SUMMARY - IS CONTROLS

- Security controls are core program assets.
- Open-source and proprietary control catalogs may be used.
- Controls should be managed within a lifecycle, from development to retirement.
- Security controls are most effectively deployed and managed using descriptive attributes.
- Controls should reside in a control catalog.
- Security services should reside in a service catalog.
- Security controls can have varying degrees of maturity depending on their contribution to risk treatments.

DOMAIN 2: SUMMARY - COMPLIANCE MANAGEMENT

- CISOs should be prepared to spend approximately half their time on compliance related activities.
- Acts are written ordnances or statutes published by a legislative body.
- Regulations are rules or directives that are created, maintained, and (in many cases) enforced by a central authority.
- Standards are consensus-based guidelines that prescribe specific controls.
- Guidelines and best practices are voluntary security controls.
- CISOs must find balance with governance, risk management, and compliance to best leverage resources and investments.

DOMAIN 2: SUMMARY - AUDIT MANAGEMENT

- Audits determine if an organization is keeping its commitment to comply with legal, regulatory, and internal requirements.
- Information security audits follow general auditing practices and standards.
- Audits can be conducted by internal or external teams.
- Risk-based Internal Audits (RBIA) allow organizations to focus on operational areas that have or may introduce risk.
- CISOs should review audit findings to verify accuracy, and correct inaccuracies.

DOMAIN 2 PRACTICE QUESTIONS

PRACTICE QUESTIONS

1. The Information Technology Infrastructure Library Version 4 (ITIL® 4) Information Security Management Practice is based on which standard?

Choose the BEST answer.

A. International Organization for Standardization (ISO) 31000.

B. International Organization for Standardization (ISO) 27001.

C. National Institute of Standards & Technology (NIST) Special Publication 800-30.

D. National Institute of Standards & Technology (NIST) Special Publication 800-124.

PRACTICE QUESTIONS

2. You see compromised employee account details on a web site that could result in exposed organizational data and financial information.

From the choices provided, what should you do FIRST to minimize this threat?

A. Reset passwords for suspected compromised accounts.

B. Educate users about the threat of phishing.

C. Monitor the perimeter firewall for signs of phishing.

D. Contact a reputable security vendor to install an anti-phishing appliance.

PRACTICE QUESTIONS

3. An effective method for reducing the impact of credential theft is:

Choose the BEST answer.

A. Gaining the trust of your users so they will listen to you.

B. Implementing employee monitoring so they don't go to unauthorized sites.

C. Deploying multi-factor authentication so accounts are better protected.

D. Resetting passwords every thirty days.

PRACTICE QUESTIONS

4. Metrics capable of demonstrating that an organization is susceptible to, or has a high probability of being susceptible to, a risk that exceeds the acceptable risk appetite are known as:

A. Key Performance Indicators (KPI).

B. Key Risk Indicators (KRI).

C. Insurance Actuary Tables (IAT).

D. Risk Assumption Tables (RAT).

PRACTICE QUESTIONS

5. A primary consideration when selecting to transfer risk as a risk treatment option is which of the following?

Choose the BEST answer.

A. Capital cost.

B. Selection of a security control vendor.

C. Security consultant fees.

D. Insurance cost.

C|CISO

CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER

DOMAIN 3

INTRODUCTION

This domain teaches students how to:

- Manage information security projects and programs.
- Build relationships with key stakeholders,
- Build an information security program strategy.
- Assess and staff an information security program.
- Converge DRP/BCM and information security activities.
- Build effective incident response and digital forensics programs.
- Design a security operations capability.
- Identify infrastructure vulnerabilities.

KNOWLEDGE ASSUMPTIONS

Students are expected to have:

- Five years of domain experience.
- Familiarity of operations management vocabulary.
- Working knowledge of project management principles.
- Basic understanding of disaster recovery practices.
- Basic understanding of data backup and recovery.
- Working knowledge of security information and event management techniques.
- Basic understanding of digital forensics.
- Understanding of threat and vulnerability management.

SECURITY PROGRAM MANAGEMENT AND OPERATIONS

DOMAIN 3

SECURITY PROGRAM MANAGEMENT AND OPERATIONS

DOMAIN OUTLINE

1. Program Management

2. Operations Management

Summary and Practice Questions

1. PROGRAM MANAGEMENT

1.1 A SECURITY CHARTER, OBJECTIVES, REQUIREMENTS, STAKEHOLDERS, AND STRATEGIES

As the CISO of a portfolio or program, you will need to:

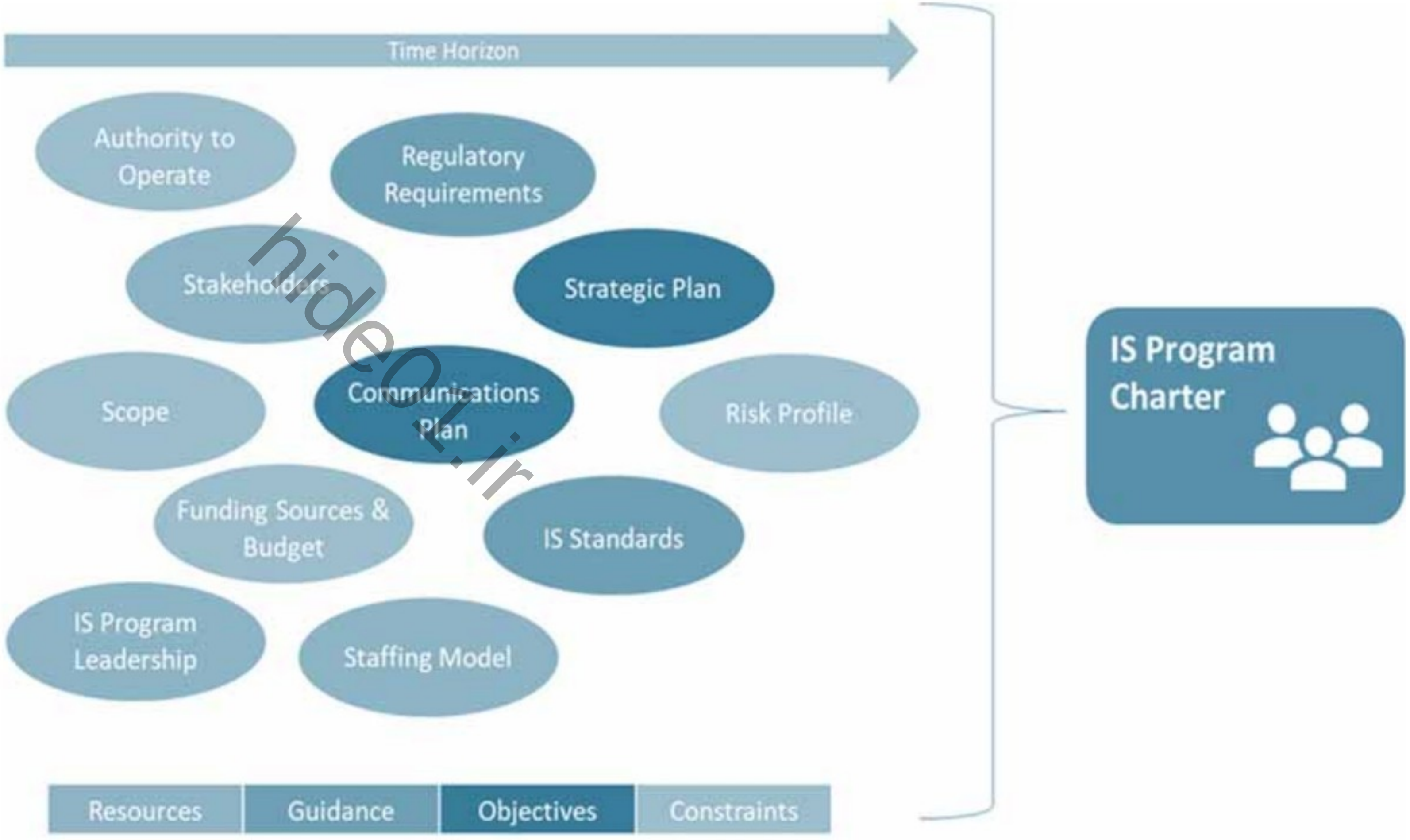
- Define a charter establish the focus and goals of the organization.
- Specify the objectives you wish to accomplish and when they will be completed.
- Identify program requirements to assure continuous support of security services and operations.
- Identify key stakeholders and influencers to help establish program support.

1.1.1 SECURITY PROGRAM CHARTER

- A charter is a document detailing the authority, responsibility, and authority to operate a security program.
- The charter provides a clear explanation of the mission, goals, and operational objectives of the security team.
- CISOs rely on prior experience, knowledge, and frameworks to define the elements that should exist in the organization's security program.

1.1.1 SECURITY PROGRAM CHARTER MODEL

This figure provides the major sections of an information security program charter.



Information Security Program Charter Model

1.1.1 SECURITY PROGRAM CHARTER ELEMENTS

Elements of the information security program charter include:

- **Resources** - the personnel who will support, staff, and lead the information security program.
- **Guidance** - influences that formulate the design of the information security program.
- **Objectives** - initial planning points that shape the foundation of the information security program.
- **Constraints** - factors that could inhibit program progress and delivery of services.

1.1.2 SECURITY PROGRAM OBJECTIVES

- Effective information security programs require clearly defined objectives.
- Examples of information security program objectives include:
  - Align the program with critical business functions through a partnership with asset owners.
  - Integrate security planning within the SDLC function.
  - Identify assets and assign risk owners.
  - Invest in asset protections commensurate with asset values.
  - Leverage human resources as the first line of defense.
  - Recover critical security functions with minimal impact to the business.

1.1.3 PROGRAM REQUIREMENTS

- When creating a security program, supporting requirements should be identified and integrated into the program.
- The following are a few examples of a security program's supporting design requirements:
  - Identify assets requiring protection.
  - Inventory legal, regulatory, and compliance requirements.
  - Define the attack surface.
  - Determine risk profiles.
  - Complete Business Impact Assessments (BIAs).

1.1.4 SECURITY PROGRAM STAKEHOLDERS

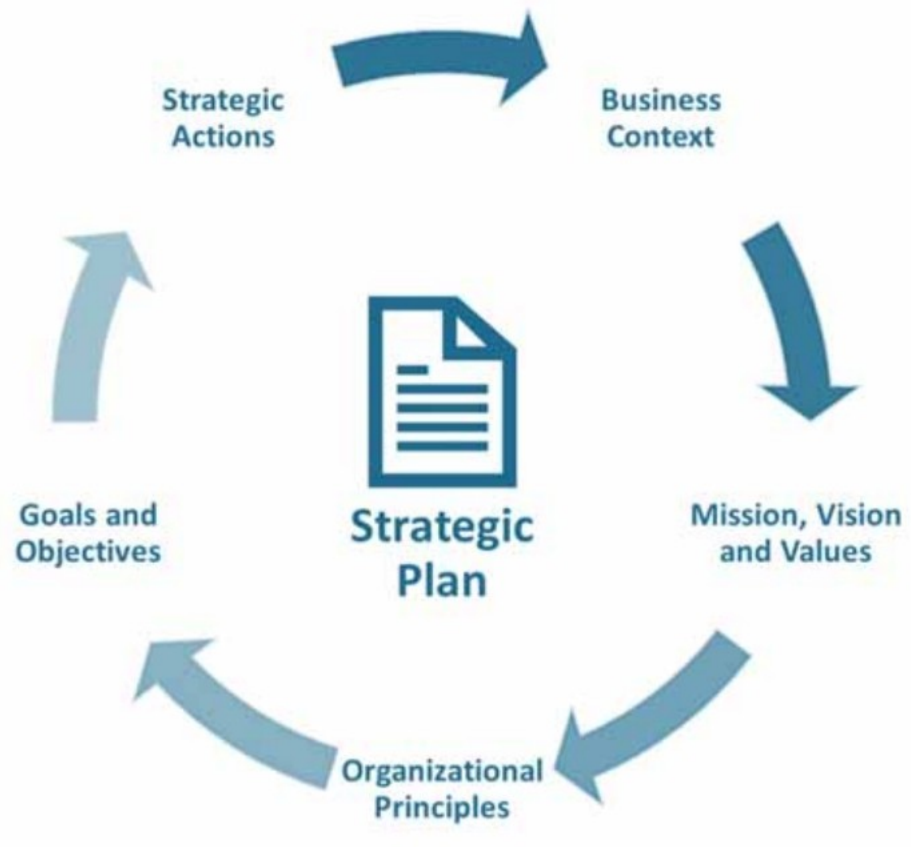
- A stakeholder is a person who has a vested interest in a program or project.
- Stakeholder planning input helps to assure the information security program delivers expected outcomes.

Stakeholder Management Plan	
Stakeholder Name	Jane Doe
Program Interests	ERP and SAP application development
Program Role	Application Development Manager
Success Goals	Integration of security protocols within Agile development sprints
Communications and Reporting Strategy	Weekly AppDev status meeting attendance Monthly application security incident reports
Communications and Reporting Schedule	Monthly

Sample Stakeholder Management Plan

1.1.5 SECURITY PROGRAM STRATEGY DEVELOPMENT

- Strategic plans are periodically reviewed and updated to incorporate changes in the business and technical infrastructure.
- CISOs should understand the business context of the security program and monitor it to assure the program aligns to the organization.
- Organizational operations establish how the security program will operate.
- Goals and objectives guide strategic planning.



Strategic Plan Development Life Cycle

1.1.5 SECURITY PROGRAM STRATEGY DEVELOPMENT (CONT'D)

The following are the three basic approaches to developing a strategic plan:

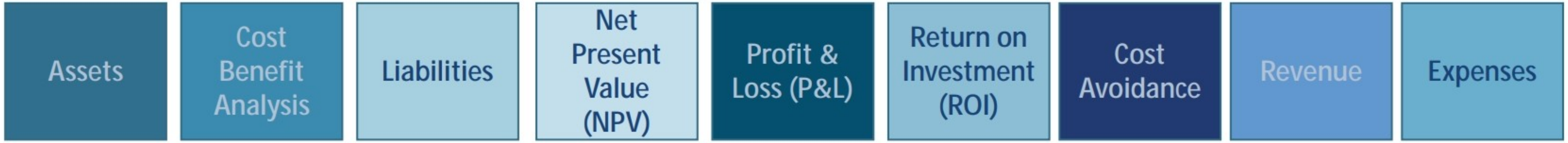
1. **Protect the 'crown jewels'** - this is a traditional approach based on protecting the most important assets of the organization.
2. **'Football playbook' approach** - this sports approach is usually preferred by organizations with substantial resources and funding. It executes an information security program based on a published playbook.
3. **Attack surface approach** - this approach is based on identifying and defending against threats to the broad range of assets and is applied according to ranked criticality.

1.2 EXECUTING AN INFORMATION SECURITY PROGRAM

- Executing the information security program is the implementation of processes and activities identified during the program design phase.
- Program execution is accomplished to achieve objectives.
- Measuring outcomes is important to assure the program is sufficiently delivering intended goals.
- Programs that do not achieve the intended goal are typically adjusted to improve performance. Communication is critical if changes occur.
- Successful programs often use externally defined maturity models, such as the Capability Maturity Model Integration (CMMI), to improve results.

1.3 DEFINING, DEVELOPING, MANAGING, AND MONITORING THE INFORMATION SECURITY PROGRAM

- Financial management is a critical role of a CISO.
- Accounting management delivers financial information to help decision makers plan, direct, and control business operations.
- Knowing the organization's accounting rules will help you maintain your program according to rules and established processes.
- Key financial terms and concepts a CISO should understand include:
- What do these areas provide as indicators of program budget support



Assets

Cost Benefit Analysis

Liabilities

Net Present Value (NPV)

Profit & Loss (P&L)

Return on Investment (ROI)

Cost Avoidance

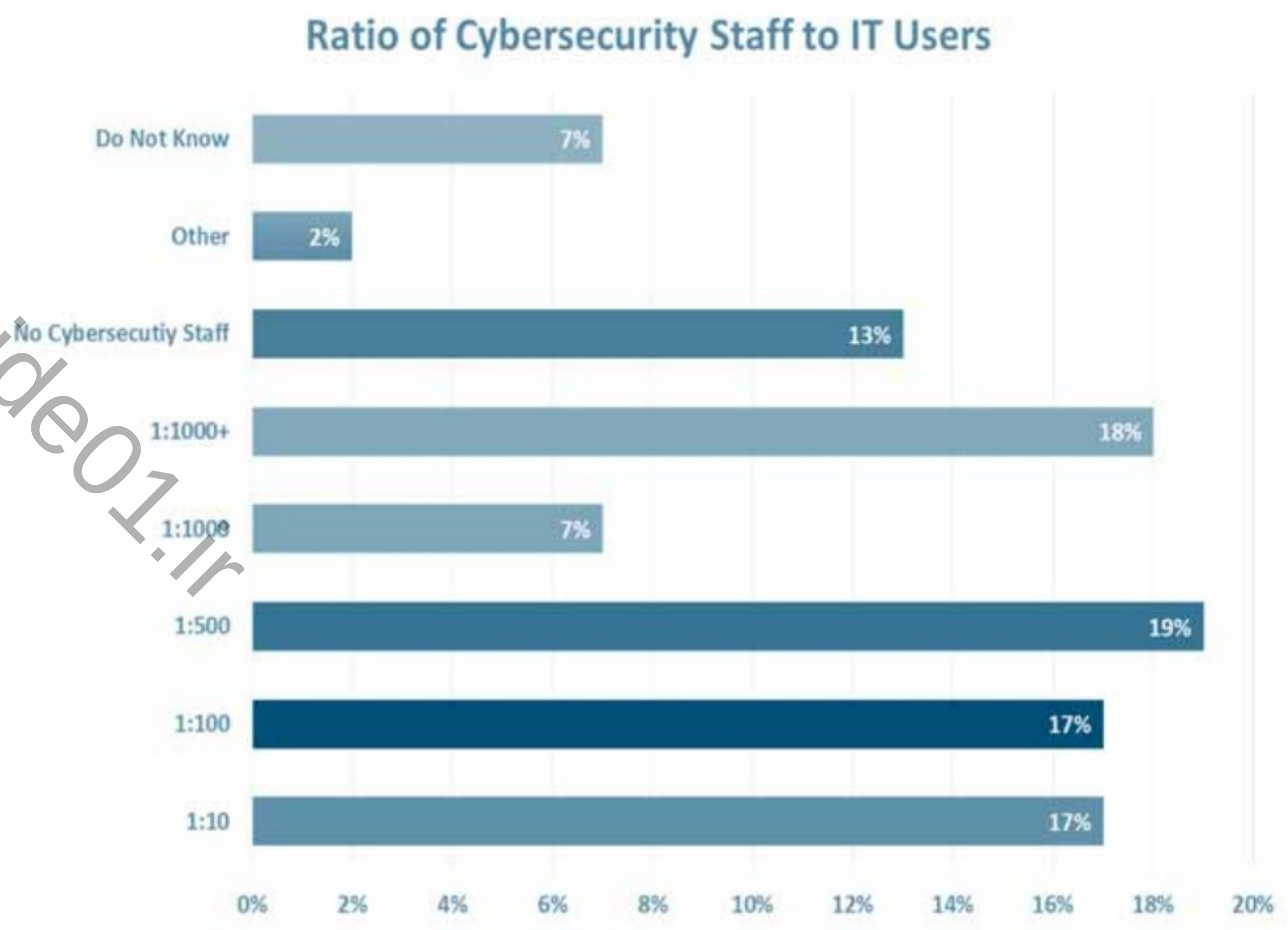
Revenue

Expenses

Building Blocks of IS Program Financial Management

1.4 DEFINING AND DEVELOPING INFORMATION SECURITY PROGRAM STAFFING REQUIREMENTS

- Critical security program activities must deliver without interruption
- Adequate resources must be available to support activities.
- Security operations staffing plans identify hours and resources for activities supporting the operation.
- The staffing plan should define 24-hour resource availability and identify possible overlap and peak-time support needs.



A 2017 Health Information and Management Systems Society cybersecurity survey of 126 healthcare organizations revealed the following staffing ratios.

1.4 DEFINING AND DEVELOPING INFORMATION SECURITY PROGRAM STAFFING REQUIREMENTS

Administrative & Analyst Staff

- Admin support
- Risk analysts
- Compliance analysts

Technical Staff

- Network security engineers
- Security Product specialists
- Security architects
- System admins

Security Operations Staff

- Penetration testers
- SOC analysts
- Threat hunters

Specialized Staff

- Data scientists
- Digital forensics investigators
- Malware engineers
- Threat analysts

1.5 MANAGING THE PEOPLE OF A SECURITY PROGRAM

Don't just manage.

Be a leader and mentor.

- Find what motivates each employee and use that as inducement for obtaining optimum performance.
- Apply positive corrective feedback to counsel employees who make mistakes.
- Challenge employees to surpass their core skills to add value to other parts of the information security program.
- Give employees a voice in the information security program evolution.
- Provide a growth plan for employees by providing training, certification goals, and career path advisement.
- Know when to manage out problem employees before they affect team morale.

1.5.1 RESOLVING PERSONNEL AND TEAMWORK ISSUES

- CISOs should have an open communication environment where employees are encouraged to talk about work issues.
- Creating a conflict resolution strategy with the HR department ensures company policies are followed and the potential for personnel issues is minimized.
- There is always a balance that can be found between meeting the needs of the organization and those of the employee.

1.5.1 RESOLVING PERSONNEL AND TEAMWORK ISSUES

UC Berkeley's Human Resources Manual suggests the following actions to resolve workplace discord

- Acknowledge that a difficult situation exists.
- Let individuals express their feelings.
- Define the problem.
- Determine the underlying needs.

- Find common areas of agreement, no matter how small.
- Find solutions to satisfy needs.
- Determine the follow-up to monitor actions.
- Determine what you will do if the conflict goes unresolved.

1.5.2 MANAGING TRAINING AND CERTIFICATION OF SECURITY TEAM MEMBERS

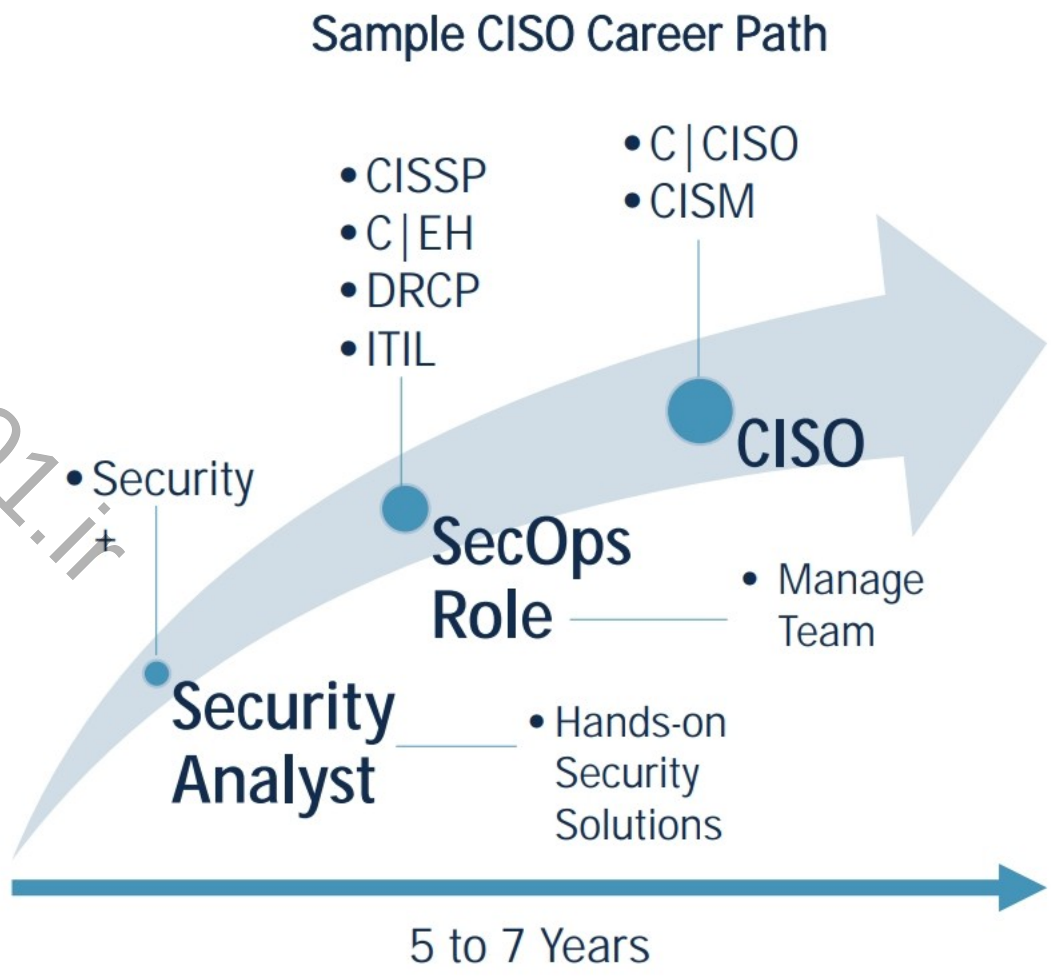
- CISOs own the responsibility to ensure their personnel have adequate training and the opportunity to achieve career objectives.
- Certifications are typically paid for by the organization to incent employees to improve foundational skills.
- CISOs should have a plan for the potential loss of key personnel.
- Having employees cross-trained in core disciplines will limit disruptions due to vacancies or absence.

Which is worse?

You train employees and they leave.
You don’t and they stay.

1.5.3 CLEARLY DEFINED CAREER PATH

- Members of your security team should know how their career will progress.
- Be a leader and enable them.
- It is important to clearly communicate expectations and provide employees with feedback on their commitments.
- This provides a strong, positive reward mechanism and improves morale.



1.5.4 DEIGNING AND IMPLEMENTING A USER AWARENESS PROGRAM

- Every organization should have a security awareness program with the goal of educating and reinforcing security.
  - To emphasize the importance of protecting sensitive information.
  - To reinforce To identify and avoid a variety of attacks.
  - To help shift the culture to one of higher security awareness.
- The following are the minimum requirements for a security awareness program:
  - Determine supporting technologies, processes, roles, and responsibilities.
  - Establish and communicate the goal – to create a security aware culture.
  - Define metrics to assess awareness training effectiveness.
- Don't make it boring. This is to provide value to the organization, not simply check a box!

1.6.1 MANAGING THE ARCHITECTURE AND ROADMAP OF THE SECURITY PROGRAM

- The CISO will often act as a security architect (or, at a minimum, review and approve architectures).
- A core part of the security program is to design and develop the security program architecture and plans for implementation.
- CISOs are comparable to a program director that monitors and guides efforts of the defining security architectures.
- These activities cannot be accomplished with an isolationist approach – CISOs need consensus from organizational stakeholders and influencers.

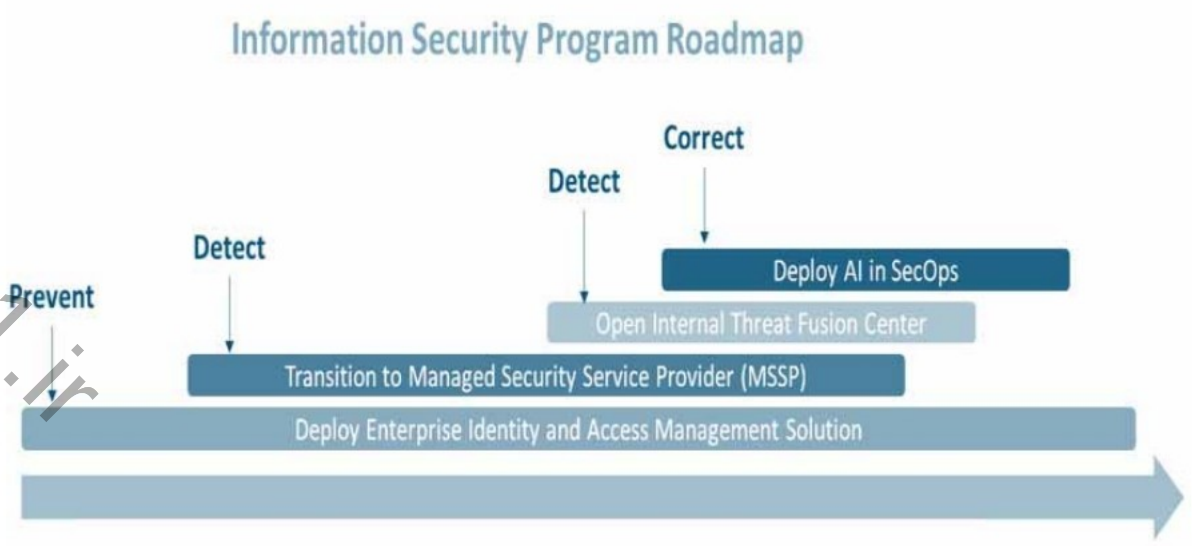
1.6.1 INFORMATION SECURITY PROGRAM ARCHITECTURE

- The security program architecture is the representation of what is provided to the organization when implemented.
- It embodies the vision of the program and is focused on business outcome.
- The architecture has multiple layers, with each providing a different abstraction or view of the security program.
- The following are sources for information security program architectures:
  - DOE IT Security Architecture.
  - Open Enterprise Security Architecture (OESA).
  - Sherwood Applied Business Security Architecture (SABSA).

Discussed in Domain 5

1.6.2 INFORMATION SECURITY PROGRAM ROADMAP

- Roadmaps provide a method to graphically communicate the goals and objective of the information security program.
- They are an easy way to communicate the strategic direction of the program to the employees, stakeholders, and sponsors.
- Roadmaps can have short, medium, and long-term perspectives.


Information Security Program Roadmap
Correct
Detect
Detect
Prevent
Deploy AI in SecOps
Open Internal Threat Fusion Center
Transition to Managed Security Service Provider (MSSP)
Deploy Enterprise Identity and Access Management Solution

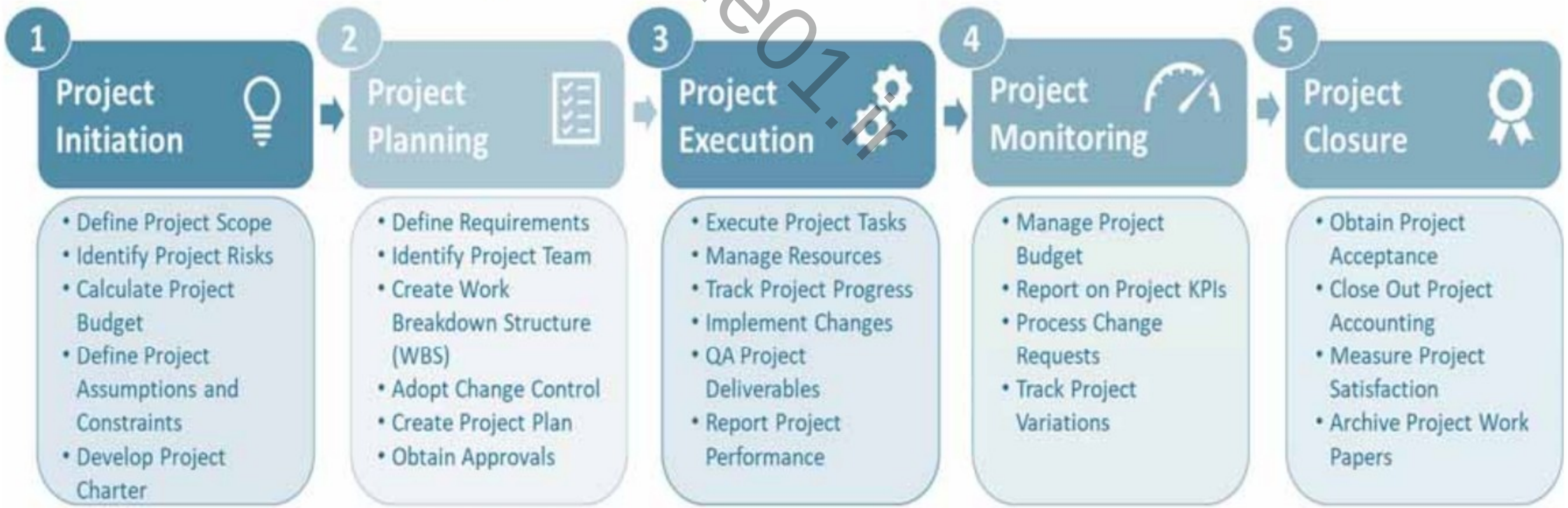
Information Security Program Roadmap

1.7 PROGRAM MANAGEMENT AND GOVERNANCE

- Program management describes the efforts of an organization to coordinate related projects and activities to achieve major goals or outcomes.
- It describes requirements to coordinate projects and deliver the expected product or solution.
- Program management controls a wide range of activities and deliverables in support of organizational objectives.
- CISOs must leverage project management as a tool to consistently deliver security solutions, controls, and remediation within an organization.

1.1.7 UNDERSTANDING PROJECT MANAGEMENT PRACTICES AND CONTROLS

- Project management methodology depends on the size and scope of a project and the adopted organizational project management methodology.
- CISOs need to work with the Project Management Office (PMO) and understand how to best leverage the available capabilities to achieve security program success.
- The traditional project management model includes five phases that divide project work into manageable and related activities supporting project delivery.



1 Project Initiation
- Define Project Scope
- Identify Project Risks
- Calculate Project Budget
- Define Project Assumptions and Constraints
- Develop Project Charter

2 Project Planning
- Define Requirements
- Identify Project Team
- Create Work Breakdown Structure (WBS)
- Adopt Change Control
- Create Project Plan
- Obtain Approvals

3 Project Execution
- Execute Project Tasks
- Manage Resources
- Track Project Progress
- Implement Changes
- QA Project Deliverables
- Report Project Performance

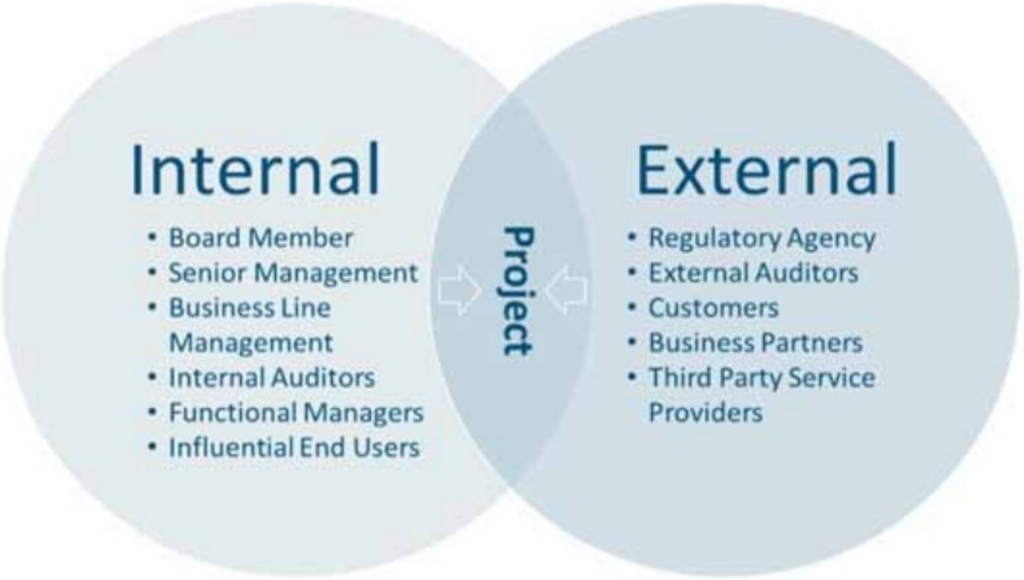
4 Project Monitoring
- Manage Project Budget
- Report on Project KPIs
- Process Change Requests
- Track Project Variations

5 Project Closure
- Obtain Project Acceptance
- Close Out Project Accounting
- Measure Project Satisfaction
- Archive Project Work Papers

Project Management Life Cycle

1.7.2 IDENTIFYING AND MANAGING PROJECT STAKEHOLDERS

- At the project level, a stakeholder is anyone who has a vested interest in the successful outcome of the project.
- It is essential to identify the stakeholders of a project and how they influence the overall project.
- Stakeholders can be internal or external to the organization.



Project Stakeholders

1.7.3 MEASURING THE EFFECTIVES OF PROJECTS

- Key Performance Indicators (KPIs) aid in measuring the success or failure of projects.
- Understanding KPIs and selecting the ones that are best suited to measuring a specific project team's performance is not always easy.
- The types of project management KPIs used to measure performance and strength include:
  - Financial.
  - Quantitative.
  - Qualitative.
  - Process.
  - Team effectiveness.

1.8 BUSINESS CONTINUITY MANAGEMENT (BCM) AND DISASTER RECOVERY PLANNING (DRP)

- CISOs are increasingly responsible for other, but related business roles and responsibilities.
- These roles typically include business continuity and disaster recovery functions.
- These disciplines are not mutually exclusive, and one cannot occur without the other if an organization desires to successfully recover from an adverse event.

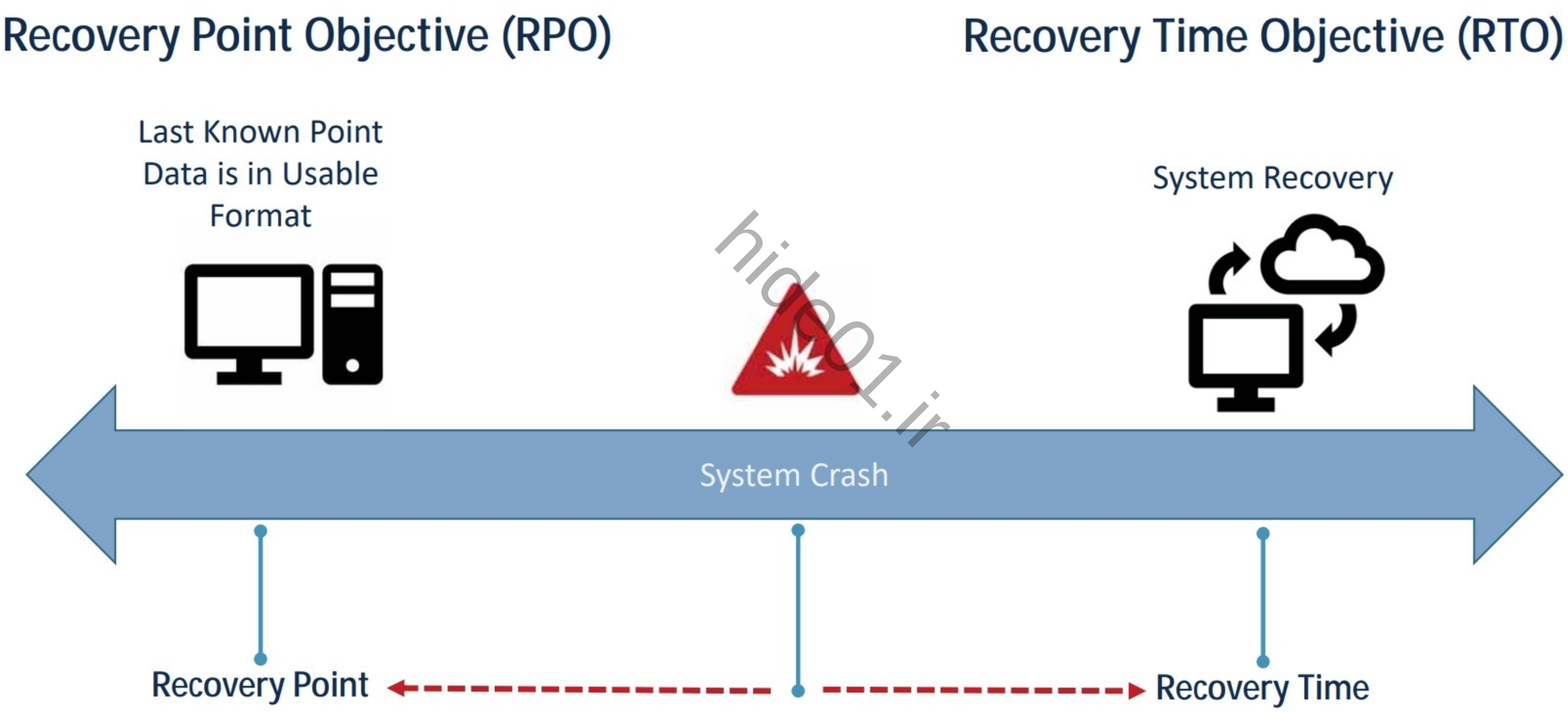
1.9 DATA BACKUP AND RECOVERY

- The needs of the organization and Recovery Time Objectives (RTOs) are the primary drivers of recovery operations.
- CISOs should assure data encryption and encryption key management requirements are included in data backup solutions.
- CISOs should consider the wide range of backup methods and approaches that are currently available.

- Tapes.
- Redundant Array of Independent Disks (RAID).
- Full data backups versus incremental backups.

- Differential backups.
- Storage Area Network (SAN).
- Cloud solutions.
- Air gap data backups.

1.10 BACKUP STRATEGY


Recovery Point Objective (RPO)
Recovery Time Objective (RTO)
Last Known Point Data is in Usable Format
System Recovery
System Crash
Recovery Point
Recovery Time

RPO and RTO Figure

1.10 BUSINESS IMPACT ASSESSMENT (BIA)

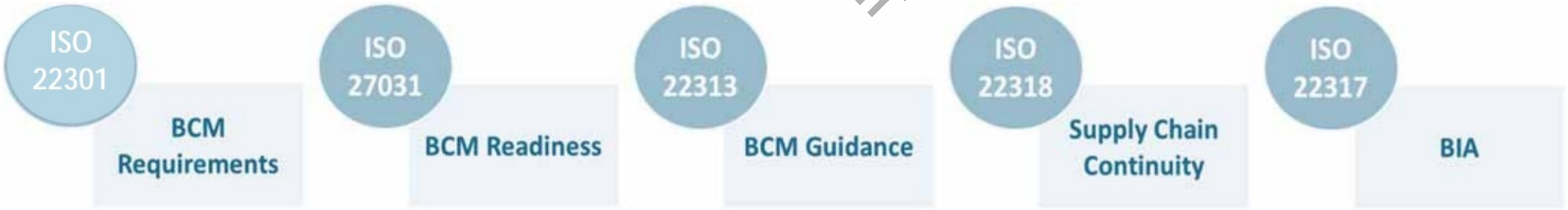
The Business Impact Assessment (BIA) is a critical first step for creating Business Continuity Plans (BCP).

- It is used to determine:
  - Business value of systems.
  - Prioritization for recovery of systems.
  - Asset owners.
  - Risk management program connection requirements.

1.11 ISO BCM STANDARDS

ISO Business Continuity Management standards provide guidance for strategy, planning, and technical recovery.

The following are the most used business continuity ISO standards.



ISO Continuity of Operations Standards

1.11.1 BUSINESS CONTINUITY MANAGEMENT (BCM)

- Business continuity planning (BCP) assures that business operations can continue successfully in the event of a disruption.
- BCP activities consist of steps to implement formal plans and procedures to restore or maintain operations.
- Plans combines analysis from the BIA with procedures required to restore operations after a disruption.
- Plans can include content determining requirements for HR, law enforcement, safety, transportation, security, and many other functions.

1.11.1 BUSINESS CONTINUITY MANAGEMENT (BCM)

The business continuity plan should include the following content:

- BCP roles and responsibilities.
- Lines of authority, succession of management, and delegation of authority.
- Notification rosters and call lists for key personnel and external partners.
- Communication plans for external customers and support organizations.
- RPO and RTO from the BIA.
- Detailed procedures, resources, and logistics for recovery of processes and systems.
- Manual process alternatives to automated processes in case of failure.
- Test plans and training exercises.
- Schedules, triggers, and requirements for plan maintenance and updates.

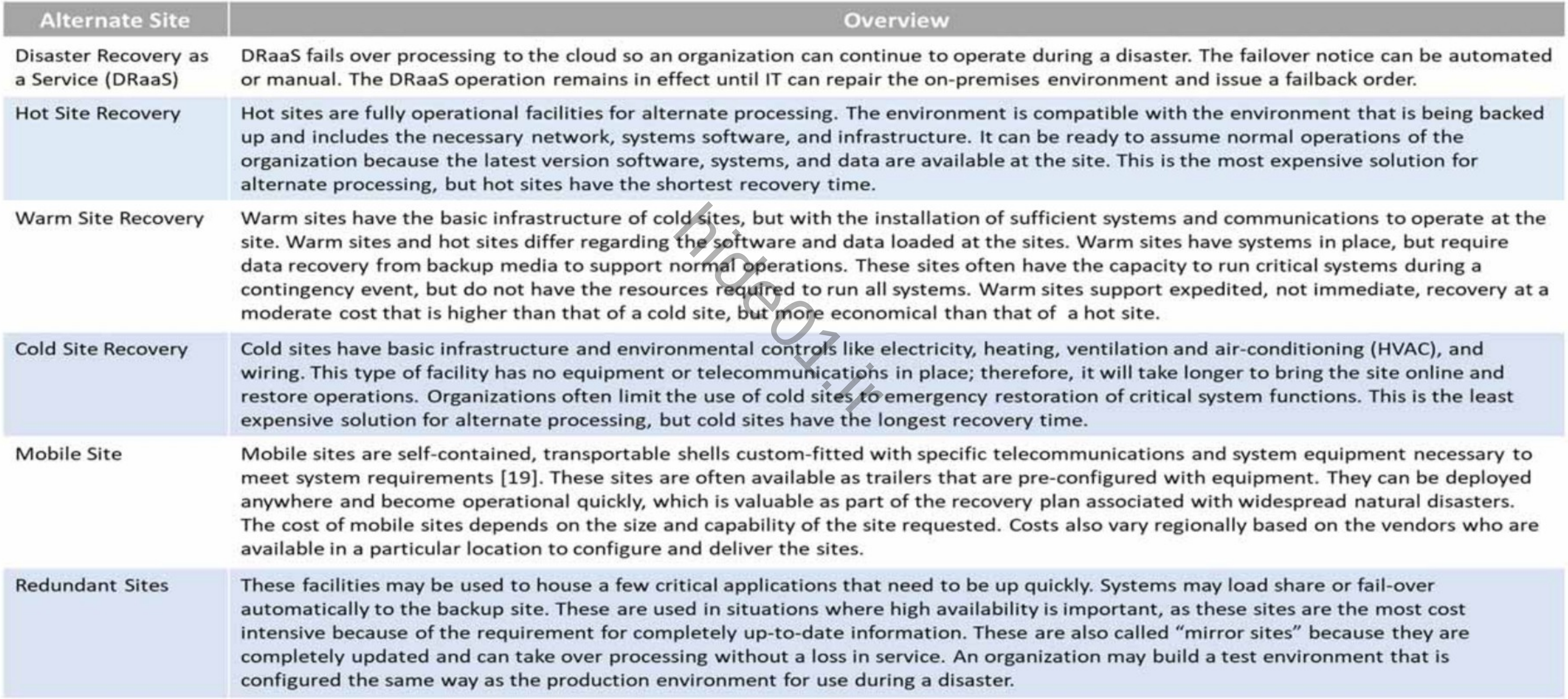
1.11.2 DISASTER RECOVERY PLANNING (DRP)

- The Disaster Recovery Plan (DRP) traditionally focuses on the sequence of activities required to restore IT systems to an operational state after a major outage or adverse event.
- Execution of the DRP ensures that the IT infrastructure is recovered to a point where the business can continue to run.
- Continued operations may occur at an alternate processing site or at reduced operational support capacity.

1.11.2 DISASTER RECOVERY PLANNING (DRP) - CONTINUED

- Alternate processing sites enabling restoration of systems is a common DRP strategy.
- Organizations can set aside space in their facilities to support alternate processing, or they can partner with another organization that specializes in providing alternate sites.
- The three common sites for alternate processing include hot sites, warm sites, and cold sites.
- Each type has unique benefits and considerations that organizations must evaluate to identify the best solution to support DRP needs.

1.11.2 DISASTER RECOVERY PLANNING (DRP) - CONTINUED



Alternate Site	Overview
Disaster Recovery as a Service (DRaaS)	DRaaS fails over processing to the cloud so an organization can continue to operate during a disaster. The failover notice can be automated or manual. The DRaaS operation remains in effect until IT can repair the on-premises environment and issue a failback order.
Hot Site Recovery	Hot sites are fully operational facilities for alternate processing. The environment is compatible with the environment that is being backed up and includes the necessary network, systems software, and infrastructure. It can be ready to assume normal operations of the organization because the latest version software, systems, and data are available at the site. This is the most expensive solution for alternate processing, but hot sites have the shortest recovery time.
Warm Site Recovery	Warm sites have the basic infrastructure of cold sites, but with the installation of sufficient systems and communications to operate at the site. Warm sites and hot sites differ regarding the software and data loaded at the sites. Warm sites have systems in place, but require data recovery from backup media to support normal operations. These sites often have the capacity to run critical systems during a contingency event, but do not have the resources required to run all systems. Warm sites support expedited, not immediate, recovery at a moderate cost that is higher than that of a cold site, but more economical than that of a hot site.
Cold Site Recovery	Cold sites have basic infrastructure and environmental controls like electricity, heating, ventilation and air-conditioning (HVAC), and wiring. This type of facility has no equipment or telecommunications in place; therefore, it will take longer to bring the site online and restore operations. Organizations often limit the use of cold sites to emergency restoration of critical system functions. This is the least expensive solution for alternate processing, but cold sites have the longest recovery time.
Mobile Site	Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements [19]. These sites are often available as trailers that are pre-configured with equipment. They can be deployed anywhere and become operational quickly, which is valuable as part of the recovery plan associated with widespread natural disasters. The cost of mobile sites depends on the size and capability of the site requested. Costs also vary regionally based on the vendors who are available in a particular location to configure and deliver the sites.
Redundant Sites	These facilities may be used to house a few critical applications that need to be up quickly. Systems may load share or fail-over automatically to the backup site. These are used in situations where high availability is important, as these sites are the most cost intensive because of the requirement for completely up-to-date information. These are also called “mirror sites” because they are completely updated and can take over processing without a loss in service. An organization may build a test environment that is configured the same way as the production environment for use during a disaster.

Recovery Site Overview

1.12 CONTINUITY OF SECURITY OPERATIONS

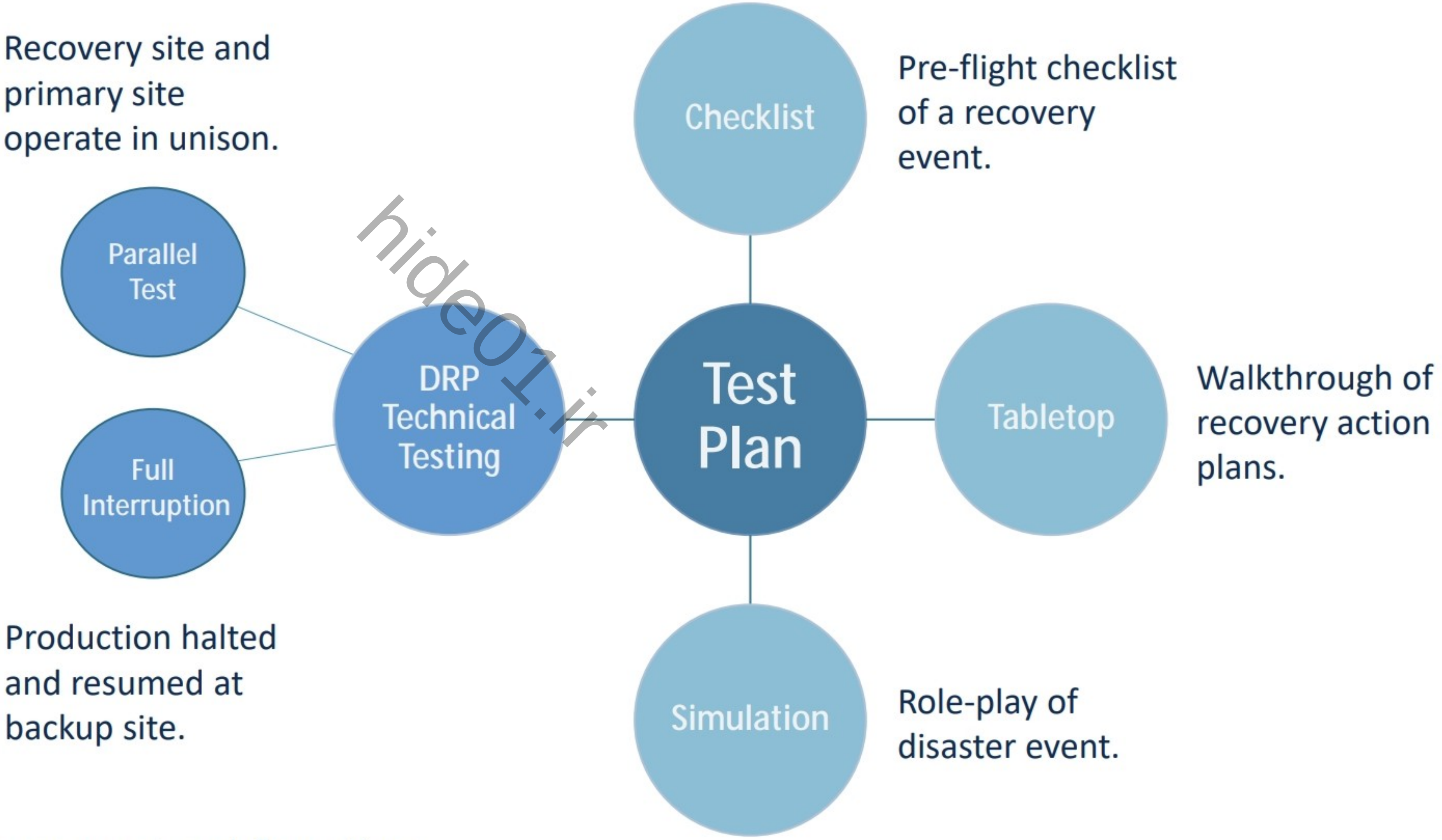
- CISOs should determine how the continuity of information security services are integrated within DRP or BCP processes.
- In the absence of formal business continuity and disaster recovery planning, it should be assumed that information security requirements remain the same in adverse situations as in normal business operations.

1.13 BCM PLAN TESTING

- Testing BCM plans and practicing execution increases the probability of successful recovery during an actual event.
- There are several methods for testing.
    - These range from basic walk-thru events involving minimal expense to full cutover tests, where the operations are intentionally interrupted.

1.13 BCM PLAN TESTING - CONTINUED

Types of Business Continuity Tests



Recovery site and primary site operate in unison.

Parallel Test

Full Interruption

Production halted and resumed at backup site.

DRP Technical Testing

Test Plan

Checklist

Pre-flight checklist of a recovery event.

Tabletop

Walkthrough of recovery action plans.

Simulation

Role-play of disaster event.

1.14 DRP TESTING

Datacenter recovery testing typically includes 2 types of tests:

- Parallel Test – testing of backup processing without disrupting current business processes.
- Full Interruption – shutting own of production and failover to a recovery center

1.15 CONTINGENCY PLANNING, OPERATIONS, AND TESTING PROGRAMS TO MITIGATE RISK AND MEET SLAS

Service Level Agreements (SLAs)

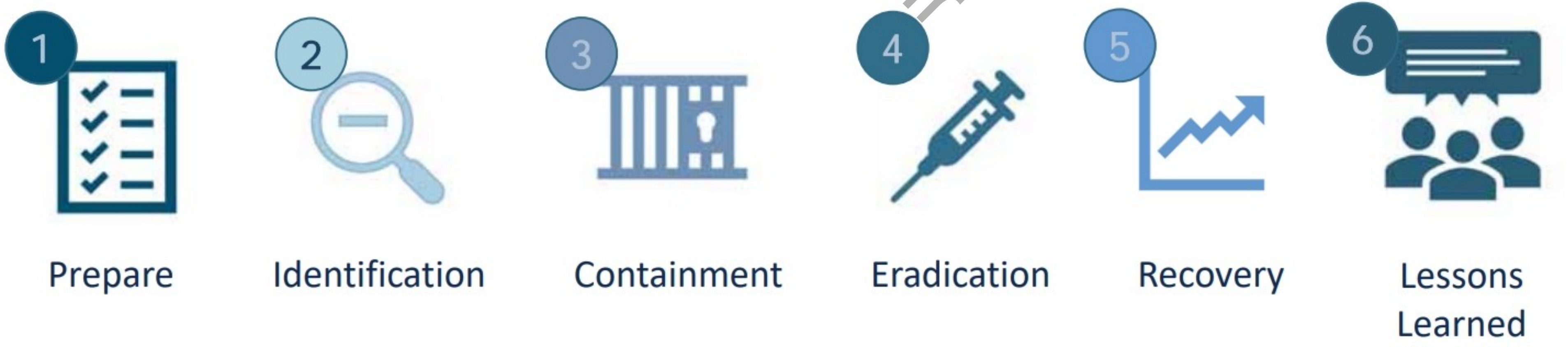
- SLAs define acceptable outages within an IT environment.
- CIOs are evaluated by how well they meet SLA agreements with the business or external customers.
- IT outages adversely affect SLA agreements.
- IT outages are risks requiring risk treatments.
- The security program can also have SLAs defined for security services to the business and customers.

1.16 COMPUTER INCIDENT RESPONSE PLANNING

Incident response requires a comprehensive approach that begins with preparing for, identifying, and containing incidents.

The response continues through eradication and recovery, to include after-action reviews.

* details on slide 75



1.17.1 CRISIS MANAGEMENT

- Most, if not all, crisis management processes and procedures are an integral part of the business continuity program.
- Incident response is a subset of crisis management.
- Digital forensics is not always performed but are typically integrated with event and incident planning.
- Internal and external emergency communications are a core part of crisis management that require planning and role identification.
- There are third party vendors that specialize in managing critical events. They can be put on retainer or contracted as-needed.

1.16.1 INCIDENT RESPONSE TOOLS

- Security Information and Event Management (SIEM) is a core technology for identifying events and incidents using system logs.
- The CISO should also consider other tools to support response and recovery activities such as:
  - Laptops with security analyzer software.
  - Forensic workstations.
  - Storage and replication solutions.
  - Network security equipment.
  - Log analyzers.
  - Evidence tape.
  - Tags and storage.

1.16.2 INCIDENT RESPONSE MANAGEMENT

- Incident analysis is the basis of an organization's ability to effectively determine the cause of security incidents.
- Computer security incidents are often complex, multifaceted problems that require advanced analysis of technical details to understand what happened, find the root cause, and identify remediation steps for recovery and response.
- The goal of analysis is to identify the impact of an incident and escalate accordingly to accomplish timely remediation.
- The impact to the business will define the incident response priority with current activities and needs being managed by the security operations team.

1.16.3 INCIDENT RESPONSE COMMUNICATIONS

- **Internal Incident Communication:**

  Effective internal communication is critical for keeping personnel informed and reducing anxiety during an incident,

- **External Incident Communication:**

  Organizations should develop a strategy for communication with emergency responders and conduct incident management in a manner that supports legal action or criminal investigations if necessary.

  Organizations should also plan communication with the media for effective public relations management.

1.16.4 POST-INCIDENT ANALYSIS

- Post-incident analysis provides an opportunity to evaluate the effectiveness of event management and incident response procedures.
- Post-event reviews allow staff to discuss root cause, lessons learned, and ways to improve processes.
- The CISO is ultimately responsible to assure these types of historical lessons are not lost.
  - Wherever practical, provide after-action reviews for other portfolio services such as risk assessments, threat management, etc.
  - Think CIP – Continuous Improvement Program.

1.16.5 TESTING INCIDENT RESPONSE PROCEDURES

- The following list can aid for planning and executing an incident response test:
  - Select a scenario that poses the greatest risk to the organization.
  - Add as much realism as possible.
  - Ensure members of the incident response team only use procedures documented in the incident response plan.
  - Document plan variances that occur during the test.
  - Determine if cross-training is necessary to ensure the plan does not rely on a single person.
    - The test can have a secondary goal of providing cross-training for critical roles.

1.17 DIGITAL FORENSICS

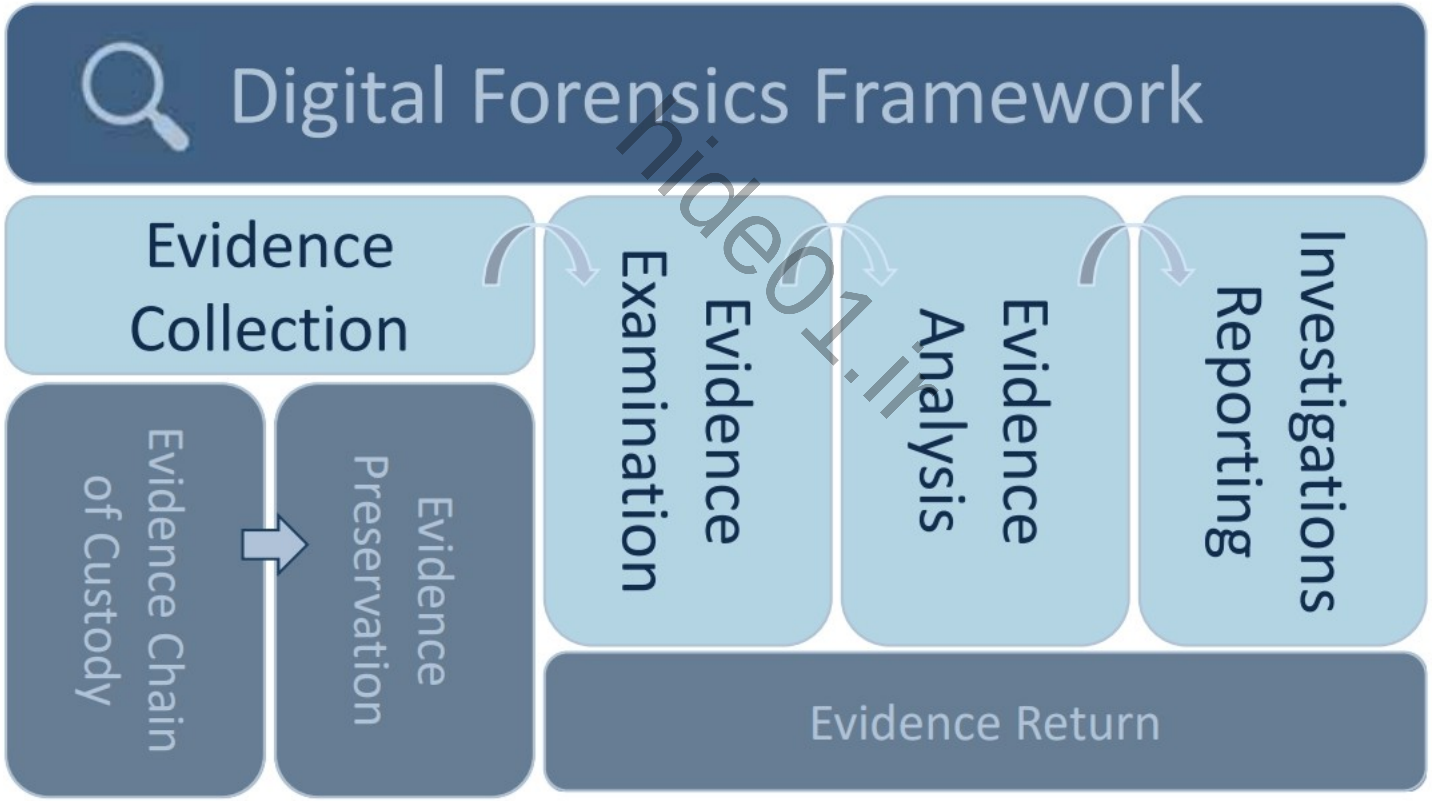
- Digital forensics provides processes for methodical investigation and preservation of evidence.
- It is typically accomplished during all incident management processes to determine root cause.
- Digital forensics is always used to support litigation or assist with law enforcement efforts.
- Decision points to initiate digital forensic actions are typically integrated within incident response processes.
- Digital forensics output is also valuable for integration into after-action analysis for continuous program improvement.

1.17.2 DIGITAL FORENSICS LIFE CYCLE

- The National Institute of Standards and Technology (NIST) defines four phases in the digital forensics process:
  - Collection.
  - Examination.
  - Analysis.
  - Reporting.
- Each phase defines distinct activities for the digital forensic investigation process.

1.17.2 DIGITAL FORENSICS LIFE CYCLE - CONTINUED

The following framework provides guidance in formulating your information security program's digital forensics program.



Digital Forensics Framework

1.17.2 DIGITAL FORENSICS LIFE CYCLE (CONTINUED)

Evidence Collection: The organization determines the intent of the investigation before starting the collection process. Evidence is identified and protected.

Chain of Custody: Each collection step and interaction with the evidence is recorded to maintain chain of custody. Chain of custody refers to the documented record that provides accountability for each step of the handling process.

Evidence Preservation: The evidence is collected a manner that prevents inadvertent changes. Processes should exist that define methods to safely acquire or copy data.

1.17.2 DIGITAL FORENSICS LIFE CYCLE (CONTINUED)

Evidence Examination: The second phase of the digital forensics process is examination. Files marked for further analysis are identified during this phase.

Evidence Analysis: The third phase of the digital forensics process is analysis. The goal is to determine historical knowledge.

- What occurred?
- Who was involved?
- When did it occur?
- Where did the action originate and what was the resulting impact?
- How was it accomplished?

1.17.2 DIGITAL FORENSICS LIFE CYCLE - CONTINUED

Investigation Reporting: In this phase, a report is created detailing the information that was collected, how the investigation was accomplished, event details, and the outcomes or changes that occurred as a result of this incident.

Evidence Return: This requires returning of the physical and digital sources back to rightful owners.

2. OPERATIONS MANAGEMENT

2.1 ESTABLISHING AND OPERATING A SECURITY OPERATIONS (SECOPS) CAPABILITY

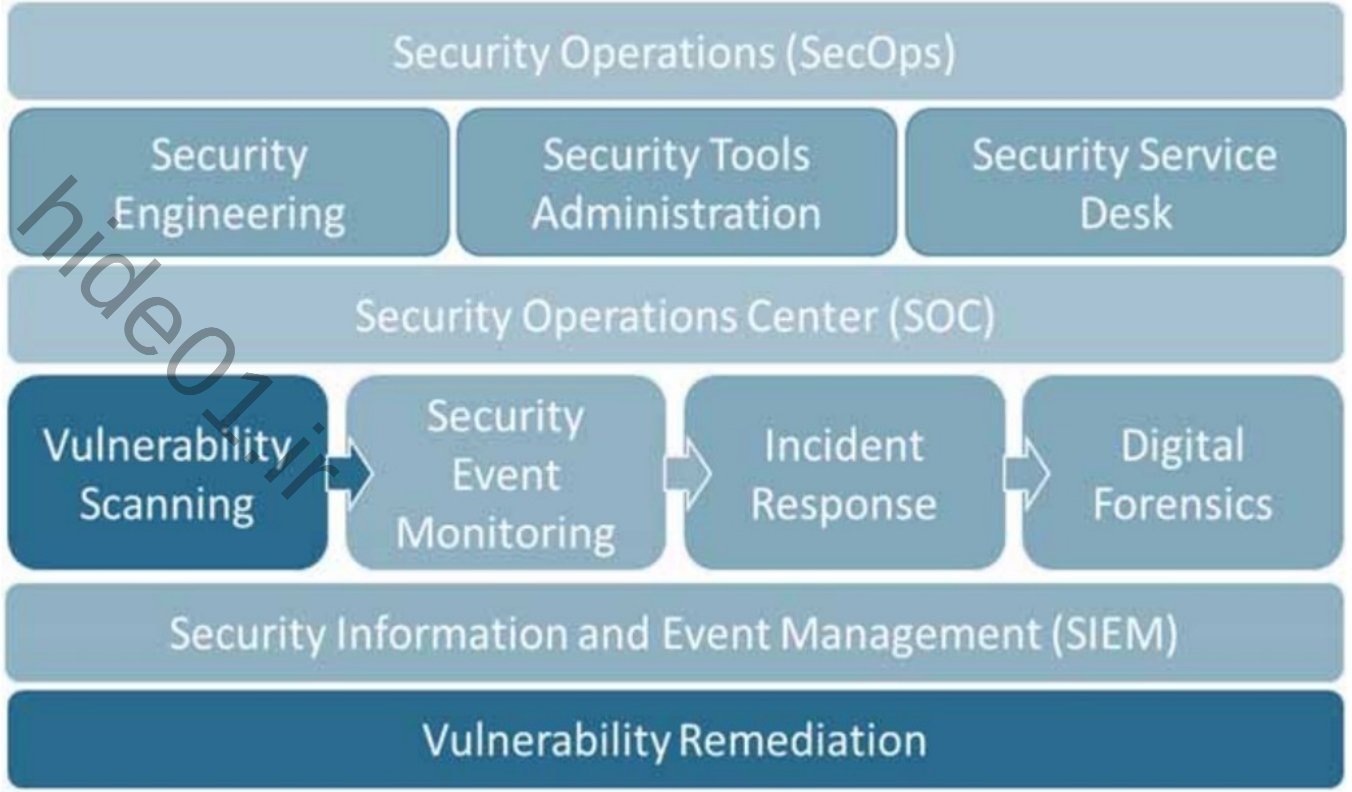
- Security operations is one of the more important programs within the information security portfolio.

- This program orchestrates people, processes, and technologies to deliver technical security services such as systems monitoring, anomaly research, event identification, incident response, and digital forensics.

2.1 ESTABLISHING AND OPERATING A SECURITY OPERATIONS (SECOPS) CAPABILITY

These capabilities can be performed by internal resources or outsourced to a third party.

How the model is deployed is based on the organization's needs and resource availability.


Security Operations (SecOps)
Security Engineering
Security Tools Administration
Security Service Desk
Security Operations Center (SOC)
Vulnerability Scanning
Security Event Monitoring
Incident Response
Digital Forensics
Security Information and Event Management (SIEM)
Vulnerability Remediation

SecOps Framework

2.1 ESTABLISHING AND OPERATING A SECURITY OPERATIONS (SECOPS) CAPABILITY

Security Engineering provides security tool planning, deployment, and management to fulfill the mission of the SecOps team.

Security Tools Administration deals with daily operational support of cybersecurity technology and troubleshooting operational issues. This can reside inside of the SecOps team or with the IT team, depending on the deployment strategy.

Security Service Desk provides user support for security technology, user device virus infections, and access administration.

2.1 SECURITY ENGINEERING PRINCIPLES

Principle 1 - establish a sound security policy as the foundation for design.

Principle 2 - treat security as an integral part of the overall system design.

Principle 3 - clearly delineate the physical and logical security boundaries governed by security policies.

Principle 4 - ensure that developers are trained to develop secure software.

Principle 5 - reduce risk to an acceptable level.

Principle 6 - assume that external systems are insecure.

Principle 7 - identify potential trade-offs between adding security and user functionality.

Principle 8 - implement tailored system security measures to meet organizational security goals.

Principle 9 - protect information while it is being processed, in transit, and in storage.

Principle 10 - consider custom products to achieve adequate security.

2.2 SECURITY MONITORING AND SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM is the primary tool used to support the Security Operations Center (SOC).

The SOC typically manages the SIEM, monitors the output, and reacts to anomalies detected by the tool.

Because of CapEx and OpEx concerns, some organizations leverage Managed Security Service Providers (MSSPs) to provide SOC operational support, to include SIEM use and management.

2.2 SECURITY MONITORING AND SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM tools have core functions that are common to all these types of tools.

Collect relevant data about an enterprise's security.

Aggregate information from multiple locations.

Correlation of information for analysis.

Present information simply to allow rapid identification of potential issues.

2.2 SIEM USE CASES

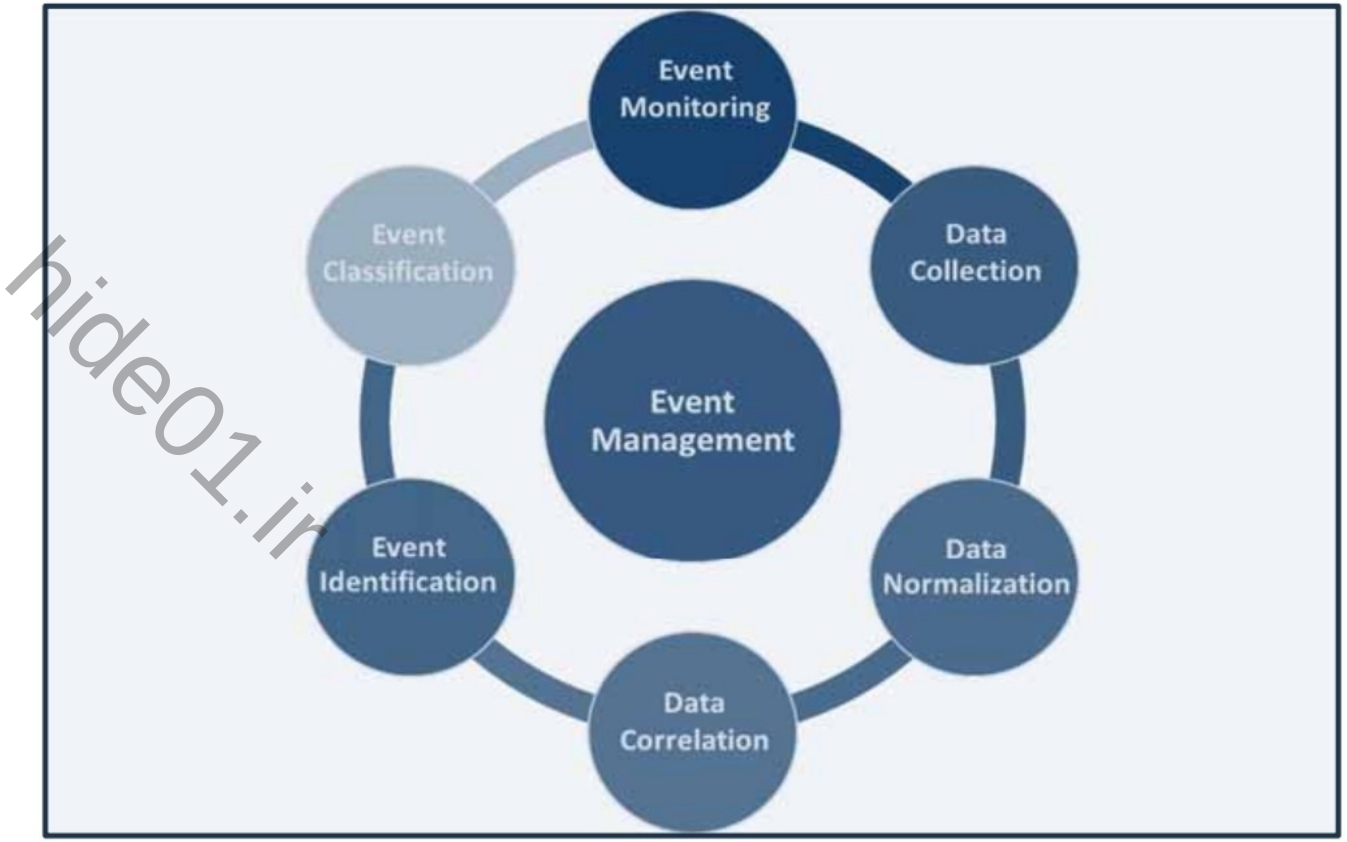
Use cases provide a focused approach to choose detection processes, evaluate detection and response capabilities, and train personnel.

Developing SIEM Use Cases

- Define the scope of the SIEM solution.
- Define the requirements via use cases and identify intended outcomes.
- Validate event sources that support use cases.
- Define the logic of the alert and the associated attack vectors.
- Conduct implementation and testing to confirm the SIEM produces the intended result.
- Define response procedures.
- Conduct SIEM solution reviews for continuous improvement and tuning.

2.3 EVENT MANAGEMENT

Event management follows a systematic process that begins with monitoring or searching for events and ends with classifying events.



Event Management Model

2.3 EVENT MANAGEMENT

Event Monitoring:

- IT environments present a challenge for event monitoring due to the volume of information and complexity of systems.
- The CISO should use automated tools to support effective event monitoring and detection. Examples include:
    - Security log aggregators and filters.
    - Normalized events through baseline creation – identify normal activities within the enterprise for easier identification of anomalies.
    - Generation of alerts that are routed to response individuals when suspicious or anomalous activity has been identified.

2.3 EVENT MANAGEMENT

Data Collection

- SOC data collection describes the systematic approach used by the organization to gather timely and relevant information about the enterprise.
- The CISO must develop a strategy to ensure collected information is sufficient for identification and analysis of issues.

Data Normalization

- Normalization allows analysis and identification tools to use standardized queries and data structure input to evaluate data from multiple sources and isolate signs of anomalous or malicious activity.
- Because normalization transforms data, the CISO should develop a strategy to obtain original data if additional investigation is necessary.

2.3 EVENT MANAGEMENT

Identification

- Identifying the type of event and assigning a category supports the subsequent event management and incident response processes.
- The CISO must define what distinguishes an incident from an event.

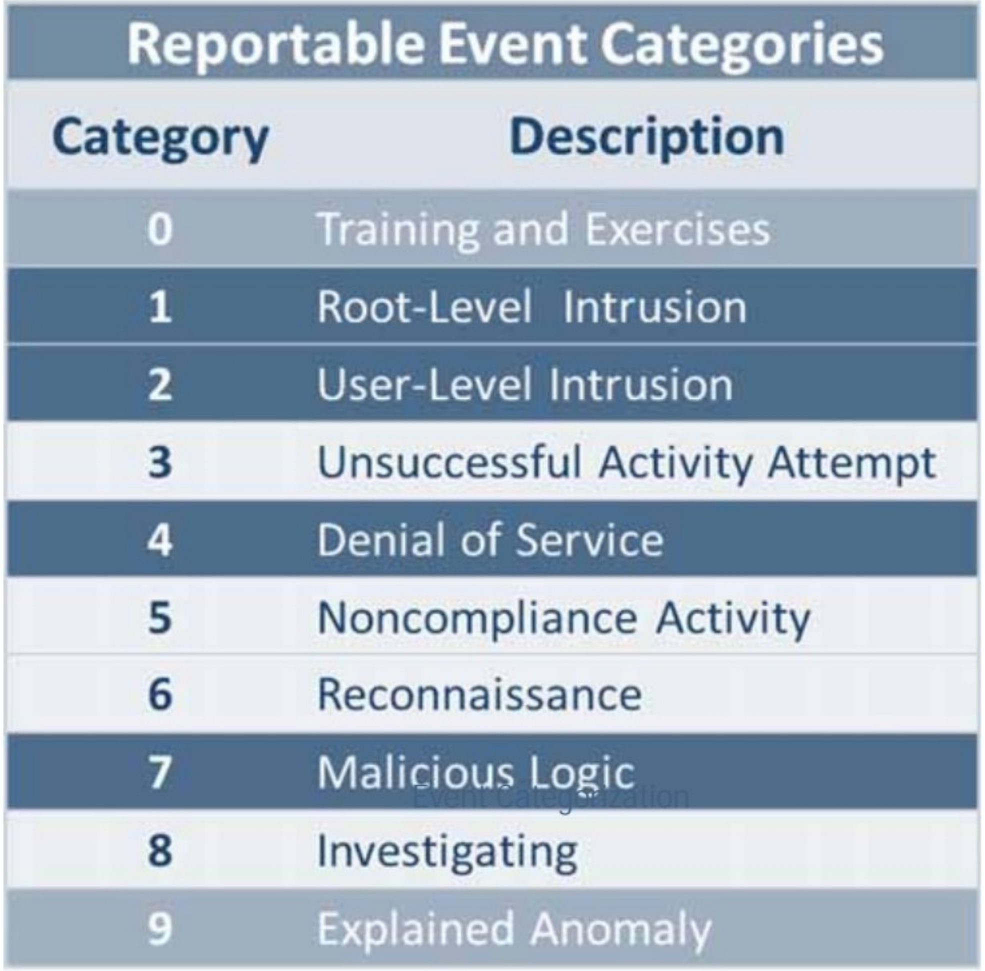
Classification

- This is often based on the type and impact of the threat.
- It includes assessing, prioritizing, and relating events to other potential incidents and events.
- With proper context, events can be categorized based on criticality, impact, and the relationship to other events being managed by the security operations team.

2.3 EVENT MANAGEMENT

This table provides an example of events and incidents defined by the US Department of Defense.

It highlights the value of categories mapped to a description of the event or incident.



Reportable Event Categories	
Category	**Description**
0	Training and Exercises
1	Root-Level Intrusion
2	User-Level Intrusion
3	Unsuccessful Activity Attempt
4	Denial of Service
5	Noncompliance Activity
6	Reconnaissance
7	Malicious Logic
8	Investigating
9	Explained Anomaly

Event Categorization

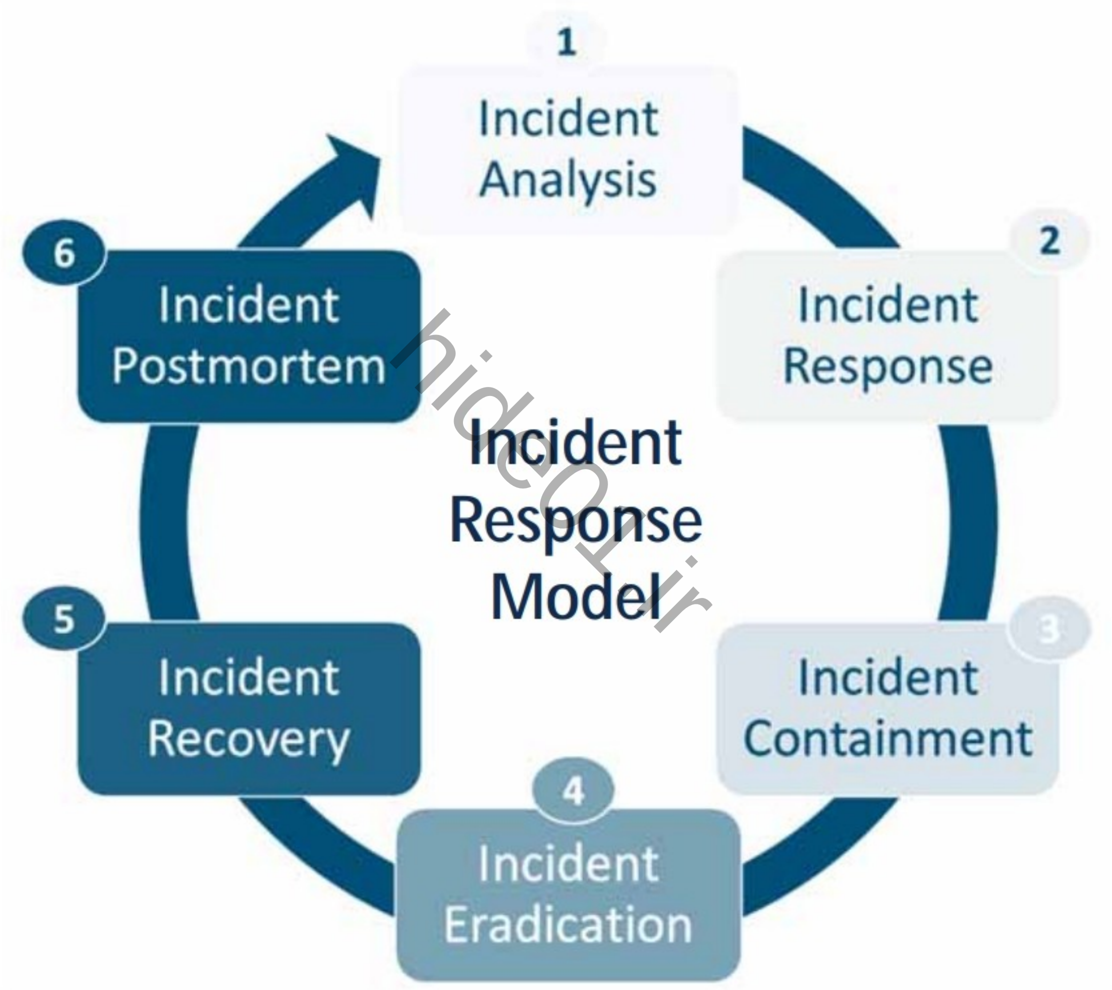
2.4 INCIDENT RESPONSE MODEL

- Incident response is an organized approach for managing the aftermath of a security breach or cyberattack.

- The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

- Although there are several variations in incident response approaches, they all tend to follow six basic phases.

2.4 INCIDENT RESPONSE MODEL



Incident Response Model

2.4 INCIDENT RESPONSE MODEL PHASES

Phase 1 Incident Analysis - forms the basis of an organization's ability to respond effectively to computer security incidents.

Phase 2 Incident Response - defines the tasks of individuals involved in the response.

Phase 3 Incident Containment - provides limiting the extent of the attack or breach and potential losses.

2.4 INCIDENT RESPONSE MODEL PHASES (CONTINUED)

Phase 4 Incident Eradication - defines the process of eliminating the cause of the incident.

Phase 5 Incident Recovery - defines the steps required to return the affected systems or services to their normal state of operations.

Phase 6: **Incident Postmortem** - provides an opportunity to evaluate the event management and incident response procedures in the organization in support of continual improvement.

2.4.1 DEVELOPING INCIDENT RESPONSE SCENARIOS

Incident response plans generally provide specific response approaches to some of the more common or likely incidents.

These are also known as incident response play books.

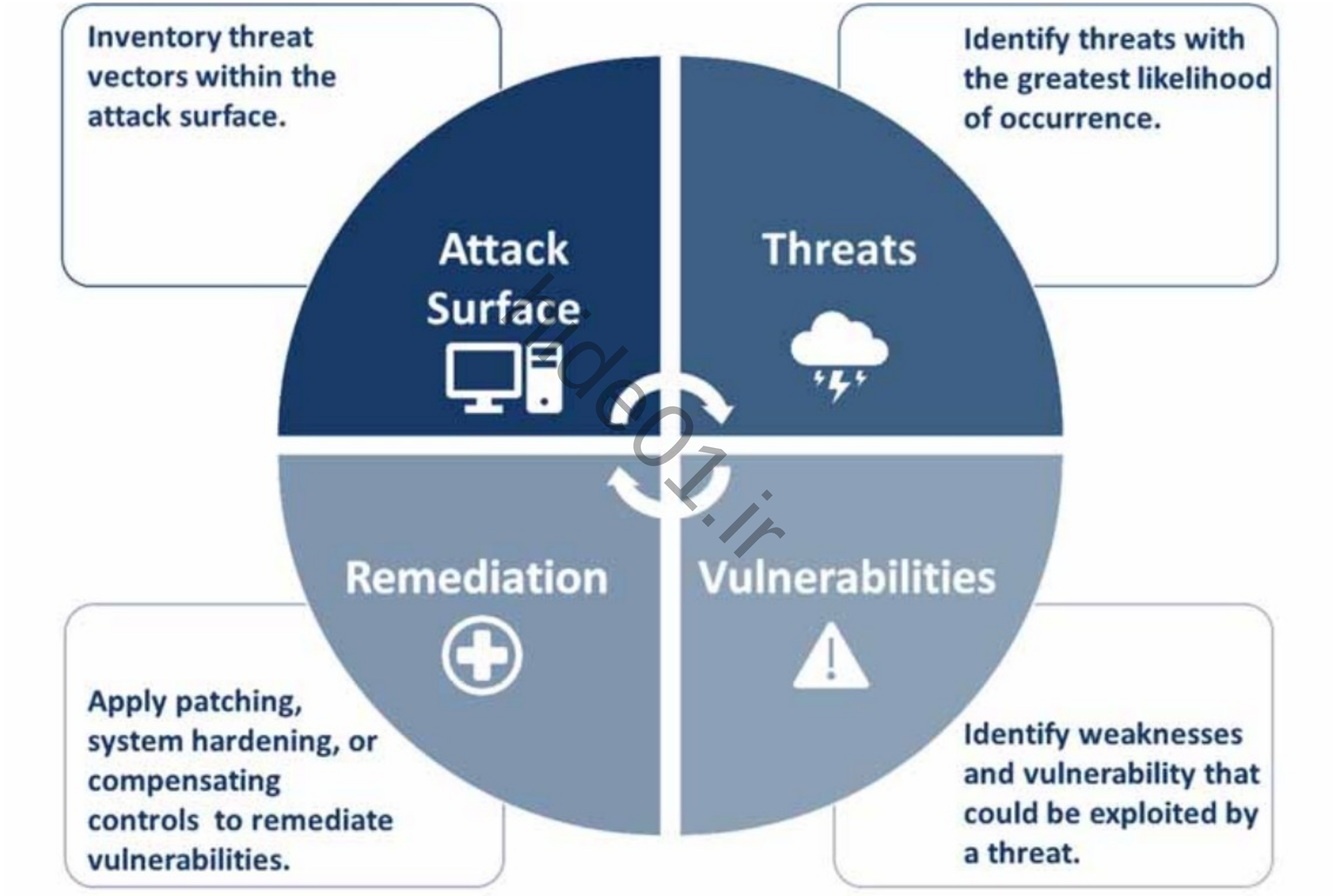
The following are some of the most common response scenarios:

- Insider threat.
- Identity theft.
- Mobile device loss or theft.
- Phishing and spear-phishing attacks.
- Ransomware.
- Social engineering.

2.5 THREAT MANAGEMENT

- Threat management begins by identifying and understanding who or what can harm an organization.
- Understanding threats and their sources is the focus of a threat management strategy.
- Once the threats are understood, the CISO determines the likelihood of a threat exploiting a vulnerable system or process.
- The conclusion of this process is an opportunity to rank and prioritize mitigations and controls to limit the damage that could be caused by identified threats.

2.5 THREAT MANAGEMENT MODEL


Inventory threat vectors within the attack surface.
Identify threats with the greatest likelihood of occurrence.
Attack Surface
Threats
Remediation
Vulnerabilities
Apply patching, system hardening, or compensating controls to remediate vulnerabilities.
Identify weaknesses and vulnerability that could be exploited by a threat.

Threat Management Model

2.5 THREAT MANAGEMENT: ORIGINS

- **External Threats**: cybercriminals often focus on the remote exploitation of systems to yield significant information and value to themselves.
- **Insider Threats**: Insider threats include the intentional and unintentional actions by employees that can harm an organization.

2.6 THREAT INTELLIGENCE

- Actionable intelligence is key to guiding threat management investments and program decisions.
- Organizations can subscribe to external threat intelligence services to aid in their threat identification and decision-making process.
- Threat intelligence sources include:
  - SIEM tools, can be internal or supplied buy third parties (managed services).
  - Honeynets and honeypots, typically within your infrastructure.
  - Information Sharing and Analysis Center (ISAC).
  - Open-Source Intelligence Feeds (OSINT).
  - Threat Intelligence Subscriptions.

2.6.1 INFORMATION SHARING AND ANALYSIS CENTERS (ISAC)

- ISACs collect, analyze and disseminate actionable threat information to their members and provide advice or tools to mitigate risks and enhance resiliency.
- The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998
  - The us federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities.
- Currently 27 ISACs share threat intelligence for a variety of sectors

https://www.nationalisacs.org/

2.7 VULNERABILITY MANAGEMENT

- Vulnerability management reduces the likelihood that threat actors can exploit weaknesses in the IT architecture.
- The CISO should ensure that vulnerabilities are identified in the platforms used by the organization.
- Scanning tools are typically used to determine if known vulnerabilities exist within IT systems.
- Vulnerability management includes prioritization of vulnerabilities according to ease of exploit, exploit criticality, and potential impact if exploited.
- Vulnerabilities cannot be completely mitigated due to financial, technical, and business constraints.

2.7.1 VULNERABILITY ASSESSMENTS

There are many types of vulnerability identification tools and methods for detecting system weakness.

- Cloud-based vulnerability assessment solutions.
- On-premise vulnerability assessment platforms.
- Continuous vulnerability scanning and assessment methods.
- Credential-based vulnerability assessments, scans without credentials, or a mix of both.

2.7.1 VULNERABILITY ASSESSMENTS

- Vulnerability assessments are typically performed using software tools, such as scanners, to identify weaknesses in systems.
- Findings from the assessment help to develop a remediation strategy to eliminate or reduce vulnerabilities before exploitation.
- Examples of factors that inhibit vulnerability mitigation include:
  - Business pressures.
  - IT resource constraints.
  - IT system interdependencies
  - Funding.
  - Time.
  - Planned infrastructure changes.

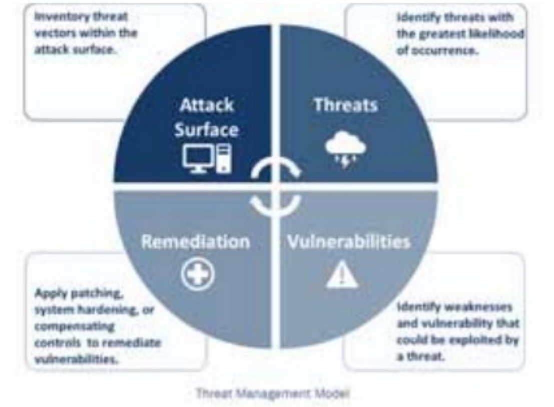
2.7.2 VULNERABILITY MANAGEMENT

- An attack that exploits numerous low vulnerabilities could have the same impact on the organization as a single attack that exploits a moderate or a high vulnerability.
- The three common approaches used for vulnerability identification and management are:
  - Vulnerability assessment.
  - Penetration testing.
  - Patch management.

2.7.2 VULNERABILITY MANAGEMENT IN PRACTICE

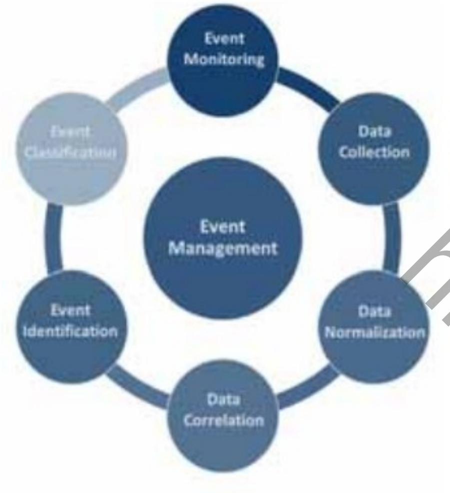
- Vulnerability management programs vary between organizations.
- There is usually a direct correlation between the effectiveness of vulnerability management and the maturity of a security organization.
- An effective vulnerability management program will rely on:
  - Organizational policies defining the vulnerability management program and the expectations of the program.
  - Accurate and effective asset management.
  - Mature, process-driven change management.
  - Organizational executive support, which can be difficult when starting a new vulnerability management program (think of IT resource and business needs).

2.7.2 PUTTING IT ALL TOGETHER


Inventory threat vectors within the attack surface.
Identify threats with the greatest likelihood of occurrence.
Attack Surface
Threats
Remediation
Vulnerabilities
Apply patching, system hardening, or compensating controls to remediate vulnerabilities.
Identify weaknesses and vulnerability that could be exploited by a threat.

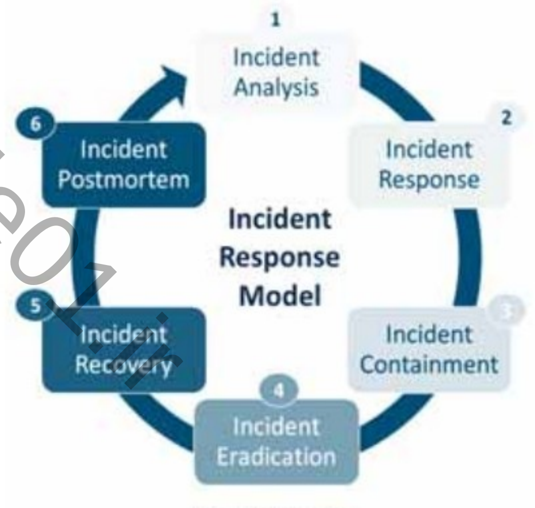
Threat Management Model

What could hurt us?



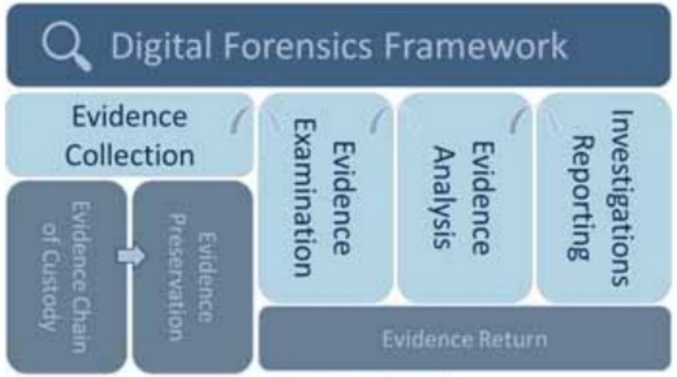
Event Management Model

Is anybody trying?



Incident Response Model

Can we make them stop?



Digital Forensics Framework

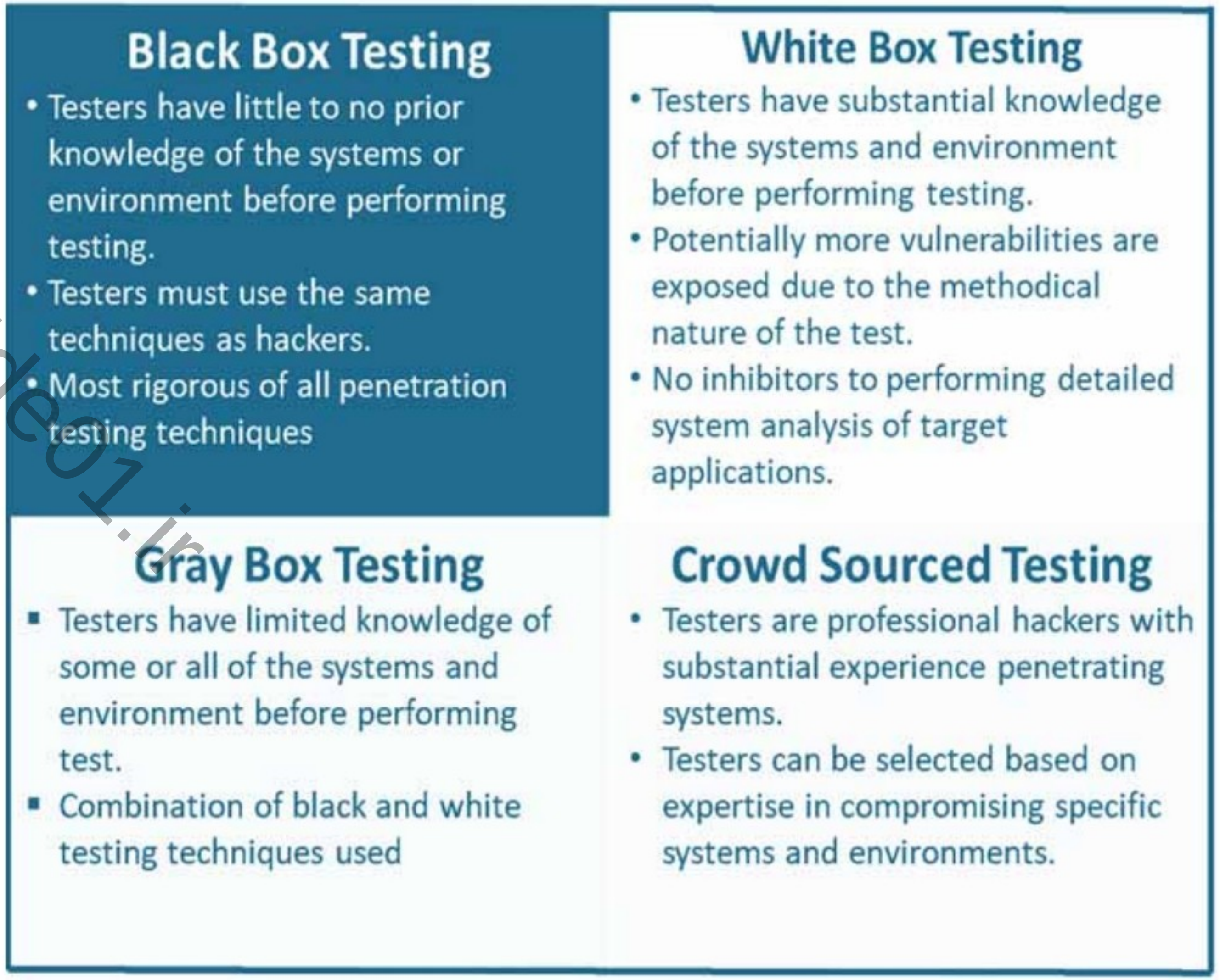
Who did what?

2.7.3 PENETRATION TESTING

- Penetration testing is the process of attempting to gain access to resources.
- Penetration tests discover information system flaws that might not be identified by vulnerability scans and assessments.
- Periodic penetration tests are useful for discovering information system design or implementation flaws.
- Because of the potential to disrupt operations, testing should be performed carefully and only after obtaining prior written permission from asset owners.

2.7.3 PENETRATION TESTING

Penetration testing can occur in the form of external or internal tests and can be conducted by employees or third parties.



Black Box Testing

- Testers have little to no prior knowledge of the systems or environment before performing testing.
- Testers must use the same techniques as hackers.
- Most rigorous of all penetration testing techniques

White Box Testing

- Testers have substantial knowledge of the systems and environment before performing testing.
- Potentially more vulnerabilities are exposed due to the methodical nature of the test.
- No inhibitors to performing detailed system analysis of target applications.

Gray Box Testing

- Testers have limited knowledge of some or all of the systems and environment before performing test.
- Combination of black and white testing techniques used

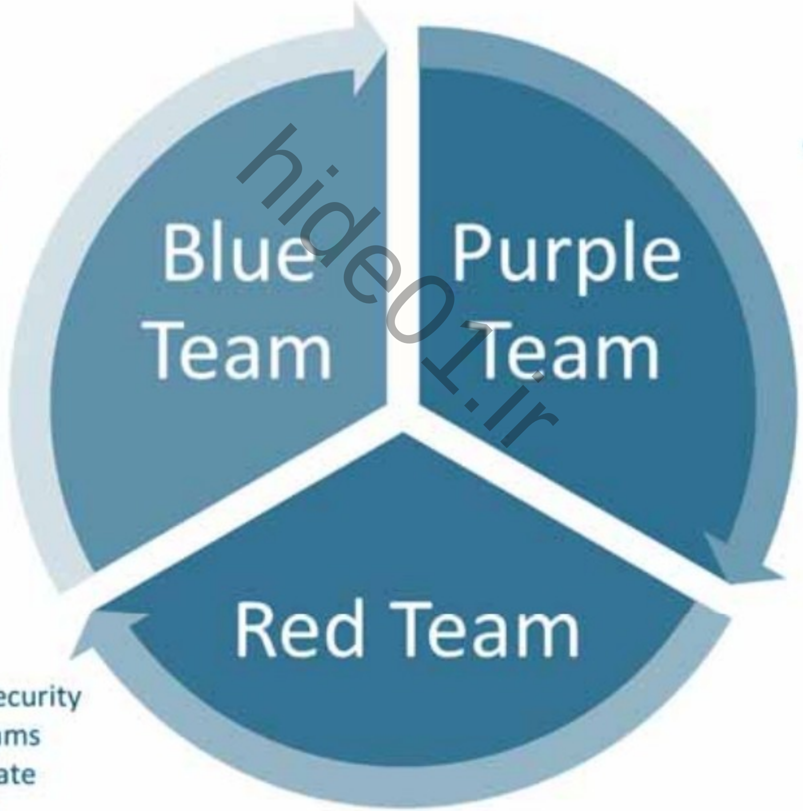
Crowd Sourced Testing

- Testers are professional hackers with substantial experience penetrating systems.
- Testers can be selected based on expertise in compromising specific systems and environments.

Penetration Testing Options

2.7.4 SECURITY TESTING TEAMS

There are 3 types of security testing teams



- Defend against Red Team simulated and actual cyberattacks

- Integrate defensive tactics and controls identified through Blue Team to ward off future Red Team attacks

- External security testing teams who emulate hackers to compromise systems

Testing Team Interrelationship Model

2.7.5 REMEDIATION – PATCH MANAGEMENT

- Patch management is a complex activity that requires careful coordination with the business, the project management office, and IT functions.
- The CISO must work closely with each function to create an effective patch management strategy.
- Guidelines for patch management include:
  - Organizations should deploy patch management tools.
  - Patching should be completed in a controlled approach.
  - Asset owners choose between vulnerability or availability.
  - Unpatched systems should be integrated into the risk management program for communication of risk and further monitoring or management.

2.8 THREAT HUNTING

- Threat hunting uses tactics, techniques, and procedures to aggressively search for potential threats within an IT environment.
- The activities conducted by the threat hunting team can also analyze automated tool capabilities and configurations to improve their discovery capabilities.
- Whereas event management and incident response are reactive, threat hunting is proactive.

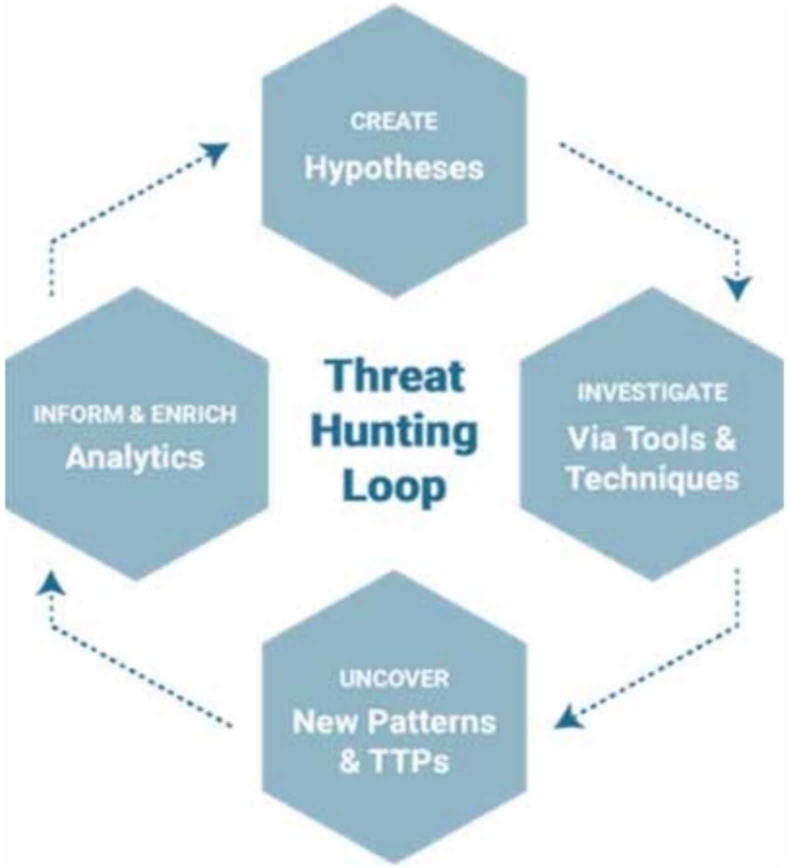
2.8 THREAT HUNTING

Threat hunting mission, strategy, and tactics.

- The goal is to uncover new patterns of behavior related to an unknown attack vector
- The results provide insight for tuning existing security tools to automatically identify attacks more effectively or change processes to thwart attacks.
- 3 primary methods are used for conducting a threat hunt within an IT environment:
  - Exploratory – see what can be found with no prior goals.
  - Structured – analyze a specific target or piece of infrastructure.
  - Guided – know what to generally look for before starting.

2.8 THREAT HUNTING

- The four phases of this Threat Hunting Loop represent an iterative process.
- Each phase produces information that can be used to start new hunts or provide intelligence on existing threats.
- Ideally, once a cycle has been completed, the results of that hunt can be integrated or automated in existing discovery tools.



Amazon Threat Hunting Loop

DOMAIN 3
END

DOMAIN 3 SUMMARY

DOMAIN 3: SUMMARY - GENERAL

- This domain provided an overview of a wide range of CISO activities beginning with creating a strategic plan, to staffing an IS program, to recovering from disasters.
- Many organizations outsource one of more aspects of their SecOps function.
- The largest investment in an IS program will generally be made in the SecOps area.
- CISOs need to oversee security testing of the infrastructure using the results to revise risk communications and enhance key or compensating controls.

DOMAIN 3: SUMMARY - PROGRAM MANAGEMENT

- CISOs juggle a myriad of projects and programs to meet the information security needs of their organizations.
- An information security program is comprised of many sub-programs, projects, and activities.
- Projects are typically contained with programs.
- Projects are typically tactical, whereas programs are strategic.
- Successful projects and programs require stakeholder support.
- Programs are best described in the security program charter.
- Charters assign responsibility, specify resources, and outline constraints.
- CISOs need to be adept at project and program management.

DOMAIN 3: SUMMARY - STRATEGY

- Successful CISOs follow a strategic plan that clearly outlines the mission and objectives of their information security program.
- Strategic security plans must align with the organization's business strategies.
- Strategic plans allow the security function to develop processes and adopt technologies to provide asset protection.
- Developing a business-aligned and functional strategic plan can be one of the most challenging activities of a CISO.
- The security strategy should be available to the business and clearly communicated when created.

DOMAIN 3: SUMMARY - STAFFING

- CISOs must determine the proper types of information security program staffing that takes into consideration the available resources and business support needs.
- Identifying and staffing key roles of the information security program will determine program performance.
- A small number of direct reports allows the CISO to easily adhere to internal HR practices and effectively manage them.
- Training and certifications is a cornerstone for motivating security program personnel.
- CISOs need to provide team members with leadership, not just personnel management.

DOMAIN 3: SUMMARY - USER AWARENESS PROGRAM

- Systems users are the first and last line of defense, they need to be trained to be both.
- Users can act as human firewalls; however, they need to first learn what to look for and how to be a first responder.
- Users learn in different ways; tailor security awareness programs to engage the end user.
- Use awareness training to elevate security participation as part of the organization's culture.

DOMAIN 3: SUMMARY - BCM AND DRP

- CISOs are increasingly asked to oversee business continuity programs to a greater extent and disaster recovery programs to a lesser extent.
- Disaster recovery planning is concerned with the recovery of data and IT technology.
- Business recovery is concerned with continuing critical business functions during a disaster.
- Many leverage points exist between information security, business continuity, and disaster recovery.
- Data recovery requires knowing the organization's RPO and RTO.
- Business impact assessments (BIA) serve as valuable input to risk assessments.

DOMAIN 3: SUMMARY - BCM AND DRP CONTINUED

- ISO publishes a family of BCM standards, the most important of which is ISO 22301.
- Recovery strategies are available in many forms to include cold sites, mobile operations, hot sites, and cloud-based recovery services.
- CISOs need to ensure the security of information and systems while normal operations and functions are impaired.
- Business continuity testing and incident response plans common characteristics but different focus.
- Business continuity and disaster plan testing can consist of tabletop exercises, simple checklist reviews, or full recovery simulations.

DOMAIN 3: SUMMARY - COMPUTER INCIDENT RESPONSE

- Incident response is concerned with the identification, containment, eradication and recovery from computer events and incidents.
- Computer incidents are generally multifaceted and require play books to guide the teams for response actions.
- CISOs typically lead the incident response team, although they are not generally the first responders.
- SecOps function need to provide response for common attacks and outcomes.
- Communications is a key factor for effective incident response; however, need-to-know should prevail throughout an event.
- Incident postmortems provide additional risk management and controls application.

DOMAIN 3: SUMMARY - DIGITAL FORENSICS

- During an incident, digital forensics may be required to determine root cause or gather evidence to support a legal case.
- Digital forensics is concerned with the collection, examination, analysis, and reporting of computer crime or policy violation.
- CISOs must assure evidence protection by provisioning effective chain of custody and evidence preservation processes.
- Many organizations are too small to have their own dedicated digital forensics team. Retainers are often used to secure forensics expertise.
- If an insurance company offers data breach or cyber crime insurance policies, it will typically have forensics resources available to their policy holders. The cost is typically covered by the policy.

DOMAIN 3: SUMMARY - OPERATIONS MANAGEMENT

- Security operations (SecOps) is a core information security program function.
- SecOps is comprised of people, processes and technologies to identify and respond to security events.
- SecOps typically monitors and provides active defense.
- SecOps can include security engineering, tools administration, and security service desk functions.
- SIEM is the primary tool of SecOps and are used to collect, aggregate, correlate, and analyze vast amounts of logs and other data.
- SecOps typically develops SIEM use cases based on organizational risk, and the CISO reviews and approves those use cases.

DOMAIN 3: SUMMARY - EVENT MANAGEMENT

- Event management is the handling of adverse events affecting IT infrastructure and results in the gathering, identifying, and reporting of security-related events.
- SIEM is typically a core tool for event management.
- The volume and velocity of transactions and events within today's IT environment makes sifting through events problematic.
- Automated tools, especially those offering machine learning and Artificial Intelligence (AI), are effective in dealing with large volumes of event data.

DOMAIN 3: SUMMARY - INCIDENT RESPONSE

- Incident response are activities performed by trained SecOps personnel to respond to computer emergencies.
- Many aspects of incident response can be automated to respond to incidents at machine speed. This includes tasks such as closing ports to stop command and control communications.
- Incident response focuses on limiting additional potential damage.
- Incident response is generally integrated with event management.
- CISOs work with SecOps to create play books, which provide response scenarios to address the most critical threats.
- Incident response actions and playbooks are created according to assumption of a breach.

DOMAIN 3: SUMMARY - THREAT MANAGEMENT

- Threat management begins with the identification of actions that can exploit a vulnerability in an IT infrastructure causing impacts.
- CISOs need to separate threats by likelihood, focusing on those threat events posing the greatest probability of damage to the organization.
- A threat inventory or registry provides categorization and management of known threats.
- A threat management model is typically used effectively manage threats.
- CISOs must recognize insider threats can pose an equal or greater level of risk to organizations.
- Threat intelligence sources must be credible and provide actionable information.

DOMAIN 3: SUMMARY - VULNERABILITY MANAGEMENT

- Vulnerability management is concerned with identifying weakness in an IT infrastructure, third party support, end user devices and many other points of attack.
- Vulnerability management is a continuous process whereas an organization's attack surface is monitored for changes that can potentially introduce weaknesses that can be exploited.
- Automation, such as scanning, integrates threat intelligence with vulnerability scanning to quickly identify potential areas of compromise.
- Financial, business, IT resources, and time constraints typically prevent remediation of vulnerabilities.

DOMAIN 3: SUMMARY - PENETRATION TESTING

- Penetration testing is one of the most effective ways to test for network, system or device vulnerabilities.
- Penetration testing can uncover weaknesses that would otherwise go unnoticed.
- Penetration testing can be performed in black, white or grey formats.
- Bug bounty programs have emerged as an effective way of outsourcing or crowd sourcing penetration testing.
- Penetration testing is used as the basis for red teaming where the red team attacks an IT infrastructure, and the blue team defends against the attack.

DOMAIN 3: SUMMARY - PATCH MANAGEMENT

- A key remediation strategy for vulnerability management is patch management.
- CISOs do not generally own the patch management process; however, they must clearly understand process.
- Patch management is typically integrated with change and configuration management processes.
- Many system compromises originate from unpatched devices.
- Risk management can be used to communicate the need for critical patches.

DOMAIN 3: SUMMARY - THREAT HUNTING

- Threat hunting is an active defense strategy to identify areas of potential weakness or existing compromise using the same Tactics, Techniques, and Procedures (TTPs) that hackers use.
- Threat hunting looks beyond known alerts and threats to uncover new or unknown threats and vulnerabilities.
- Penetration teams use threat hunting activities as part of their arsenal of security testing tools.
- Threat hunting is typically performed because the CISO is acting under the 'assumption of breach' viewpoint.

DOMAIN 3 PRACTICE QUESTIONS

PRACTICE QUESTIONS

1. A CISO has a limited budget for security-technology purchases. The desire is to create a tiered security architecture using a phased approach.

Which of the following represents the BEST approach for obtaining the security program's objectives and supporting the organization's security needs?

A. Complete the easiest hardening actions first to demonstrate positive action toward the security goal.

B. Apply technology against the highest target value infrastructure while closely monitoring spending.

C. Install protections on Information Technology (IT) assets experiencing the highest number of intrusive activities.

D. Determine the necessary security-program reporting metrics and apply protections according to monthly report results.

PRACTICE QUESTIONS

2. For a CISO to have true consolidated situational awareness, there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which of the following tools represents the BEST choice to achieve this awareness?

A. Vulnerability scanning system.

B. Intrusion Detection System (IDS).

C. Firewalls.

D. Security Incident Event Management (SIEM).

PRACTICE QUESTIONS

3. What is the **MAIN** responsibility of a Purple Security Testing team?

A. They defend against simulated hacker attacks.

B. They emulate hackers to compromise systems.

C. The integrate the defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team.

D. They oversee security testing and results.

PRACTICE QUESTIONS

4. Your company leverages an employee self-service portal for common human-resource-related tasks such as providing annual tax documents, changing direct-deposit information, and signing up for health benefits. Several employees have complained that they have not received their paychecks this month; everyone else received their paychecks as usual.

What is the MOST likely cause?

A. Their respective financial institutions were compromised right before payroll was deposited and their accounts were emptied.

B. An accounting “glitch” skipped their pay accounts during the payroll audit and failed to issue them a check.

C. They failed to submit their timecards by the deadline.

D. Their company credentials were stolen and used to modify bank routing and account information.

PRACTICE QUESTIONS

5. Controlled phishing campaigns against your own employees:

A. Help you identify areas where you have the potential to improve your training efforts to increase employee resilience against attacks.

B. Target employees that are not following company policy and therefore must be let go.

C. Reduces the amount of time that employees read real fraudulent email and therefore prevents the opportunity to be compromised.

D. Should not be conducted because it desensitizes them to real-world threats, hindering their ability to detect phishing attempts.

C|CISO

CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER

Domain 4

INTRODUCTION

- This domain provides the following topics:
  - Core technical competencies.
  - Building information security technology playbooks.
  - Methods to protect an attack surface.
  - Aligning countermeasures with the OSI Model.
  - Understanding DevSecOps approaches.
  - Security concerns within a cloud computing infrastructure.
  - Security within a virtualized environment.
  - Next-generation security technologies.

KNOWLEDGE ASSUMPTIONS

- Students are expected to have:
  - Five years of experience working around endpoint protection, firewalls, IDS/IPS, SIEM, encryption, etc. technologies.
  - A familiarity of information security technology vocabulary.
  - A basic understanding of network functionality including routers, switches, segmentation, etc.
  - A basic understanding of datacenter operating principles.
  - A basic understanding of cryptosystems.
  - A basic understanding of cloud and virtualized computing.
  - A basic understanding of physical security concepts.

INFORMATION SECURITY CORE COMPETENCIES

DOMAIN 4

GOVERNANCE AND RISK MANAGEMENT

DOMAIN OUTLINE

1. Access Control
2. Physical Security
3. Network Security
4. Endpoint Security
5. Application Security
6. Encryption Technologies
7. Virtualization Security
8. Cloud Computing Security
9. Transformative Technologies

Summary and Practice Questions

1. ACCESS CONTROL

ACCESS CONTROL

- Unauthorized access is one of the primary failure point of security protections.
- Social engineering is the primary tool used to gain unauthorized access.
- Data theft is ranked first as the goal of gaining unauthorized access.
- Access control implementation weaknesses or deficiencies can lead to policy violations and security incidents.

AUTHENTICATION, AUTHORIZATION, AND AUDITING

Authentication, authorization, and auditing (AAA) is the model for articulating how to control access to computer resources.

- **Authentication:** The act of confirming a single piece of data claimed true by an entity. An entity is a person or system. Identity must be authenticated to grant access to assets or resources.
- **Authorization:** Once an identity has been confirmed, the function of specifying access rights to assets and resources is required. Privilege is granted to users.
- **Auditing (Accounting):** Once validated users have authorized access to assets and resources, it is important to monitor and report on how they use the resources to which they have been granted access. This is typically accomplished by logging access and activities associated with systems and applications.

AUTHENTICATION

- **Electronic authentication** is the process of establishing confidence in user identities electronically in an information system.
  - Systems can use the authenticated identity to determine if individuals are authorized to perform activities or system transactions.
- **Authenticator management** involves the processes and procedures for issuing and revoking authenticators.
  - It includes authenticators including passwords, tokens, biometrics, and public key infrastructure (PKI) certificates.

AUTHENTICATION - CONTINUED

The risk of compromised credentials emphasizes the importance of authentication and the need for effective authentication processes.

Identity management defines the process used to identify individuals before granting access to systems, facilities, and resources.

Single-factor authentication maps an authenticator (usually a password or other metric) to an account and facilitates authentication. Account credentials grant access to resources with the rights, privileges, and access associated with that account.

Multifactor authentication maps two or more attributes to an account to facilitate access. This strategy combines something you have, something you know, or something you are in the authentication process.

The CISO should clearly understand the benefits and risks and select the best option that supports the needs and priorities of the organization.

AUTHORIZATION

Authorization defines the process of granting permission to a user or object to perform an action or to obtain something.

Least privilege principle states that users, programs, or processes should only have the minimum privileges necessary to perform its function. For example, an account created for pulling records from a database doesn't need admin rights.

Need to know principle states that access to systems should only be granted to individuals or systems with a legitimate need to know the information contained within those systems. For example, a nurse may only need to know the information on an individual's medical record for assisting a patient.

The CISO's role in authorization is to assure that the security program defines access policies, processes, and procedures.

AUDITING

- Access auditing is essential for compliance and security reporting.
- CISOs should not assume authenticated and authorized users will behave or use information in a proper manner.
- The following outlines the minimum level of user account auditing:
  - Failed data access: when an authorized system or user tries to access restricted information.
  - Privileged accounts performing Create, Read, Update, or Delete (CRUD security matrix) activities.

AUDITING - CONTINUED

The following behaviors should be recorded within an access audit system:

1. User logged on from more than one location simultaneously.
2. Sign-ins while users are on vacation, sick leave, or otherwise absent from work.
3. Inappropriate level of access attempts for job responsibilities.
4. User access lapses of more than 30 days.
5. Suspicious patterns of accesses.
6. Suspicious time and day access.

USER ACCESS CONTROL RESTRICTIONS

- Users can be instrumental in reporting or preventing potential system abuse provided they have adequate tools.
- Access control systems can be deployed to provide users with an automated notification of the following:
  - Last sign in.
  - Unsuccessful sign ins.
  - Concurrent sessions.

USER ACCESS BEHAVIOR MANAGEMENT

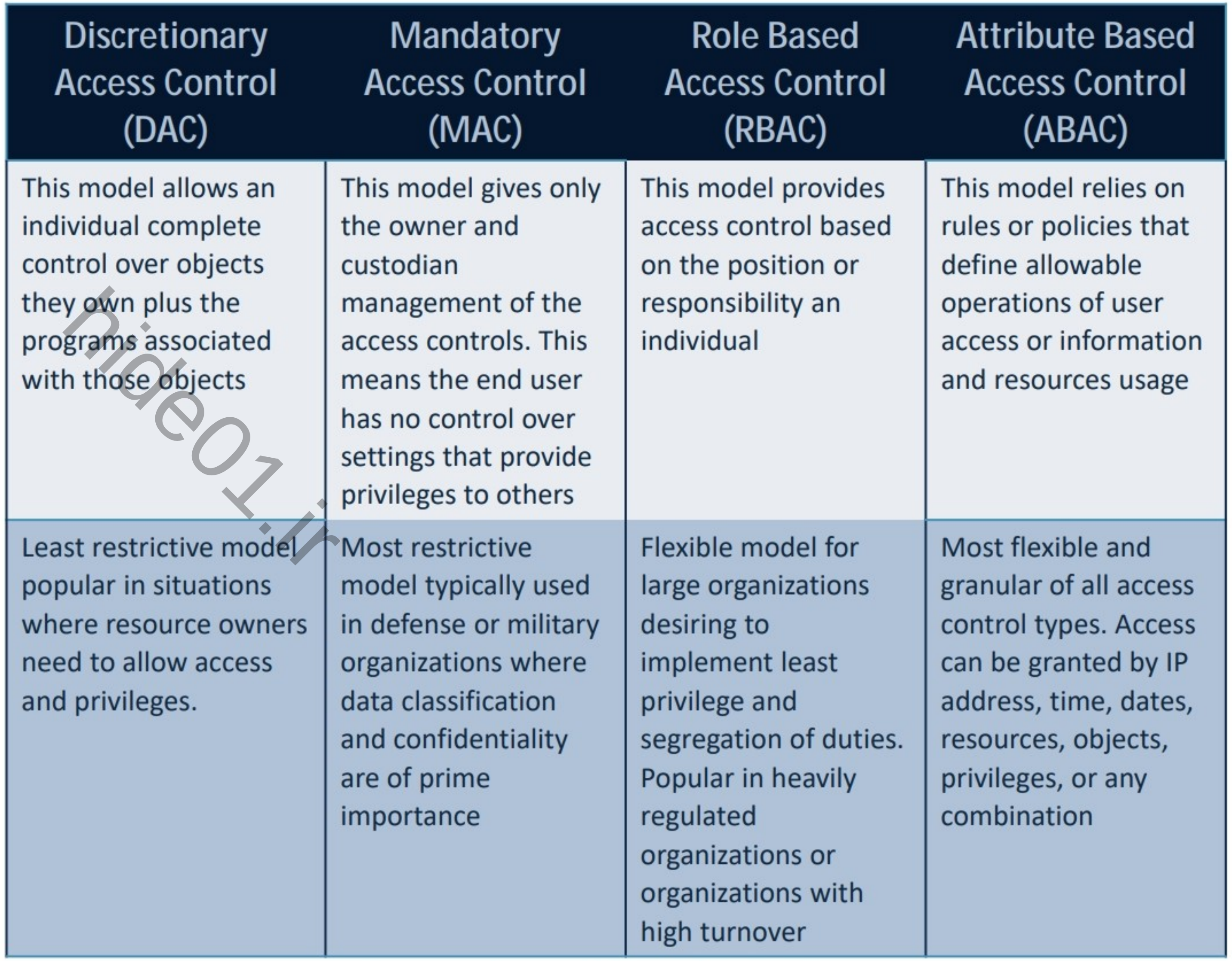
Influencing behavior through system restrictions and awareness are effective messaging that can be used in access control implementations.

Two behavioral management techniques include:

- **Separation of duties** divides the responsibilities associated with an action or process to decrease the opportunity for misbehavior or policy violations through collusion.
- **Banners** that notify the user they are accessing a confidential system and, if they access this system, that they may be subject to monitoring and audits within the system.

TYPES OF ACCESS CONTROL MODELS

- Identity management systems are typically composed of three major elements: users, applications, and policies.
- The following table presents the four most common models of access control models.



Discretionary Access Control (DAC)	Mandatory Access Control (MAC)	Role Based Access Control (RBAC)	Attribute Based Access Control (ABAC)
This model allows an individual complete control over objects they own plus the programs associated with those objects	This model gives only the owner and custodian management of the access controls. This means the end user has no control over settings that provide privileges to others	This model provides access control based on the position or responsibility an individual	This model relies on rules or policies that define allowable operations of user access or information and resources usage
Least restrictive model popular in situations where resource owners need to allow access and privileges.	Most restrictive model typically used in defense or military organizations where data classification and confidentiality are of prime importance	Flexible model for large organizations desiring to implement least privilege and segregation of duties. Popular in heavily regulated organizations or organizations with high turnover	Most flexible and granular of all access control types. Access can be granted by IP address, time, dates, resources, objects, privileges, or any combination

Access Control Type Comparison

DESIGNING AN ACCESS CONTROL PLAN

- An access control plan defines how the organization will implement the objectives defined in the organization's access control policy.
- Developing an access control plan helps the CISO formalize the approach for managing access to IT environments or facilities.
- This plan is typically communicated to the broader organization.

DESIGNING AN ACCESS CONTROL PLAN - CONTINUED

The access control plan should answer the following questions

- What are the access control goals and objectives of the organization?
- What risks will the access control strategy mitigate?
- What account types and security groups are required to support this strategy?
- What are the procedures for authentication, authorization, and access administration, to include provisioning, recertifying, and decommissioning access?
- What unique security policies are required for remote access, system accounts, and system connections?
- What is the relationship between the access control plan and other security program plans?

ACCESS ADMINISTRATION

Access administration is the processes and procedures to manage system users and objects, from provisioning to termination.

Access provisioning establishes the account for a user or object, provides only the access required, and is typically performed using well-documented procedures.

Access monitoring determines if users still require access, and it is particularly critical to verify privileged accounts.

Access termination are the processes to remove access at the conclusion of the need for it. It is typically integrated into the change management or IT ticket system and HR department processes.

2. PHYSICAL SECURITY

PHYSICAL SECURITY

- The physical security is the protection of personnel and assets from events and circumstances that could cause loss or damage to an organization.
- Physical controls protect an organization's interests and assets and can be as important as the logical controls within IT systems.

PHYSICAL RISK ASSESSMENT

Physical risk assessments are performed against 'hard targets' within the organization. Not all CISOs have responsibility for physical assets protection.

If, as a CISO, you are tasked with physical protection:

- Leverage work from BCM and DRP teams.
- Follow ISO and NIST guidance.
- Focus on facilities housing technology.
- Create documentation showing asset connections to site locations.
- Obtain vendor and third-party support physical security requirements within executed contracts.

PHYSICAL LOCATION CONSIDERATIONS

Geographic location: The physical location is critical. For instance, a facility may be in an area having a high probability of tornadoes, earthquakes or floods.

Multi-tenancy: Organizations often occupy offices in a building shared with other tenants. Physical control may be more difficult when sharing resources with other tenants in a facility.

Building Materials: The construction of a building will contribute to the overall security of the facility. For instance, steel doors provide more protection than glass or wooden doors.

OBSTACLES AND PREVENTION

- Physical security strategies focus on barriers and protections that limit potential damage to facilities due to physical attack or natural disasters.
- Protection from physical attackers is achieved by using a strategy of layered defense. The layers create an increasingly difficult set of obstacles an attacker must overcome to conduct a successful attack or compromise.
- Areas requiring higher levels of protection may include server rooms, file areas, communication closets, datacenters, or areas with consistent concentrations of personnel.

OBSTACLES AND PREVENTION - CONTINUED

Protection can be achieved by implementing physical and environmental controls to mitigate the outcome of physical incidents.

- National Institute of Science and Technology (NIST) SP 800-53 R5 includes a family of controls dedicated to physical and environmental protections:
  - PE-1: Physical and environmental protection policies and procedures require consideration for controls that facilitate the implementation of physical and environmental protection controls.
  - PE-9: Power equipment and cabling requires consideration for protecting power equipment and cabling from damage or destruction.
  - PE-11: Emergency power requires consideration for short-term uninterruptable power supplies to facilitate orderly shutdown of systems.
  - PE-13: Fire protection requires consideration for fire suppression and detection systems.
  - PE-15: Water damage protection requires consideration for protecting systems from damage resulting from water leakage by master shutoff and isolation valves.

SECURITY OPERATIONS CENTER

Physical security – Security Operations Center types

In-house (I-SOC) – the classic in-house dedicated SOC.

Hybrid (H-SOC) – a combined in-house and managed services SOC.

Managed (M-SOC) – third party provided managed security operations center or SOC as a service (SOCaaS).

Security Network Operations Center (SNOC) – combined network and security operations center.

Virtual (V-SOC) – is a distributed SOC capability consisting of tools and analysts.

SENSITIVE COMPARTMENTED INFORMATION FACILITY

- Sensitive Compartmented Information Facilities (SCIFs) create a secure area with protections to ensure that highly sensitive information inside the facility can not be compromised.
- These specific requirements are outlined in Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities—Version 1.5.1—IC Tech Spec—for ICD/ICS 705— July 26, 2021.

SENSITIVE COMPARTMENTED INFORMATION FACILITY – CONTINUED

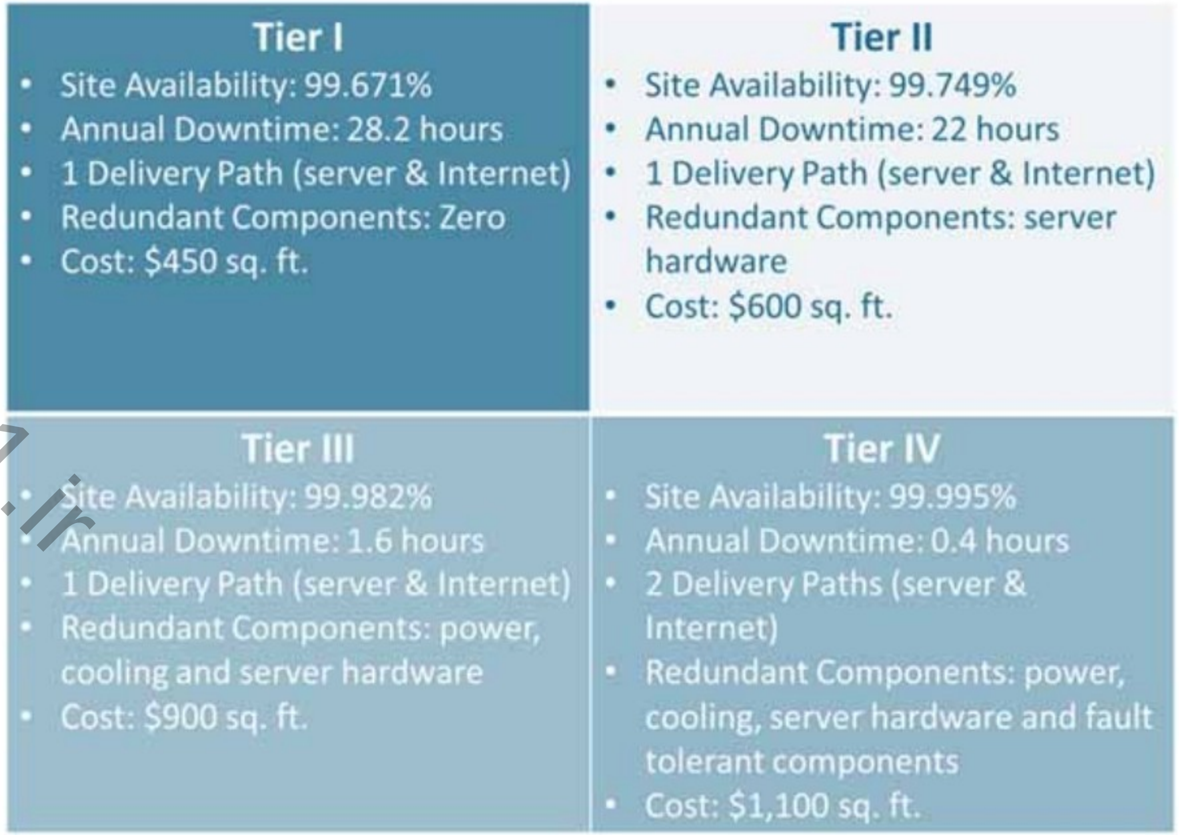
- The following is a summary of the primary SCIF design focus criteria:
  - Building profile.
  - Physical requirements.
  - Ductwork.
  - Entrance doors.
  - Access controls.
  - Intrusion detection.
  - Electronic and communication systems.
  - Sound masking.

DIGITAL FORENSIC LAB

- Designing and building a forensic laboratory can be a complicated task.
- The forensics lab must have specific controls to assure the integrity of evidence.
- Forensics lab implementations are often submitted with evidence to provide proof of due diligence in handling evidence
- It typically requires a high degree of planning to assure digital evidence is not rejected due to a poorly designed facility.

DATACENTER

- Datacenter security refers to the precautionary measures defined in the standards for datacenter infrastructures.
- The goal is to protect datacenters from natural or human disasters.
- The Uptime Institute began rating classes of datacenters in 1993 and has published four tiers of datacenters based on resiliency – still valid.



Tier I

- Site Availability: 99.671%
- Annual Downtime: 28.2 hours
- 1 Delivery Path (server & Internet)
- Redundant Components: Zero
- Cost: $450 sq. ft.

Tier II

- Site Availability: 99.749%
- Annual Downtime: 22 hours
- 1 Delivery Path (server & Internet)
- Redundant Components: server hardware
- Cost: $600 sq. ft.

Tier III

- Site Availability: 99.982%
- Annual Downtime: 1.6 hours
- 1 Delivery Path (server & Internet)
- Redundant Components: power, cooling and server hardware
- Cost: $900 sq. ft.

Tier IV

- Site Availability: 99.995%
- Annual Downtime: 0.4 hours
- 2 Delivery Paths (server & Internet)
- Redundant Components: power, cooling, server hardware and fault tolerant components
- Cost: $1,100 sq. ft.

Uptime Institute Datacenter Tier Classifications

PREPARING FOR PHYSICAL SECURITY ASSESSMENTS

- Physical security audits should be regularly performed to provide assurance that selected physical security controls are implemented and working as intended.
- Physical protection systems can often be tested by walking through areas and determining if coverage is adequate.
- For instance, A CISO can conduct periodic assessments of digital video systems by walking through areas of camera coverage and making sure images are sufficient and recorders function properly.
- As part of the walkthrough, other controls can be tested such as doorjambs for preventing forced entry or functionally testing alarm systems.

3. NETWORK SECURITY

NETWORK SECURITY

- CISO are typically responsible for assuring policies and procedures exist to support network operations security.
- The security function does not normally manage routers and configure network technology, but the CISO typically defines security controls for these systems.
- CISOs should understand the impact of new communications technologies on existing information security controls and services and modify as needed to maintain compliance with policies and procedures.

NETWORK SECURITY ASSESSMENTS AND PLANNING

- Enterprises normally divide responsibility for technology, network, and security management between varying roles.
- Most often, the CISO focuses exclusively on risk management and other security-centric activities, while the CIO or CTO leads efforts for network technology implementation.
- The following tips can help you develop an effective network security plan:
  - Collaborate within the organization to develop and implement network security strategies.
  - Strive to find the right balance between network security and usability.

NETWORK SECURITY ARCHITECTURE CHALLENGES

The following provides some of the challenges CISOs face when working with the network management function.

- Defining ownership, responsibility, and accountability of security devices and systems (such as firewalls and IDS/IPS) connected to the network.
- Balancing increased network security with decreased functionality.
- Agreeing on the need for specific network security devices and technologies.
- Defining a shared security responsibility model for network services.
- Determining budget ownership of network investment that has integrated security capabilities.

NETWORK SECURITY DESIGN

CISOs need to work closely with network architects to create a secure infrastructure design that protects the organization's information and assets.

The process of secure network design can be broken into the following steps:

1. Define a network security policy.
2. Identify network assets.
3. Analyze network security risks.
4. Analyze network security requirements.
5. Develop a security plan.
6. Develop a technical implementation strategy.
7. Achieve buy-in from users, managers, and technical staff.
8. Train users, managers, and technical staff.
9. Implement network security solutions.
10. Test the network security implementations and update if problems are found.
11. Maintain a secure network state.

NETWORK STANDARDS, PROTOCOLS, AND CONTROLS

- To determine if security with the IT network function is adequate, a new CISO should devote time for understanding current network security.
- This includes a historical review of standards, networking protocols, and network security controls.
- When you start a new CISO position, do not make assumptions.
- If you view controls as inadequate, take the time to understand why the situation exists.
- Work to integrate the CIO and network group as part of the security team to improve security within their resource constraints.

NETWORK SECURITY STANDARDS

- ISO/IEC 27033 is a multipart standard derived from the existing five-parts of ISO/IEC 18028.
- The purpose of it is to provide detailed guidance for the management, operation and use of information system networks.
- CISOs can adapt the material in this standard to guide network security requirements and controls within networks.

NETWORK SECURITY STANDARDS

ISO/IEC 27033 provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002.

ISO/IEC 27033

1:2015 - Network security **overview and concepts**.

2:2012 - Guidelines for the **design and implementation** of network security.

3:2010 - Reference **networking scenarios**—threats, design techniques, and control issues.

4:2014 - Securing communications between networks using **security gateways**.

5:2013 - Securing communications across networks using **virtual private networks**.

6:2016 - Securing **wireless** IP network access.

PROTOCOLS

Internet protocols

- File Transfer Protocol (FTP) – transfer of computer files.
- Hypertext Transfer Protocol (HTTP) – foundation of connectivity on World Wide Web.
- Transmission Control Protocol (TCP) – interconnected devices on the Internet.
- User Datagram Protocol (UDP) – low latency and loss toleration.

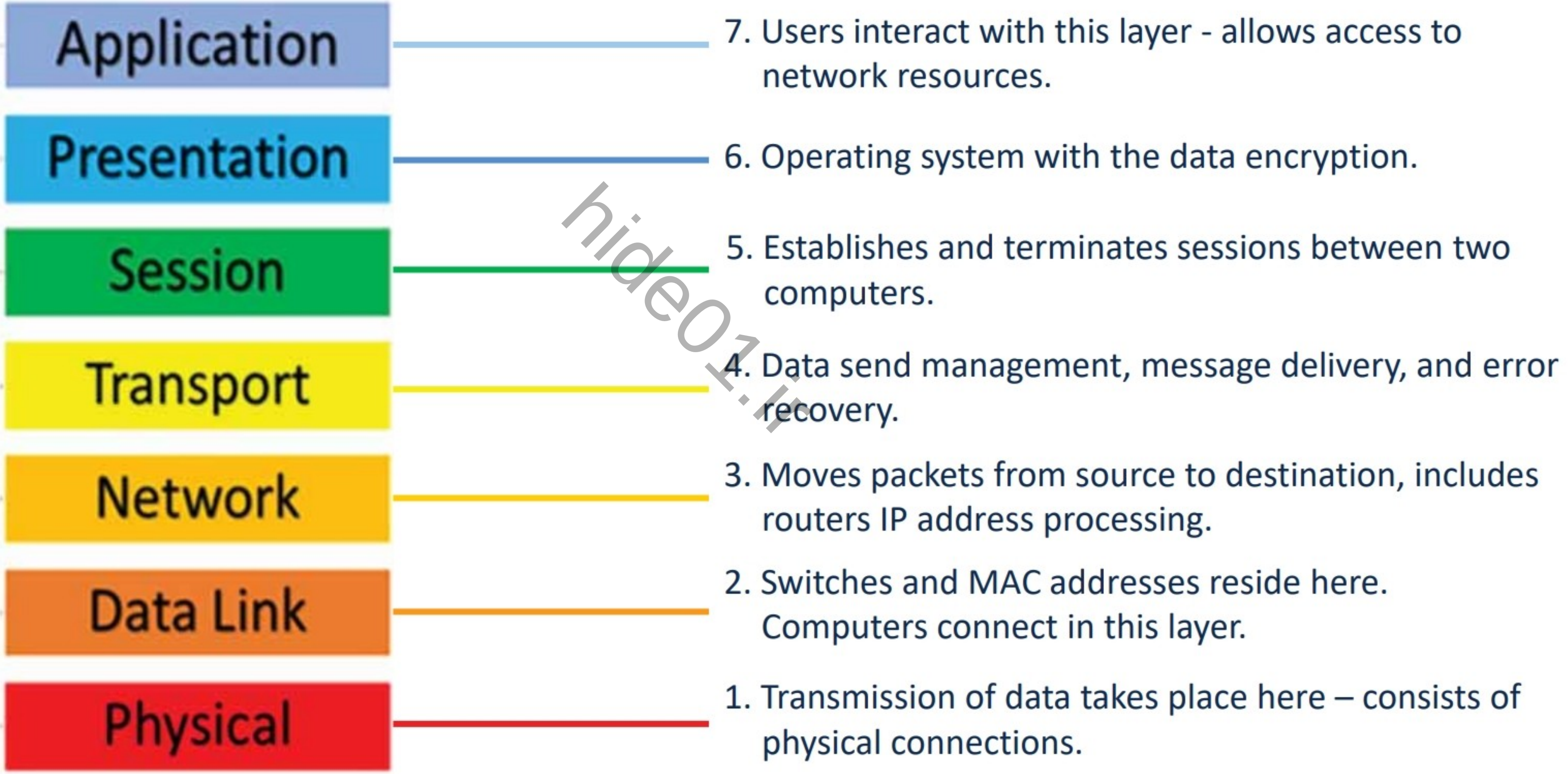
Wireless network protocols:

- Bluetooth – cable replacement protocol.
- Long-Term Evolution (LTE) – increased speed and capacity of wireless networks.

Network routing protocols

- Border Gateway Protocol (BGP) – Internet traffic routing.
- Enhanced Interior Gateway Routing Protocol (EIGRP) – Cisco automated routing decisions.

OSI MODEL



Application — 7. Users interact with this layer - allows access to network resources.

Presentation — 6. Operating system with the data encryption.

Session — 5. Establishes and terminates sessions between two computers.

Transport — 4. Data send management, message delivery, and error recovery.

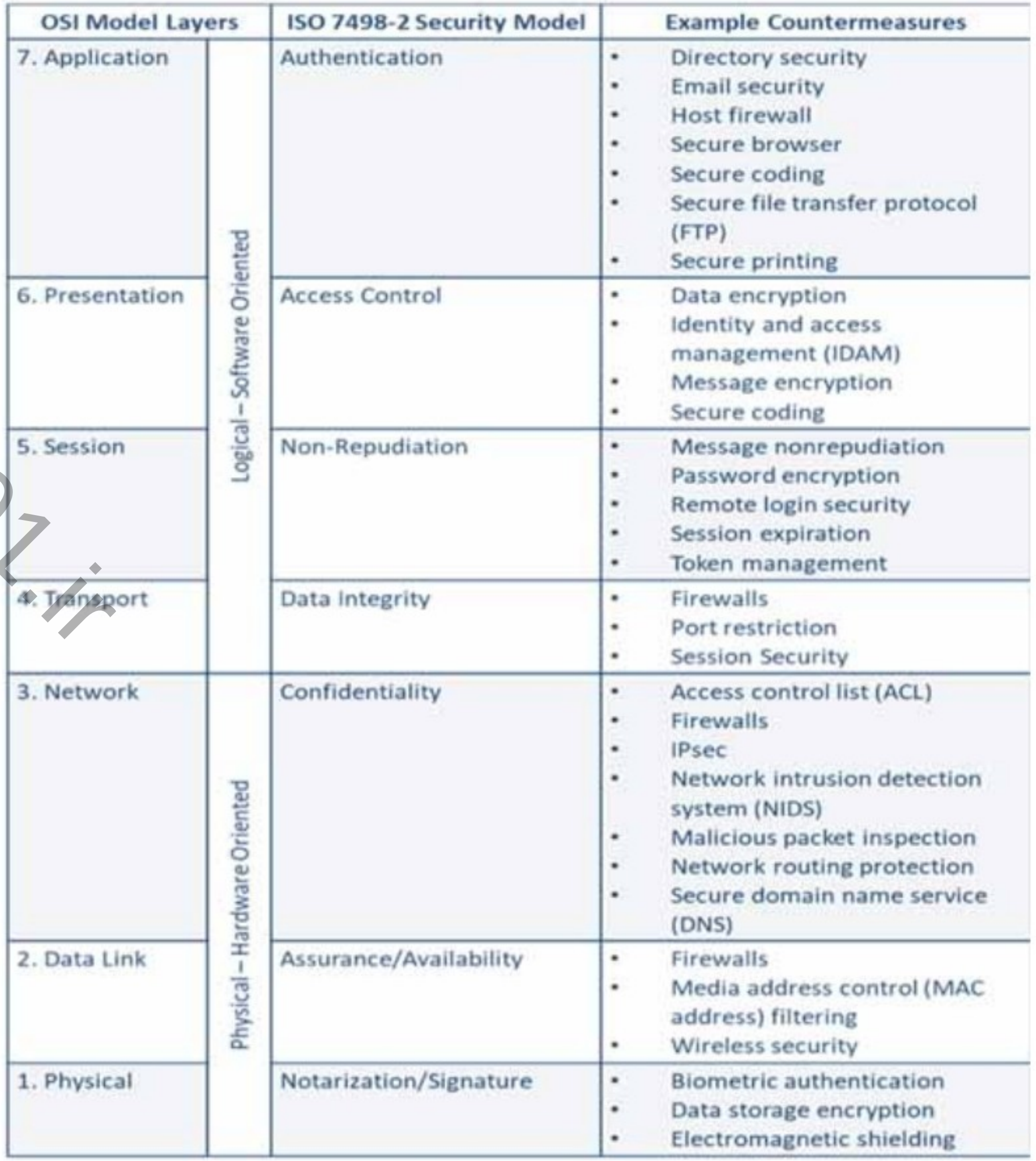
Network — 3. Moves packets from source to destination, includes routers IP address processing.

Data Link — 2. Switches and MAC addresses reside here. Computers connect in this layer.

Physical — 1. Transmission of data takes place here – consists of physical connections.

OSI MODEL SECURITY MODEL

A deeper look at OSI layers and what occurs in each.



OSI Model Layers		ISO 7498-2 Security Model	Example Countermeasures
7. Application	Logical – Software Oriented	Authentication	• Directory security • Email security • Host firewall • Secure browser • Secure coding • Secure file transfer protocol (FTP) • Secure printing
6. Presentation		Access Control	• Data encryption • Identity and access management (IDAM) • Message encryption • Secure coding
5. Session		Non-Repudiation	• Message nonrepudiation • Password encryption • Remote login security • Session expiration • Token management
4. Transport		Data Integrity	• Firewalls • Port restriction • Session Security
3. Network	Physical – Hardware Oriented	Confidentiality	• Access control list (ACL) • Firewalls • IPsec • Network intrusion detection system (NIDS) • Malicious packet inspection • Network routing protection • Secure domain name service (DNS)
2. Data Link		Assurance/Availability	• Firewalls • Media address control (MAC address) filtering • Wireless security
1. Physical		Notarization/Signature	• Biometric authentication • Data storage encryption • Electromagnetic shielding

NETWORK SECURITY CONTROLS

CISOs should understand common controls and methods for protecting network communications.

The following are common network security technologies to defend against common threats.

Boundary Protection

- Firewall (external)
- Edge router
- Network Address Translation (NAT)
- Intrusion detection systems
- Secure network gateway
- Virtual Private Networks (VPN)
- Web Proxy

Internal Network Protection

- Firewall (internal)
- Intrusion detection systems
- Intrusion prevention systems
- Network encryption
- Network segmentation

WIRELESS SECURITY AND RISKS

Wireless networking uses radio waves to facilitate communication. Because of this, an attacker does not have to be physically connected to potentially gain access.

Common wireless risks:

- Listening in – eavesdropping on network traffic to enable credential theft.
- Stealing bandwidth – unauthorized use of someone's bandwidth.
- Rogue access points – unauthorized WIFI access point added to a network.

WIRELESS CONTROLS

Common wireless security controls include the following:

- Policies – acceptable WIFI use.
- Administrative passwords – rename default passwords.
- MAC address filtering – block devices connecting without a valid MAC address.
- Service set identifier – create unique name of network to slow down attackers.
- Wi-Fi protected access (WPA2) – encryption of wireless traffic, keys changed at regular intervals.

VOICE OVER IP SECURITY

- CISOs should understand the unique security considerations for Voice Over Internet Protocol (VoIP)
- VOIP is the conversion to digital packets distributed over a switched IP network.
- Attaching IP-based telephones to the network extends the attack surface, adding potential vulnerability.
- Attacks against this infrastructure may be used to commit fraud, disclose confidential voice communication, or facilitate methods to gain access to the broader network.
- Encryption, network segmentation, filtering, strong authentication, and other controls should be used in VoIP deployments.

4. ENDPOINT PROTECTION

ENDPOINT PROTECTION

- Endpoint security is focused on user devices connected to a network, such as mobile devices, laptops, and desktop PCs.
- Hardware such as servers in a datacenter can also be considered endpoints.
- Endpoint security reduces risks present within a myriad of devices connecting to an enterprise network, including Bring Your Own Device (BYOD) mobile technologies.
- Endpoint security products may contain features and functionality such as:
    - Data loss prevention.
    - Device and email encryption.
    - Application whitelisting.
    - Network access control.
    - Endpoint detection and response.
    - Privileged user control.

ENDPOINT THREATS

Malware - malicious software that can be implanted or introduced into a target's computer and can take the form of executable code, scripts, active content, or other attack vectors.

Phishing attacks - attempt to acquire sensitive information such as usernames, passwords, and financial instrument details, by masquerading as a trustworthy entity.

Ransomware - malware that restricts access to the infected computer data or system and demands that the user remit payment for restoration of the system. Data encryption is the most common method of system denial.

ENDPOINT VULNERABILITIES

- Bring You Own Device (BYOD) introduces a broad range of devices that employees can use and increases vulnerability due to the various types of technology connecting to your networks.
- Inadequate security patching within those devices is problematic.
- Incomplete application blocking is also prevalent.
  - Whitelisting and blacklisting are difficult to support, particularly in large, diverse environments
- Shadow IT is the use of unauthorized infrastructure, such as WIFI routers, servers, and other technology.
  - This is different than the BYOD issue – it involves supporting business with unknown or informally procured assets .

END USER SECURITY AWARENESS

- Endpoint protection begins with the user or the human firewall.
- CISOs need to provide effective and engaging security awareness training to leverage the first line of defense (people).
- To assist with creating an effective security awareness program, the following guidelines may be useful:
  - Security policies should be easy to understand and relevant - complicated and verbose policies can do more harm than good.
  - A security awareness portal is a valuable resource to communicate polices, best practices, and safety tips. A security function WIKI page in the internal network is a great idea.
  - Keep it simple - this is critical for communicating security awareness messages to end users.
  - Integrate security responsibilities into user responsibilities – HR should formalize security requirements into job descriptions.
  - Adherence to security should be incentivized to positively shape user behavior.
  - Security awareness training should be short, interactive, and interesting.

ENDPOINT DEVICE HARDENING

- Endpoint hardening includes endpoint patching and configuration management.
- Hardening settings can be found in the NIST National Vulnerability Database and includes the following:
  - Enabling on-platform OS encryption.
  - Restricting applications and removing user installations.
  - Applying OS and application patches.
  - Removing unnecessary software and utilities.
  - Disabling unnecessary ports and services.
  - Performing vulnerability scans.

ENDPOINT DEVICE LOGGING

- The event logging service records events from various resources and stores them in a single collection called an event log.
- Applications can be difficult to manage due to proprietary logs with unique format and user interface.
- Data from different applications might not be able to be merged into one data set for investigation, making it difficult to diagnose problems.
- The event viewer enables you to view logs; some devices also have programming interfaces that enables extraction and examination of logs.

MOBILE DEVICE RISKS

- Mobile security is the protection of smartphones, tablets, laptops, and other portable computing devices and the network connections.
- The Open Web Application Security Project (OWASP) can be useful for analyzing the current top 10 mobile device risks.
- The following is a recent example of a top 10 list:

M1: Improper platform usage.
M2: Insecure data storage.
M3: Insecure communication.
M4: Insecure authentication.
M5: Insufficient cryptography.
M6: Insecure authorization.
M7: Client code quality.
M8: Code tampering.
M9: Reverse engineering.
M10: Extraneous functionality.

MOBILE DEVICE SECURITY CONTROLS

- NIST provides guidance for Mobile Device Management (MDM) in its Special Publication 800-124 Revision 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise.
- NIST also provides a practical reference architecture for deploying MDM in an enterprise via NIST SP 1800-4.
- It also contains an example set of policies for MDM/Enterprise Mobility Management (EMM). (NIST SP 1800-4B, NIST SP 1800-4C)

INTERNET OF THINGS SECURITY

- IoT involves extending Internet connectivity beyond standard devices such as desktops, laptops, smartphones, and tablets.
- It includes connecting traditionally non-Internet-enabled physical devices and everyday devices.
- These devices can communicate and interact over the Internet, and they can be remotely monitored and controlled.
- The term ‘smart’ is typically included in the item name or description.
- Examples include smart door locks, cars, pet feeders, aquarium heaters, televisions, refrigerators, lighting systems, and a vast range of other electronic devices that connect to the Internet.

PROTECTING IOT DEVICES

The following are important considerations for securing IoT devices:

- Organizations should know if IoT devices are deployed within a network.
  - You can't protect it if you don't know it exists or where it is.
- Security testing of IoT devices.
  - Many IoT devices have been rapidly manufactured to gain market position.
  - This results in little consideration for security implementations within the devices.
  - CISOS should be prepared to enable testing of IoT device security features.
- IS policies should clearly state which IoT devices are allowed and what type of data exchanges are permissible within them.
- IoT devices require the same access control, encryption, device hardening, monitoring, and other security controls as are applied throughout the enterprise.

5. APPLICATION SECURITY

APPLICATION SECURITY

- We know that a key role of the CISO is evaluation of risk within the organization, and understanding vulnerabilities is a critical part of that risk responsibility.
- To that end, the CISO should remain engaged with organizational teams managing applications to assure vulnerabilities are minimized and do not present unnecessary risk for the organization.
- Enterprise applications can include email systems, collaboration tools, and file sharing capabilities.
- Other applications can be those used for specific purposes, or custom applications developed in support of business or customer needs.

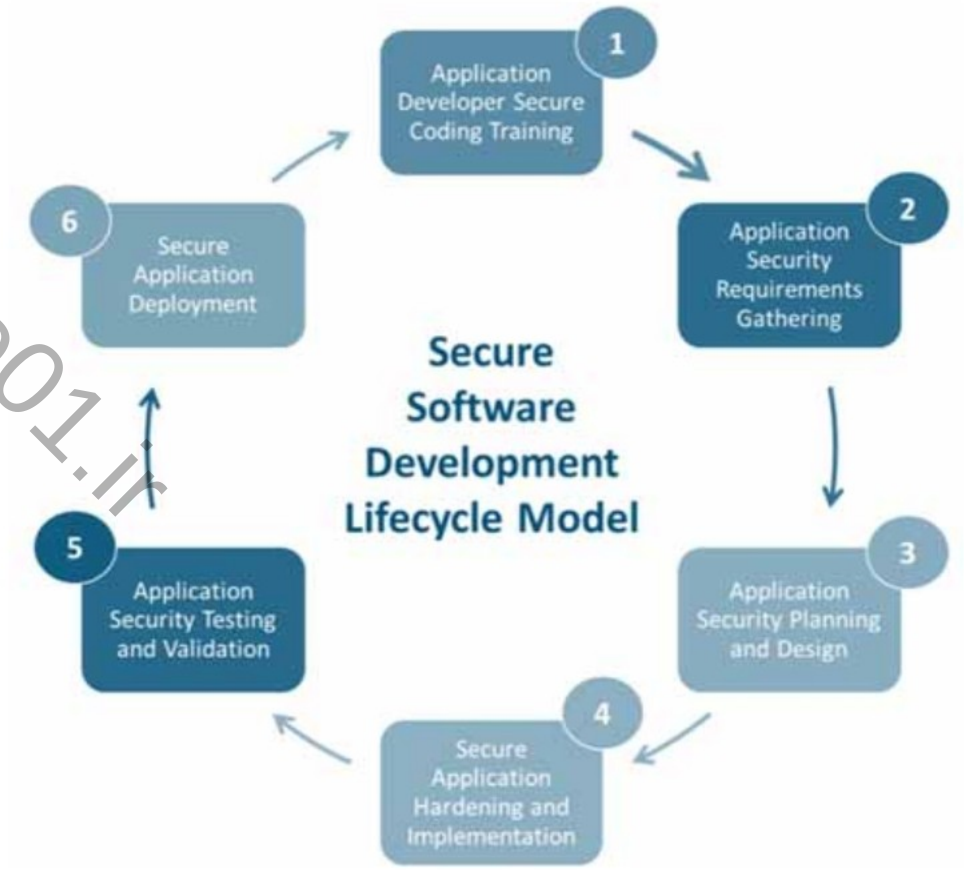
SECURE CODING PRACTICES

- Secure coding is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities.
- Defects, bugs, and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities.
- The following is a compendium of secure coding practices your organization should adopt:

1. Align to robust secure coding standards.
2. Define application security policies and requirements.
3. Adopt minimalist coding philosophy.
4. Apply principles of least privilege.
5. Deny access by default.
6. Validate all input.
7. Heed compiler warnings.
8. Sanitize data sent to other systems.

SECURE SDLC MODEL

- The Secure Systems Development Life Cycle (SecSDLC) model shows how to insert security requirements into software development.


1
Application Developer Secure Coding Training
2
Application Security Requirements Gathering
3
Application Security Planning and Design
4
Secure Application Hardening and Implementation
5
Application Security Testing and Validation
6
Secure Application Deployment
Secure Software Development Lifecycle Model

Secure SDLC Model

SEPARATION OF DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS

- Programmers generally have more access privilege in test and development environments than they do to production environments.
- This is to preclude the possibility of system compromise and maintain separation between production and testing environments.
- Joining test and production environments will expose production data to test code that may not be secure, or users that are not authorized access.
- This unauthorized access to production systems and data creates critical risk situations.

APPLICATION SECURITY TESTING APPROACHES

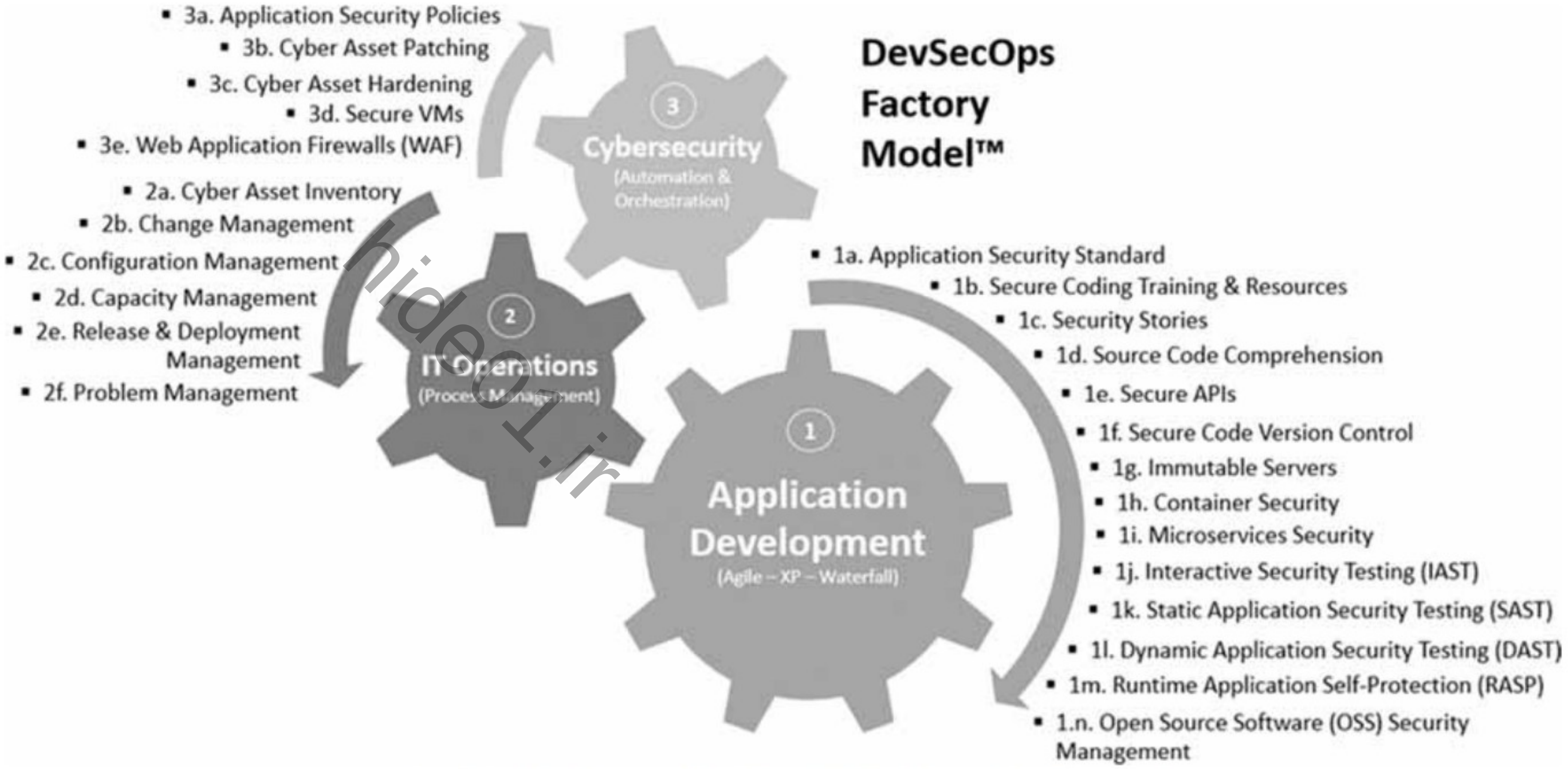
- Under ideal conditions, security is provided throughout all phases of the SDLC.
- Dynamic and static application testing provides an opportunity to evaluate the effectiveness of a system's security controls.
- Testing can include:
  - Dynamic Application Security Testing (DAST).
  - Static Application Security Testing (SAST).
  - Fuzz testing tools.
  - Interactive application security testing (IAST).
  - Application penetration testing.
  - Bug bounty program.

DevSecOps

- One of the newest ways to operationalize cybersecurity is to integrate it into your organization's Development Operations (DevOps).
- DevOps is a term used to describe the integration of application development with IT operations, which enables efficiency with continual code improvements and application suite expansions.
- CISOs can leverage DevOps functions to insert security controls throughout the development process, as most DevOps functions include workflow generators for managing the phases of code movement and quality checkpoints.

DevSecOps

The term *DevSecOps* is used when security is integrated into the DevOps workflow.



- 3a. Application Security Policies
- 3b. Cyber Asset Patching
- 3c. Cyber Asset Hardening
- 3d. Secure VMs
- 3e. Web Application Firewalls (WAF)

- 2a. Cyber Asset Inventory
- 2b. Change Management
- 2c. Configuration Management
- 2d. Capacity Management
- 2e. Release & Deployment Management
- 2f. Problem Management

- 1a. Application Security Standard
- 1b. Secure Coding Training & Resources
- 1c. Security Stories
- 1d. Source Code Comprehension
- 1e. Secure APIs
- 1f. Secure Code Version Control
- 1g. Immutable Servers
- 1h. Container Security
- 1i. Microservices Security
- 1j. Interactive Security Testing (IAST)
- 1k. Static Application Security Testing (SAST)
- 1l. Dynamic Application Security Testing (DAST)
- 1m. Runtime Application Self-Protection (RASP)
- 1.n. Open Source Software (OSS) Security Management

DevSecOps Factory Model™ (By Tari Schreider, licensed under a Creative Commons Attribution-Non-Commercial-NoDerivitives 4.0 International License).

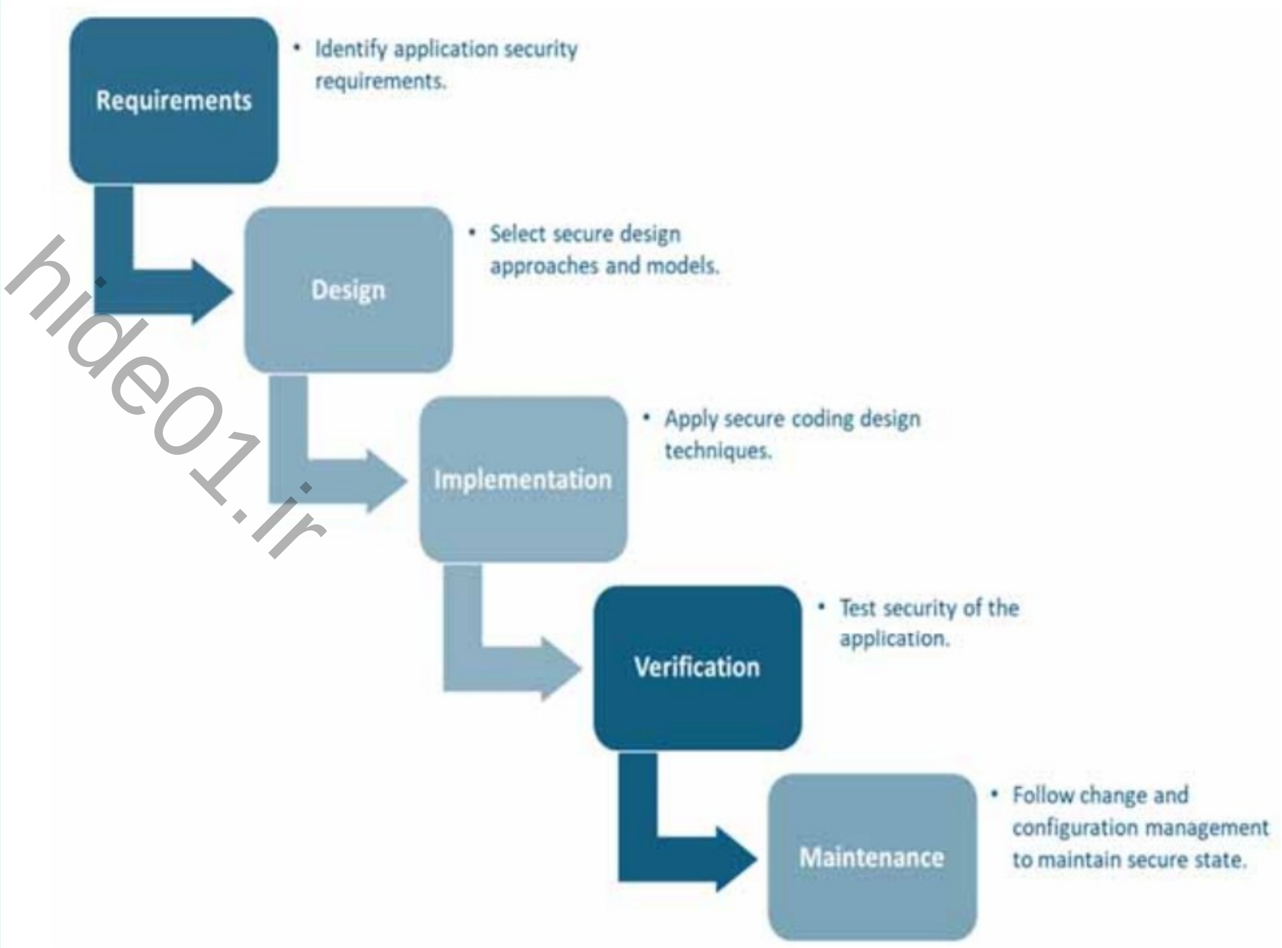
WATERFALL METHODOLOGY AND SECURITY

- The waterfall model is a sequential design process, used in software development processes, in which progress is seen as flowing steadily downward (like a waterfall).
- This includes the phases of conception, initiation, analysis, design, construction, testing, production/implementation, and maintenance.
- It is one of the earliest development models, but still in use.

WATERFALL METHODOLOGY AND SECURITY – CONTINUED

The waterfall model uses five phases to produce, review, refine, and approve artifacts.

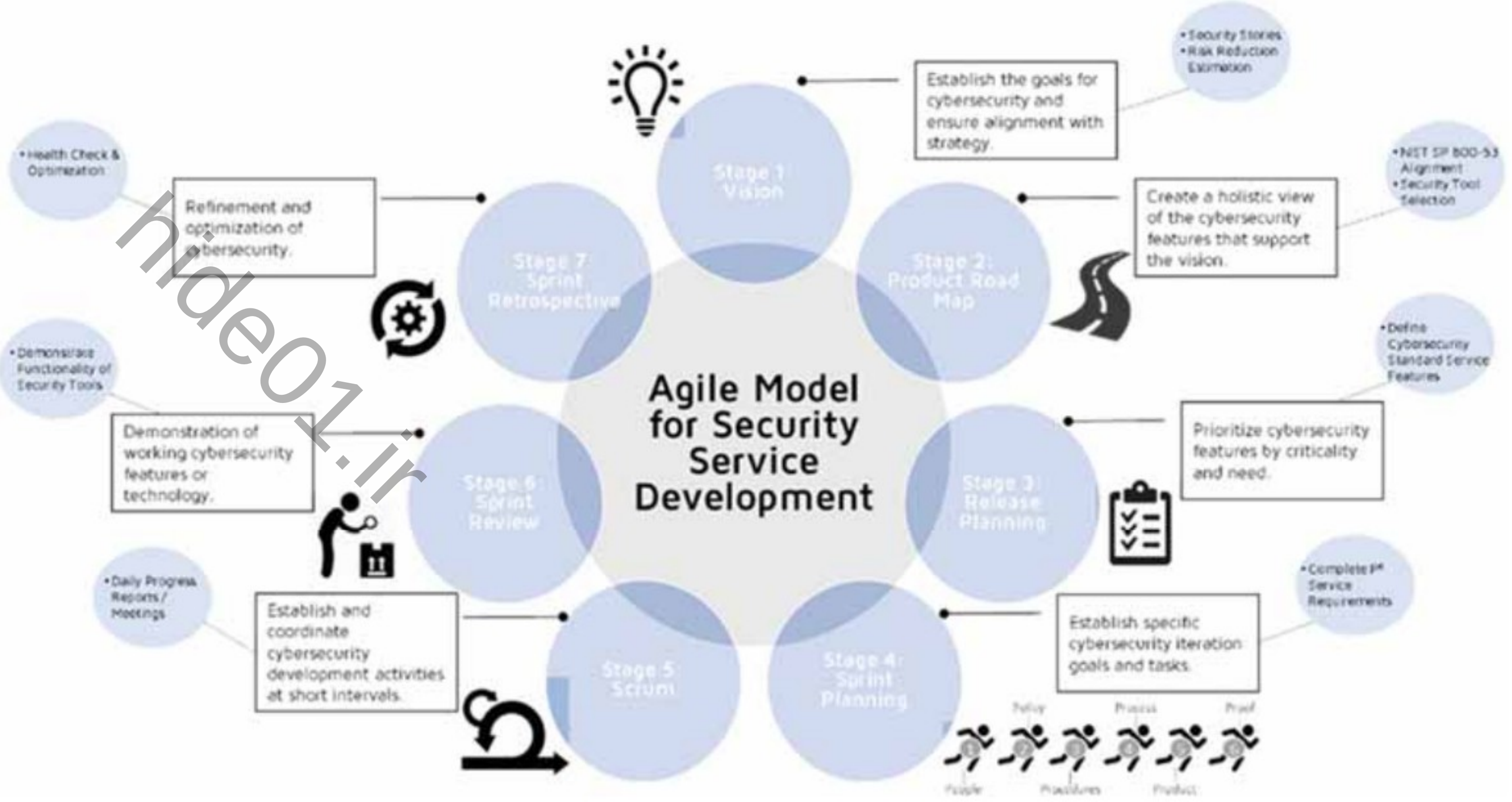
The model reflects a waterfall because it moves forward with little opportunity to return to a previous phase once it is complete.


Requirements
• Identify application security requirements.
Design
• Select secure design approaches and models.
Implementation
• Apply secure coding design techniques.
Verification
• Test security of the application.
Maintenance
• Follow change and configuration management to maintain secure state.

Secure Waterfall Diagram

AGILE METHODOLOGY AND SECURITY

- Agile was introduced in 2001.
- This process calls for teams to create artifacts at the end of relatively short periods, which are typically 4 weeks.
- Overlapping cycles create continuous improvements and release cycles.
- Very rapid, very responsive, and is excellent for managing changing requirements.


Agile Model for Security Service Development
Stage 1 Vision
Establish the goals for cybersecurity and ensure alignment with strategy.
• Security Stories
• Risk Reduction Estimation
Stage 2: Product Road Map
Create a holistic view of the cybersecurity features that support the vision.
• NIST SP 800-53 Alignment
• Security Tool Selection
Stage 3: Release Planning
Prioritize cybersecurity features by criticality and need.
• Define Cybersecurity Standard Service Features
Stage 4: Sprint Planning
Establish specific cybersecurity iteration goals and tasks.
• Complete P* Service Requirements
Policy
Process
Proof
People
Procedures
Product
Stage 5 Scrum
Establish and coordinate cybersecurity development activities at short intervals.
• Daily Progress Reports / Meetings
Stage 6 Sprint Review
Demonstration of working cybersecurity features or technology.
• Demonstrate Functionality of Security Tools
Stage 7 Sprint Retrospective
Refinement and optimization of cybersecurity.
• Health Check & Optimization

Agile Security Model

OTHER APPLICATION DEVELOPMENT APPROACHES

- Joint applications development (JAD) is a team-oriented approach whereas the customer and technology departments work together to capture the user's view of the business requirements before developing a system.
- This process is most used to determine the requirements for large, complex systems.
- Sometimes referred to as a Proof of Concept (PoC), this is a form of prototyping and is commonly used to determine system requirements before committing larger amounts of resources to an effort.
- System functionality and feasibility can be explored before developing the larger scale system.

APPLICATION HARDENING

- Applications can be difficult to secure due to system complexity, the ability to accept input from many different sources, the use of multiple protocols, and having multiple levels of access and authority within their operational environment.
- Unused applications should be removed from the environment because exploits are typically most effective on old code.
  - Older applications might not be supported, or patches might not be available for them.
- Application security controls typically include internal configurations and external or environment protections.

APPLICATION SECURITY TECHNOLOGIES

- Secure coding is only one, limited aspect of application security.
- To further protect applications from exploitation, additional technologies might be necessary. This includes:
  - **Application Programming Interfaces (API) security**
    - Security is an essential element of any application to include application interfaces. Vulnerabilities in this layer of the infrastructure can allow cybercriminals to target applications via APIs.
  - **Runtime Application Security Protection (Runtime Application Self-Protection (RASP)**
    - RASP consists of security controls within applications that provide security while the application is running. This allows the application to block attacks and provide alerting that an event occurred.

APPLICATION SECURITY TECHNOLOGIES - CONTINUED

- Software Composition Analysis (SCA)
  - This is a set of tools that provides users visibility into their open-source inventory.
  - SCA is an automated process that identifies the open-source software in a codebase.
  - This analysis is performed to evaluate security, license compliance, and code quality.
- Web Application Firewall (WAF)
  - This consists of a software solution that filters, monitors, and blocks HTTP traffic to and from Web applications.
  - A WAF is differentiated from a regular firewall in that a WAF is typically used to filter the content of specific Web applications while regular firewalls serve as a broader safety measure.

VERSION CONTROL AND PATCH MANAGEMENT

- Patch management
  - A wide variety of applications are used in business for so many reasons.
  - Whether you use Skype to contact work-from-home employees or Adobe for documents, you will probably use third-party applications in your organization.
  - As a CISO you should assure proper patching of these applications.
- Version control
  - This is a component of software configuration management and is also known as revision control or source control.
  - It is used to assist in managing changes to applications, documents, Web sites, or other assets.
  - Changes are usually identified by a number or letter code, termed the revision number, revision level, or simply version.

DATABASE SECURITY

- Database security includes a broad range of information security controls to protect databases against compromise of confidentiality, integrity, and availability.
- Database security methods include:

1. Isolating sensitive databases.
2. Hardening databases using standardized controls.
3. Threat and vulnerability management.
4. Deploying database firewalls.
5. Encrypting data at rest.
6. Enforcing least privilege.
7. Monitoring databases for operational deviations.
8. Auditing of database activity.
9. Responding to suspicious behavior.

DATABASE HARDENING

- Most of the critical information in an organization is stored in a database.
- Applying effective security controls for databases is important to reduce vulnerabilities and improve risk conditions.
- Database operating systems function in a similar manner to server and endpoint operating systems.
- The same tools, techniques, and processes used to achieve IT systems hardening can often be applied directly to database systems.

6. ENCRYPTION TECHNOLOGIES

ENCRYPTION AND DECRYPTION

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.
- Encryption does not itself prevent interference of transmitting the message, but rather denies the intelligible content to a would-be interceptor.
- In an encryption scheme, the intended information or message (referred to as plaintext) is encrypted using an encryption algorithm.
- That algorithm is called a cipher, which generates encoded text that can be read only if decrypted.

CRYPTOSYSTEMS

- A cryptosystem is a suite of cryptographic algorithms needed to implement a security service.
- Cryptosystems are used for achieving confidentiality.
- A cryptosystem typically consists of three algorithms:
  - Key generation.
  - Encryption.
  - Decryption.

BLOCKCHAIN

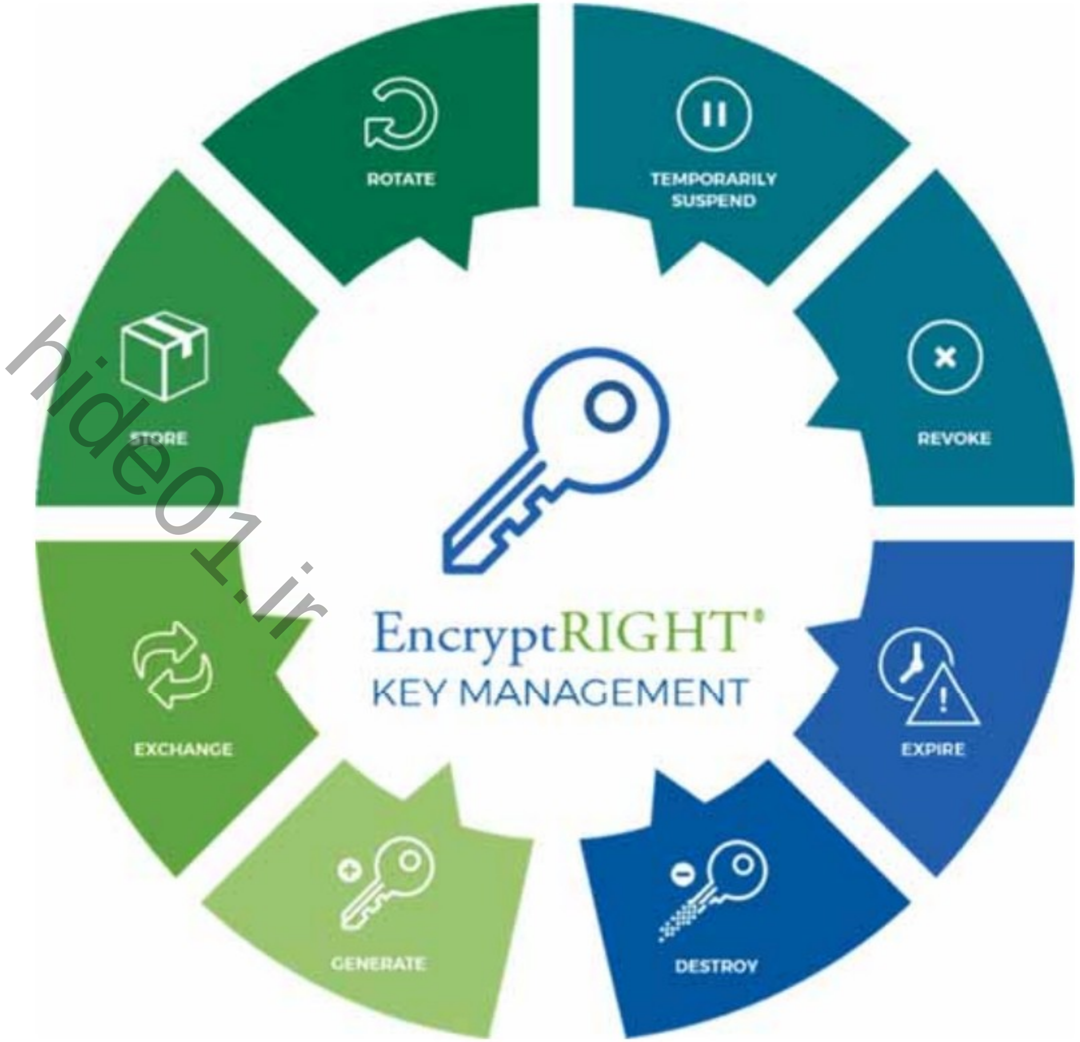
- Blockchain is an expanding list of records called blocks that are linked cryptographically as a chain.
  - Each block contains:
    - A cryptographic hash of the previous block.
    - The timestamp.
    - Transaction detail data.
- This makes blockchain one of the most secure methods for performing transactions.

DIGITAL SIGNATURES AND CERTIFICATES

- Digital signatures provide verification that a message came from the sender.
  - This creates nonrepudiation - someone sending a file with a digital signature cannot later claim they did not.
  - If the recipient can open the message sent with the public key, then the message could only have been sent by the sender who encrypted the message with the private key.
- Asymmetric algorithms are more computing intensive than symmetric algorithm
  - Asymmetric and symmetric algorithms are typically used in conjunction with each other.

KEY MANAGEMENT

This graphic provides a good example of the encryption key management lifecycle.



Source: EncryptRIGHT

HASHING

- Hash functions provide an integrity control by performing a one-way transformation of a string of characters into a fixed-length value or key that represents the original string.
- The fixed length files are relatively small, normally 128 bits in size.
- These are considered one-way functions because the hash (or message digest) cannot be used to regenerate the original message.
- It provides a rapid and lightweight method of verifying receipt of the original information.
- Common types of these algorithms are Message Direct Algorithm version 5 (MD5), and the Secure Hash Algorithms (SHA-1,-2,-3).

ENCRYPTION ALGORITHMS

- Encryption algorithms change plaintext information into a cipher text.
  - The decryption process is enabled by using a key to transform the cipher text back into plaintext.
  - Symmetric encryption and asymmetric encryption are the two primary encryption methods.
- Asymmetric encryption is also known as public/private key encryption.
  - It uses keys in pairs to encrypt and decrypt information.
  - One of the keys is kept secret and is called the private key, while the other is made public and known as the public key.

o Symmetric key encryption is simpler and often referred to as private key, shared key, secret key, single key, or same key encryption.

ENCRYPTION ALGORITHMS - CONTINUED

- Elliptical curve encryption is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite mathematical fields.
- It solves for asymmetric key issues pertaining to resolving encryption using large prime numbers.
- This method of encryption creates faster, smaller, and more efficient cryptographic keys.
  - A 256-bit elliptical curve key replaces a comparable 3072 bit-RSA key.
  - They are often used for digital currencies, replacing standard RSA encryption techniques.

DETERMINING CRITICAL DATA LOCATION AND TYPE

CISOs usually develop an encryption strategy to determine the most effective encryption for the levels of sensitive data used by an organization.

Data Location and Type:

- **Data-at-rest** is the data that is not actively moving from device to device or being transported in networks. It typically includes data stored on network storage segments, datacenters, hard drives, share drives, flash drives or other storage systems.
- **Data-in-use** is typically data being processed by a system.
- **Data-in-transit**, or data in motion, is data actively moving from one location to another via networks.

DECIDING WHAT TO ENCRYPT

Application sessions

Application user sessions, whether those be client/server or Web-based applications, that access information from a database or other server should be encrypted when in use.

Attachments and USB stored files

File-level encryption is typically applied to these types of files.

Backup media

Tape and hard drive backup require encryption prior to storing.

Classified or sensitive information

Sensitive data may require protections according to internal standards, customer contracts, international laws, or other requirements.

DECIDING WHAT TO ENCRYPT - CONTINUED

- Cloud computing

  Cloud storage providers typically offer cloud encryption services to encrypt data within the operations performed in this infrastructure (typically processing and storage).

- Mobile devices

  These present unique security challenges due to the high potential for data loss. It is common to apply full-hard drive encryption on these assets.

- Personally Identifiable Information and Protected or Personal Health Information

  Data protections for this category are typically defined by laws, regulations, and standards.

DETERMINING ENCRYPTION REQUIREMENTS

Encryption strategies usually include consideration of the following 4 supporting requirements:

- Technical capabilities or limitations.
- Regulatory and non-regulatory requirements.
- Policies and standards.
- Data classification hierarchies.

SELECTING, INTEGRATING, AND MANAGING ENCRYPTION TECHNOLOGIES

To assist Organization CISO's in establishing an encryption strategy, NIST has published NIST SP 800-53 Rev. 5 that provides encryption controls.

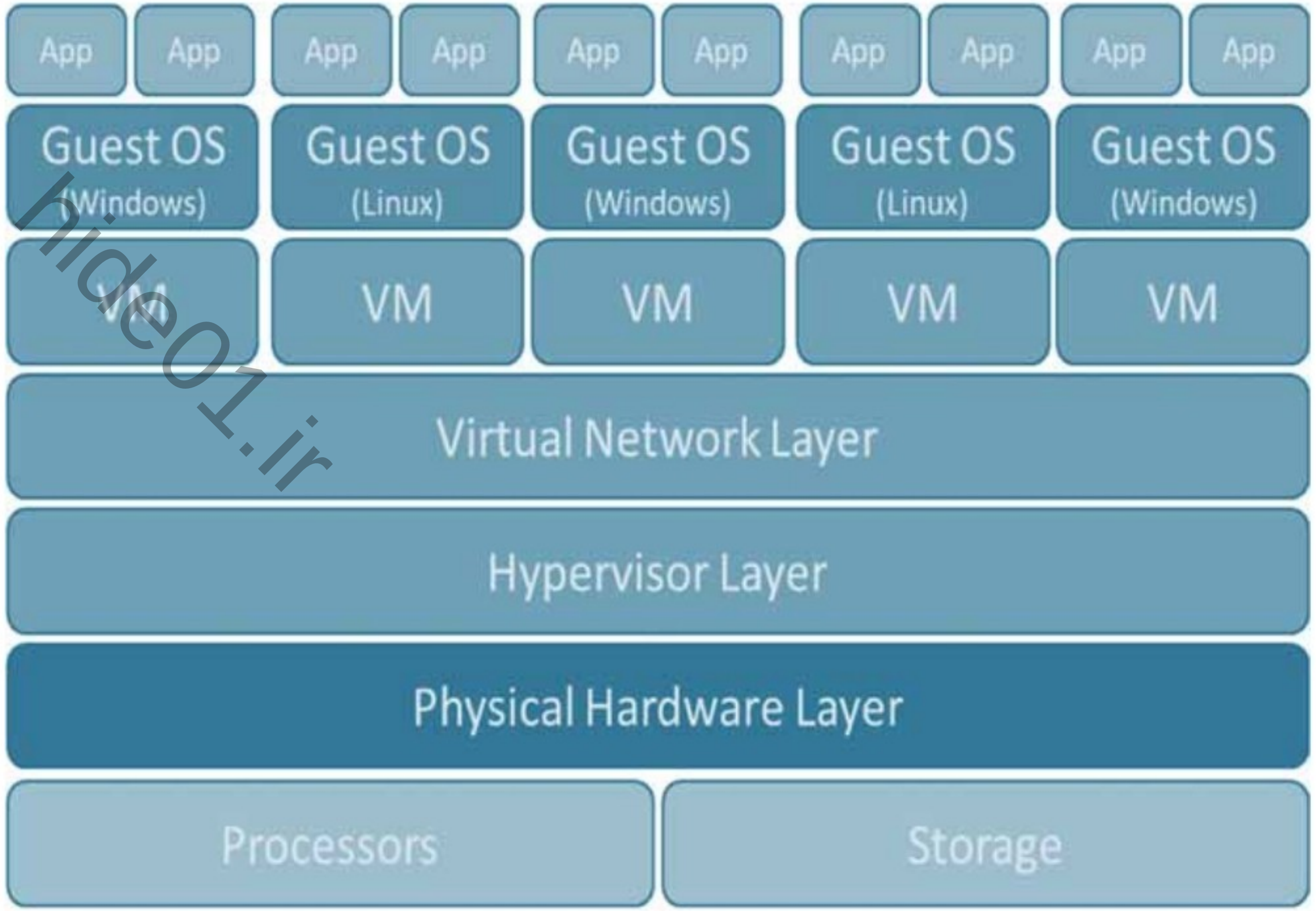
It includes:

- **IA-7**: cryptographic module authentication.
- **SC-8**: transmission integrity.
- **SC-9**: transmission confidentiality.
- **SC-12**: cryptographic key establishment and management.
- **SC-13**: use of cryptography.
- **SC-17**: PKI certificates.

7. VIRTUALIZATION SECURITY

VIRTUALIZATION OVERVIEW

- CISOs are often required to specify protections with virtual computing environments.
- Many virtual platforms exist to include operating system, storage devices, and networking resources.
- These can exist on a wide range of physical device infrastructures.



App App App App App App App App App App

Guest OS (Windows) | Guest OS (Linux) | Guest OS (Windows) | Guest OS (Linux) | Guest OS (Windows)

VM VM VM VM VM

Virtual Network Layer

Hypervisor Layer

Physical Hardware Layer

Processors | Storage

Virtualized Environment

VIRTUALIZATION OVERVIEW

- Desktop virtualization is the separation of the desktop environment and associated application software from the physical client device that is used to access it.
- Full virtualization is a technique that is a complete simulation of the underlying hardware system.
- Network virtualization is a process of combining hardware and software network resources into a single, software-based virtual network.
- Operating system virtualization is the existence of multiple isolated user-space instances, referred to as containers or partitions, that appear as computers from the point of view of programs running in them.
- Storage virtualization enables better functionality and more advanced features in computer data storage systems.

VIRTUALIZATION RISKS

The following are the top core risks developed by CSA's Virtualization Working Group.

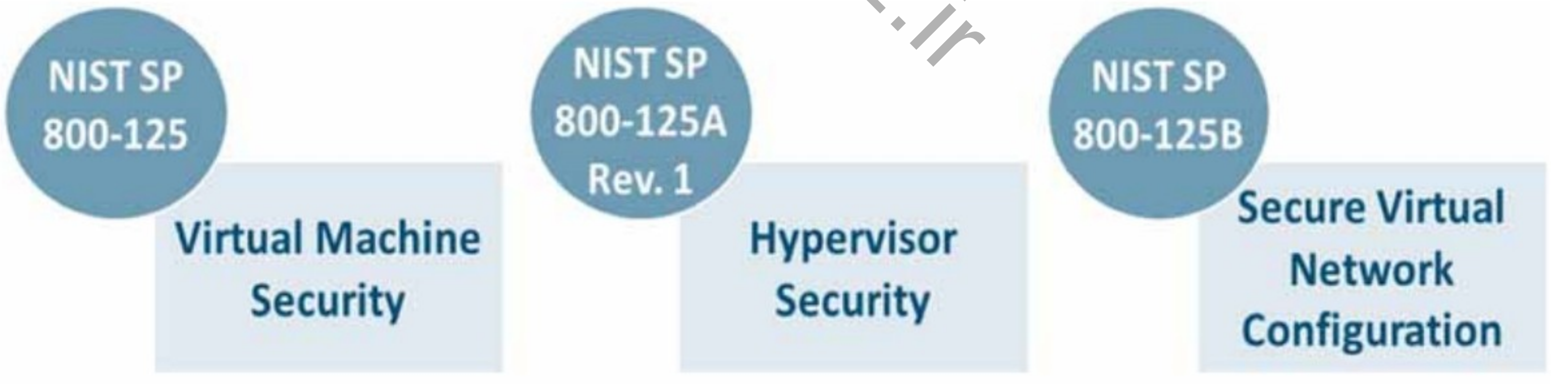
Risk	Summary
1. VM sprawl	Uncontrolled proliferation of VMs can lead to an unmanageable condition of unpatched and unaccounted-for machines.
2. Sensitive data within a VM	Data confidentiality within VMs can be compromised because data can be easily transported and tampered with.
3. Security of offline and dormant VMs	Dormant and offline VMs can eventually deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities.
4. Security of preconfigured (golden image) VM/active VMs	VMs exist as files on a virtualization platform, which can lead to unauthorized access, resulting in machine configuration changes or viral payload injection into the platform's virtual disks.
5. Lack of visibility into and control over virtual networks	Lack of visibility into and control over internal software-based virtual networks created for VM-to-VM communications hinders existing security policy enforcement in most organizations.
6. Resource exhaustion	Software-defined virtual networks can cause network security breaches because traffic over virtual networks may not be visible to security protection devices on the physical network.
7. Hypervisor security	A surface by which hackers can potentially gain unauthorized access to the VMs—guest OSs—hosted on it.
8. Unauthorized access to hypervisor	Administrative access controls to the hypervisor may not be adequate for protection against potential hacker attacks.
9. Account or service hijacking through the self-service portal	Self-service portal increases exposure to risks such as account or service hijacking through more administrative privileges than are typically granted to end users.
10. Workload of different trust levels located on the same server	VMs with mission-critical workloads reside on the same host as less-critical VMs, resulting in a virtual environment of mixed trust levels.
11. Risk due to cloud service provider API	Can pose security risks due to account/authentication enterprise identification, authentication, policy management, and governance framework(s) may not naturally extend into the public cloud.

VIRTUALIZATION SECURITY CONCERNS

- Virtual risks are present because virtualization adds additional layers of complexity.
- Not only does a CISO need to be concerned with the risk inherent to the physical host environment, but also with the virtualized technology.
- Securing virtualized infrastructure includes:
  - Ensuring that cyberattacks beginning at the physical host do not permeate into the virtualized environment.
  - Tracking and monitoring Virtual Machines (VMs) to identify and manage virtual assets.
  - Implementing granular standard security templates for VM environments.
  - Maintaining control and authority over each VM to prevent unauthorized access.
  - Deploying consistent security policies across the virtualized infrastructure.
  - Implementing security solutions specifically designed to protect a virtualized environment (such as antimalware, firewalls, and IPS).
  - Ensuring security patches are applied to VM environments.

VIRTUALIZATION SECURITY CONTROLS

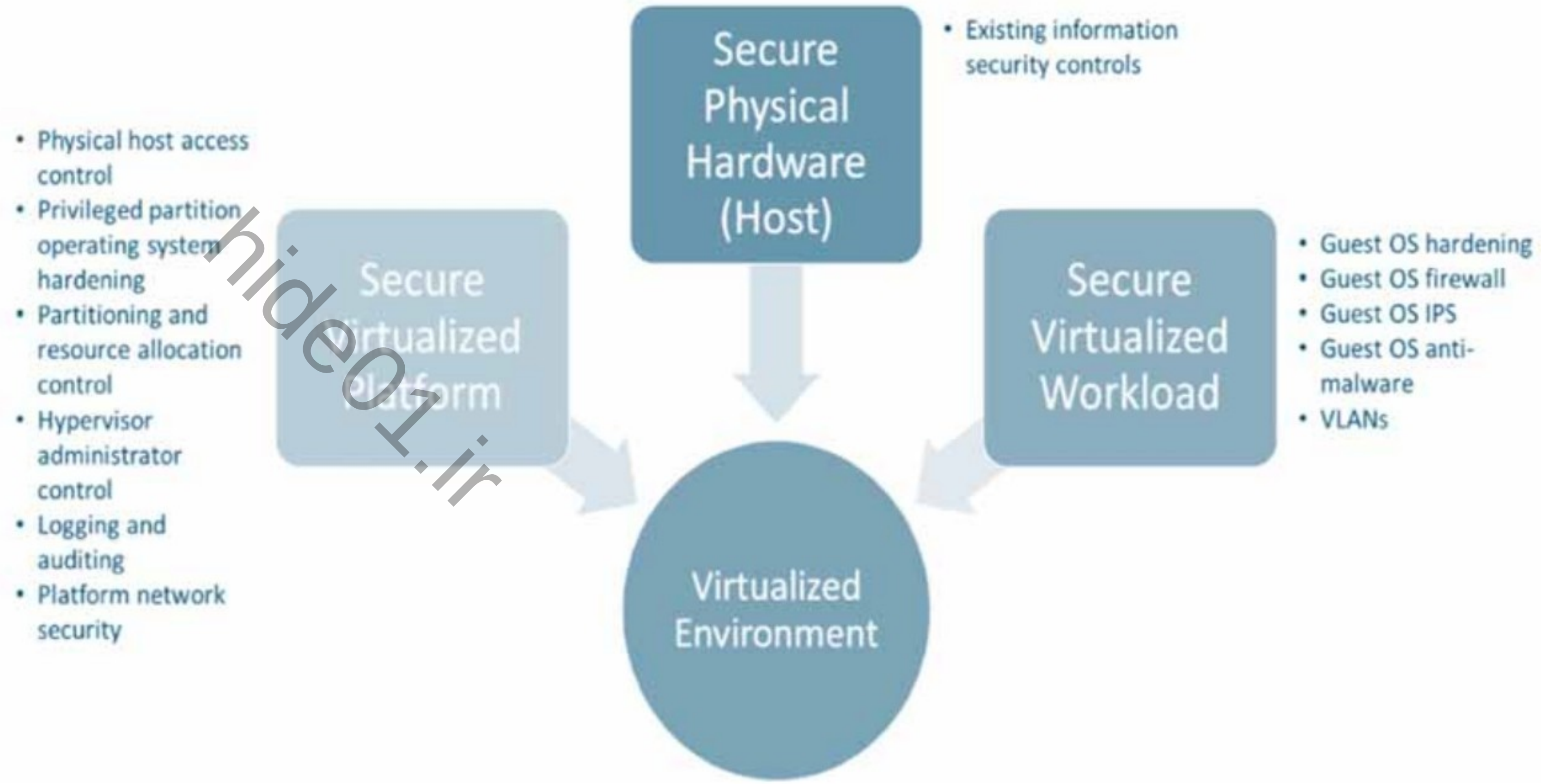
- NIST provides catalogues of guidance on how organizations can manage threats and vulnerabilities inherent to virtualized environments.
- The following presents the family of NIST special publications focused on protecting virtualized environments:



NIST SP Virtualization Protection Guidance

VIRTUALIZATION SECURITY REFERENCE MODEL

The virtualized reference model provides the types of security controls that can be applied within virtualized environments.



- Physical host access control
- Privileged partition operating system hardening
- Partitioning and resource allocation control
- Hypervisor administrator control
- Logging and auditing
- Platform network security

Secure Virtualized Platform

Secure Physical Hardware (Host)

- Existing information security controls

Secure Virtualized Workload

- Guest OS hardening
- Guest OS firewall
- Guest OS IPS
- Guest OS anti-malware
- VLANs

Virtualized Environment

Virtualized Security Reference Model

8. CLOUD COMPUTING SECURITY

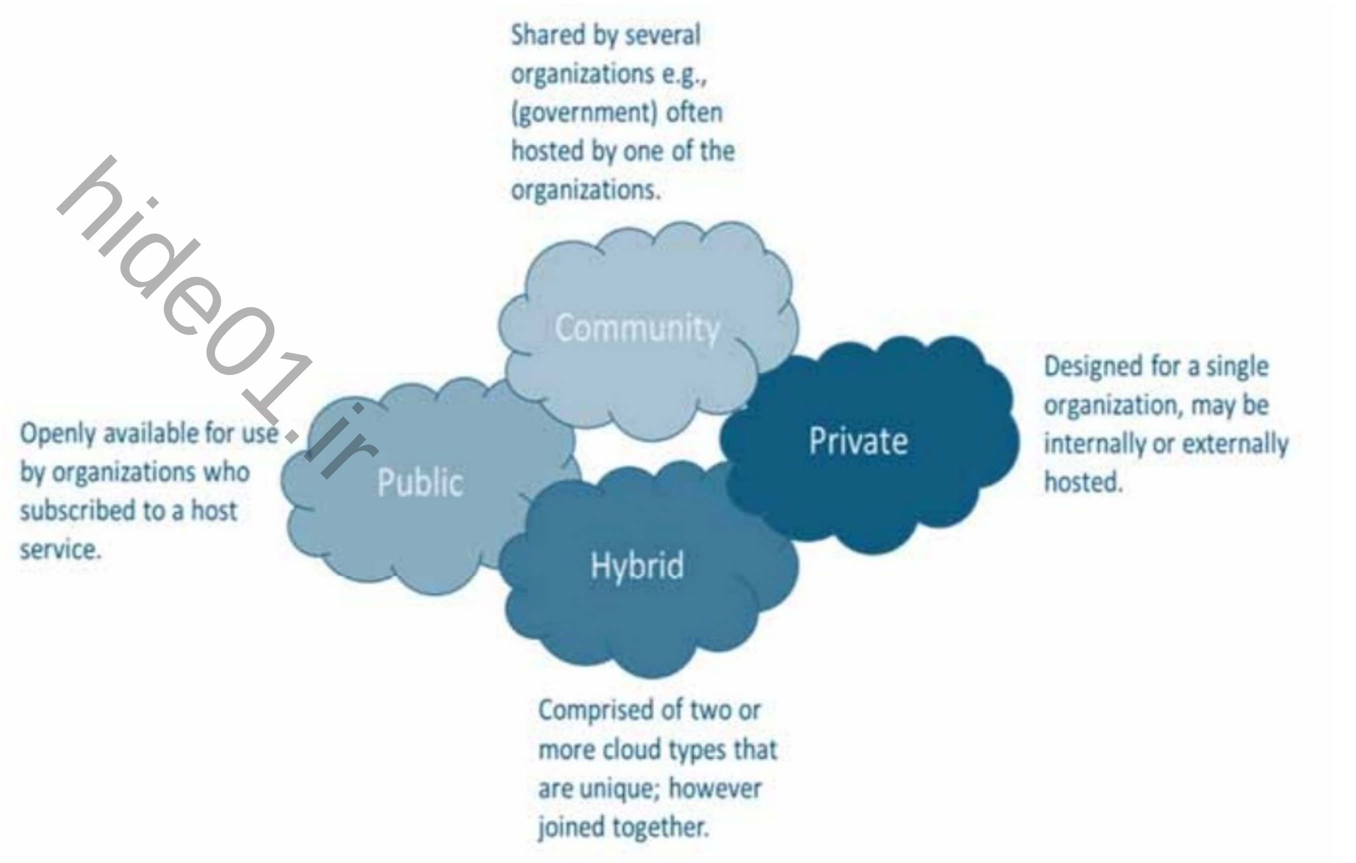
CLOUD COMPUTING SECURITY

- Most organizations use some amount of cloud-based infrastructure.
- CISOs should understand cloud technology and how to protect information processed or stored in it.
- Cloud computing security includes methods, practices, and solutions to protect an organization's internal, external, or hybrid cloud computing environments.
- As the CISO of your organization, you will need to instill business and user confidence in the security of cloud computing.

OVERVIEW OF CLOUD COMPUTING

- Cloud computing is delivery of computing services over the Internet and can consist of server processing, data storage, application operations, databases, network services, software, other IT services.

The 4 Types of Cloud Computing



Shared by several organizations e.g., (government) often hosted by one of the organizations.

Openly available for use by organizations who subscribed to a host service.

Designed for a single organization, may be internally or externally hosted.

Comprised of two or more cloud types that are unique; however joined together.

OVERVIEW OF CLOUD COMPUTING (CONT'D)

Most cloud computing services fall into three broad categories.

Infrastructure as a Service (IaaS) is the most basic category of cloud computing services. With IaaS, you basically pay for the usage of IT infrastructure such as servers and VMs, storage, networks, operating systems.

Platform as a Service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications.

Software as a Service (SaaS) is a method for delivering software applications on demand using a subscription payment model.

SECURITY AND RESILIENCY CLOUD SERVICES

- With the wide adoption of cloud computing came the emergence of specialized cloud services for information security and disaster recovery.
- As a CISO, you might consider analyzing these specialized cloud computing services and compare them to similar services provided by your IS organization.
- The following are the primary categories of security and resiliency cloud services:
  - Security as a Service (SECaaS).
  - Backup as a Service (BaaS).
  - Disaster Recovery as a Service (DRaaS).

CLOUD SECURITY CONTROLS

- The leading authority on cloud computing security controls is the Cloud Security Alliance.
  - Founded in 2008, CSA is an international member-driven organization.
  - It is chartered with promoting the use of best practices for providing security assurance within cloud computing.
  - CSA certifies cloud security practitioners, publishes the Cloud Control Matrix (CCM), and maintains a registry of certified secure cloud services providers.

CLOUD SECURITY CONCERNS

- The CSA isolated the top threats – the Treacherous 12, to cloud computing documentation. A report included the following exposures and threats associated with cloud environments:
  - Data breach.
  - Poor identity and access management.
  - Insecure APIs and interfaces.
  - System vulnerabilities.
  - Account hijacking.
  - Malicious insiders.
  - Advanced persistent threat (APT).
  - Data loss.
  - Insufficient due diligence.
  - Abuse and nefarious use of cloud services.
  - Denial-of-service.
  - Shared technology vulnerabilities.

CLOUD COMPUTING PROTECTION CONSIDERATIONS

The following are unique cloud security controls CISOs should understand:

Cloud access security broker (CASB) is a technology for controlling access from internal networks to external cloud resources and back.

Cloud application security is applied to internal physical and virtual infrastructure and data and often incorporates cloud vendor capabilities.

Cloud computing auditing should be included as a mandatory baseline in cloud support contracts, with regular monitoring, auditing, and reporting by the security function.

CLOUD COMPUTING PROTECTION CONSIDERATIONS (CONT'D)

Cloud Data Protection

Cloud operations have the same or higher risks as internal operations. This includes theft or unauthorized disclosure of data, risk of tampering or modification of data, and the risk of loss or of unavailability of data.

Cloud Access Control

The cloud service provider should have a secure system for provisioning and managing users, systems, and services in their cloud solution.

Cloud Service Agreements

Contracts should assure that applications and data hosted in the cloud are secured in accordance with the organizational security and compliance policies, to include acceptable levels of availability.

9. TRANSFORMATIVE TECHNOLOGIES

TRANSFORMATIVE TECHNOLOGIES

- Transformative technologies are those that have the potential to dramatically change or disrupt technology industries.
- Many technologies come and go, and some are short-lived.
- CISOs should pay attention to large-scale investment trends in next-generation technologies.
- Securing new technologies can be extremely challenging in terms of time to implement and supporting resource costs.
- Business value must be taken into consideration.

ARTIFICIAL INTELLIGENCE

- Artificial intelligence (AI) is becoming central to security products.
  - This includes SIEM, IPS, antimalware, IDS, sandbox, endpoint, and secure email solutions.
- AI is typically used to solve specific problems.
  - Systems are 'trained', meaning constantly changing weighted values are applied to problem solution data sets.
  - You cannot simply use it to solve other problems – it is trained to solve specific problems.
  - AI systems can be joined to solve larger problems, such as driving a car.
- AI is powerful and has already been adopted by cybercriminals for gaining faster unauthorized access.

AUGMENTED REALITY

- Augmented reality (AR) is a technology whereas computer-generated images, sounds, and other human inputs are superimposed over a user's real world, resulting in a created sense of reality.

- This technology is highly appealing to security professionals:
  - For instance, security operations centers could implement a superimposed view of a SOC environment for SecOps personnel.
    - In this example, a security organization would no longer need to build physical SOCs.
    - Personnel could manage security operations from anywhere on the planet.

AUTONOMOUS SOC

- Autonomous technology refers to machines that act independently of humans to perform tasks that are either too expensive or rote for humans.
- This technology has been widely developed in the past, such as in manufacturing line implementations.
- Now we are seeing it move to roles such as autonomous or self-driving automobiles and trucks.
- This technology is also beginning to emerge in the information security industry.
  - An example is an automated honeypot that builds a replica environment and manages attacks and alerts without SecOps personnel intervention.

DYNAMIC DECEPTION

- Many security professionals believe that simply defending against attackers is insufficient.
- Deception is based on the theory of dynamic behavior whereas a self-learning system is used to dynamically create a false environment to attract attackers.
- Called honeypots or honeynets, these systems are designed to lure an attacker to a replication of an organization's assets and information, leading them away from the real ones.
- The resulting attacks can provide deeper insight into the attacker's intentions, such as learning the types of assets being targeted.

SOFTWARE-DEFINED CYBERSECURITY

- Some vendors provide products that automatically share or distribute threat intelligence across an environment.
- These products use threat and attack data to communicate and adjust security controls across an IT environment.
- These technologies are called Unified Threat Management (UTM) platforms.
- They use proprietary operating systems or application overlays, connecting to security devices within the infrastructure.
- They allow a broad security fabric implementation by creating an environment of connected but disparate security technologies (such as firewalls, sandboxes and IPS) that automatically detect and block malicious traffic and distribute that threat intelligence to other systems.

DOMAIN 4
END

DOMAIN 4 SUMMARY

DOMAIN 4: GENERAL

- There are thousands of information security technologies, products, and services.
- RSA reports that the average number of security products used by enterprises ranges from 15 to 130 depending on company size.
- Cloud-first strategies are driving an unprecedented increase in adoption of cloud services.
- Core technologies covered in this domain represent the most widely used information security technologies.

DOMAIN 4: ACCESS CONTROL

- CISOs must develop an access control plan leveraging need-to-know and least privilege models.
- Social engineering, unauthorized access, and privilege escalation are the causes of some of the most egregious data breaches.
- The primary goal of access control is to minimize unauthorized access to information and assets.
- The triple A (AAA) of access control is authentication, authorization, and auditing.
- Multifactor authentication should be used when available and pragmatic.
- The CRUD Security Matrix describes Create, Read, Update, or Delete privileges.

DOMAIN 4: ACCESS CONTROL - CONTINUED

- User behavior analytics and management is an effective way to baseline an access control plan. Behavior analytics focuses on access habits of users.
- The four primary types of access control models consists of discretionary, mandatory, role-based, and attribute-based access control.
- Access administration includes provisioning, monitoring, and terminating access.

DOMAIN 4: PHYSICAL SECURITY

- CISOs do not typically manage physical security; however, this domain can be an important component of an information security program.
- ISO and NIST both recommend CISO involvement in physical security planning.
- Physical security is an essential early line of defense for asset protection.
- CISOs can provide a unique perspective of physical security that may be overlooked by facilities planning and management personnel.
- CISOs should be familiar with the available range of physical protection controls.

DOMAIN 4: SCIF

- A Sensitive Compartmented Information Facility (SCIF) is a secure area with protections to ensure that highly-sensitive information within the SCIF cannot be compromised.
- SCIFs are often used to house digital forensic labs.
- SCIF computers and telecommunication equipment conform to TEMPEST emanations specification as directed by a Certified TEMPEST Technical Authority (CTTA).

DOMAIN 4: DATACENTER

- Data center resiliency is based on tiers.
  - Tiers range from 1 to 4 with specific uptime and redundancy requirements for each tier.
  - The higher the tier, the higher the site availability.
- The Uptime Institute, a division of 451 Group publishes the widely used datacenter Tier Standard.
- CISOs must understand the uptime capability of data centers and cloud datacenter service providers.

DOMAIN 4: NETWORK SECURITY

- CISOs create the standards used by the network support function.
- CISOs build a relationships with all IT teams, to include the network security team.
- CISOs need to clearly understand how their network is designed and secured.
- ISO/IEC 27033 provides detailed guidance on securing networks.
- CISOs should be familiar with Internet, wireless, RF, and network routing protocols.

DOMAIN 4: NETWORK SECURITY - CONTINUED

Widely deployed network security controls include:

Boundary

- Firewalls
- Edge routers
- IDS
- Secure gateways
- VPNs

Internal network

- Firewalls
- IPS
- Network encryption
- Network segmentation

DOMAIN 4: ENDPOINT PROTECTION

- Endpoint protection is the practice of securing user devices (mobile, IoT, laptop) when connected to a network or used offline.
- Endpoints are attractive targets for hackers because of users that can potentially be socially engineered.
- Endpoint protection begins with user security awareness training.
- Endpoint device hardening covers a wide range of security controls consisting of whitelisting, hygiene, encryption enablement, and others.

DOMAIN 4: APPLICATION SECURITY

- CISOs typically do not own application security; however, they must be intimately involved with the practices of securing applications.
- Programmers are paid to write code, not secure applications.
- Standard types of application testing methods include DAST, SAST, IAST, and bug bounty platforms.
- DevSecOps integrates security in every phase of the application development lifecycle.
- Waterfall and Agile are the two primary application development models and each requires unique security considerations.

DOMAIN 4: DATABASE SECURITY

- Databases and file shares typically store most of an organization's critical data.
- Securing these data stores is a high priority.
- A broad range of security controls are available to protect databases and file shares including:
  - Isolation tactics.
  - Hardening and hygiene.
  - Firewalls.
  - Encryption.
  - Privilege account management.
  - Monitoring.

DOMAIN 4: ENCRYPTION

- Encryption is the process of encoding clear text into cypher text to prevent unauthorized users from accessing confidential information.
- A cryptosystem typically consists of three algorithms: key generation, encryption, and decryption.
- Blockchain is an expanding list of records called blocks that are linked cryptographically as a chain.
- Digital signatures provide a mechanism to verify that a message came from the sender, providing nonrepudiation.

DOMAIN 4: ENCRYPTION - CONTINUED

- Public Key Infrastructure (PKI) provides the mechanisms that ensure public keys belong to who they say they do.
- Hashing is not encryption, but it is a one-way transform providing a value of the original data.
- Hashing provides message integrity verification.
- Hash functions perform a one-way transformation of a character string into a fixed-length value or key that represents the original string.

DOMAIN 4: VIRTUALIZATION SECURITY

- Virtualized environments can inherit the vulnerabilities of their physical operating systems or hosts.
- Virtual environments contain many of the same risks as physical environments.
- The CSA Virtualization Working Group provides threat intelligence and guidance for virtualized security management.
- NIST publishes comprehensive guides for securing virtualized environments.

DOMAIN 4: CLOUD SECURITY

- Cloud computing includes private, hybrid, public, and community clouds.
- The three most popular cloud computing services consist of IaaS, PaaS, and SaaS (infrastructure, platform, and software).
- Cloud services can provide recovery services and capabilities.
- The Treacherous 12 published by CSA outlines the top cloud computing threats.
- Cloud Access Security Broker (CASB) is a technology that controls access from internal networks to external cloud resources and back.

DOMAIN 4: TRANSFORMATIVE TECHNOLOGIES

- Transformative technologies are those that have the potential to dramatically change or disrupt technology industries.
- Artificial intelligence (AI) is becoming central to security products. This includes SIEM, IPS, antimalware, IDS, sandbox, endpoint, and secure email solutions.
- Augmented reality (AR) is a technology whereas computer-generated images, sounds, and other sensory inputs are superimposed over a user's real world, resulting in a created sense of reality.
- Autonomous technology refers to machines that act independently of humans to perform tasks that are either too expensive or rote for humans.

DOMAIN 4: TRANSFORMATIVE TECHNOLOGIES - CONTINUED

- Deception technology is based on the theory of dynamic behavior whereas a self-learning system is used to dynamically create a false environment to attract attackers.
- Software-defined security (SDS) is a type of security model in which information security in a computing environment is implemented, controlled and managed by security software versus hardware.

DOMAIN 4 PRACTICE QUESTIONS

PRACTICE QUESTIONS

1. Advanced Persistent Threat (APT) is **BEST** characterized by which of the following?

A. High volumes of unauthorized insider activities such as copying data onto portable storage devices or electronic destruction of high value assets.

B. Creative insertions of malicious code into applications and databases using known code vulnerabilities and weaknesses.

C. Continuous flooding of network perimeters with system requests causing long-term delays and interruptions.

D. Methodical advancement of unauthorized access across systems as valuable assets are discovered using a variety of penetration techniques.

PRACTICE QUESTIONS

2. A vulnerability assessment discovers that it is possible for an attacker to force an authorization step to take place before the authentication step is completed successfully.

What type of issue would allow for this compromise to take place?

A. Maintenance hook.
B. Backdoor.
C. Race condition.
D. Data validation error.

PRACTICE QUESTIONS

3. A cloud computing environment that allows data and applications to be shared between public and private clouds is **BEST** referred to as a?

A. Hybrid cloud.
B. Public cloud.
C. Community cloud.
D. Private cloud.

PRACTICE QUESTIONS

4. Which of the following physical security measures is **LEAST** effective at mitigating the tailgating?

A. Mantrap.
B. Biometric scanner.
C. User awareness training (UAT).
D. Turnstile.

PRACTICE QUESTIONS

5. If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the **BEST** control to safeguard data integrity?

A. Backup to tape.
B. Backup to a remote location.
C. Maintain separate VM backups.
D. Increase VM replication frequency.

C|CISO

CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER

Domain 5

INTRODUCTION

- This domain teaches students how:
  - To build a strategic plan.
  - To create an information security architecture.
  - To understand the elements of continuous process improvement.
  - To understand the fundamentals of finance.
  - To build an information security budget.
  - To understand the procurement lifecycle.
  - To create a vendor risk management program.
  - To perform third-party delivery assurance.

KNOWLEDGE ASSUMPTIONS

- Students are expected to have:
  - Some exposure to finance and procurement practices.
  - A working vocabulary of vendor risk management.
  - Basic familiarity of at least one enterprise architecture framework.
  - Basic understanding of how budgets work.
  - A fundamental understanding of the procurement terminology and functions.
  - A working knowledge of managing risk associated with third parties.

STRATEGIC PLANNING, FINANCE, PROCUREMENT AND VENDOR MANAGEMENT

DOMAIN 5

SECURITY PROGRAM MANAGEMENT AND OPERATIONS

DOMAIN OUTLINE

1. Strategic Planning
2. Designing, Development, and Maintaining an Enterprise Information Security Program
3. Understanding the Enterprise Architecture (EA)
4. Finance
5. Procurement
6. Vendor Risk Management

Summary and Practice Questions

1. STRATEGIC PLANNING

1. STRATEGIC PLANNING

- The strategic plan must be written clearly and be concise to be understood.
- In the plan you will detail the organization's information security and risk management goals within the time frame of the plan.
- The plan includes the program roadmap, which is a sequence of major milestones that will achieve the security program goals.
- Success of the security strategy relies on:
  - The CISO's participation in organizational strategic planning.
  - The maturity of the organization.
  - The effectiveness of governance activities supporting the organization.

1. STRATEGIC PLANNING - CONTINUED

- According to the Association for Strategic Planning (ASP), strategic planning has a high impact on overall organizational success.
- Low-success organizations do not perfrom strategic planning as key activity.
- Strategic planning determines:
  - Goals for given amount of time, typically for the next 1, 3, and 5 years.
  - How the organization is going to achieve them.
  - How the organization will know if it has been successful in achieving program goals.

1.1 UNDERSTANDING THE ORGANIZATION

- Understanding an organization helps to identify the operational boundaries within which the information security program exists.
- CISOs works within these boundaries to:
    - Help protect the organization through risk management.
    - Create a culture of security awareness.
    - Deliver to stakeholder expectations.
    - Obtain program support.
    - Determine metrics to measure program success.

1.1.1 UNDERSTANDING THE BUSINESS STRUCTURE

There are several organizational structures a CISO is likely to work within:

General Corporations are also known as a C corporation, this is the most common corporate structure. It can have an a very large number of stockholders, with vested interest in the company dispersed widely (such as stocks and stock type levels).

Closed Corporations have limited stockholders with no public financial shares and is limited within some countries, territories or states.

Subchapter S Corporations are general corporations with special tax status whereas owners are taxed versus the company.

Limited Liability Companies (LLCs) are typically a proprietorship or partnership. Many business owners prefer LLCs because they combine the limited liability protection of a corporation with the pass-through taxation to individuals of a partnership.

1.1.2 DETERMINING AND ALIGNING BUSINESS AND INFORMATION SECURITY GOALS

- Alignment creates a relationship where both the business and the information security department can achieve their goals while assisting one another.
- Aligning the information security program with the company's goals makes the program an integral part of the business, increasing the investment value.

The following matrix provides an example of how CISOs can align business and information security goals.

Business Goal	Information Security Program Goal
1. Reduce risk to the business.	1. Manage or mitigate operational risk that could impact critical business functions.
2. Comply with all industry legal and regulatory compliance statutes.	2. Implement information security controls to ensure compliance with legal and regulatory requirements.
3. Provide customers with effortless buying experience.	3. Provide secure and seamless online customer transactions.
4. Lead competition through first to market advantage of new products.	4. Leverage security as an enabler to reduce time to market.
5. Maintain a disciplined approach to spending and investment.	5. Deploy automation to reduce the manual cost of securing assets and information.

1.1.3 IDENTIFYING KEY SPONSORS, STAKEHOLDERS, AND INFLUENCERS

There are three roles that CISOs interact with to build support for their security program

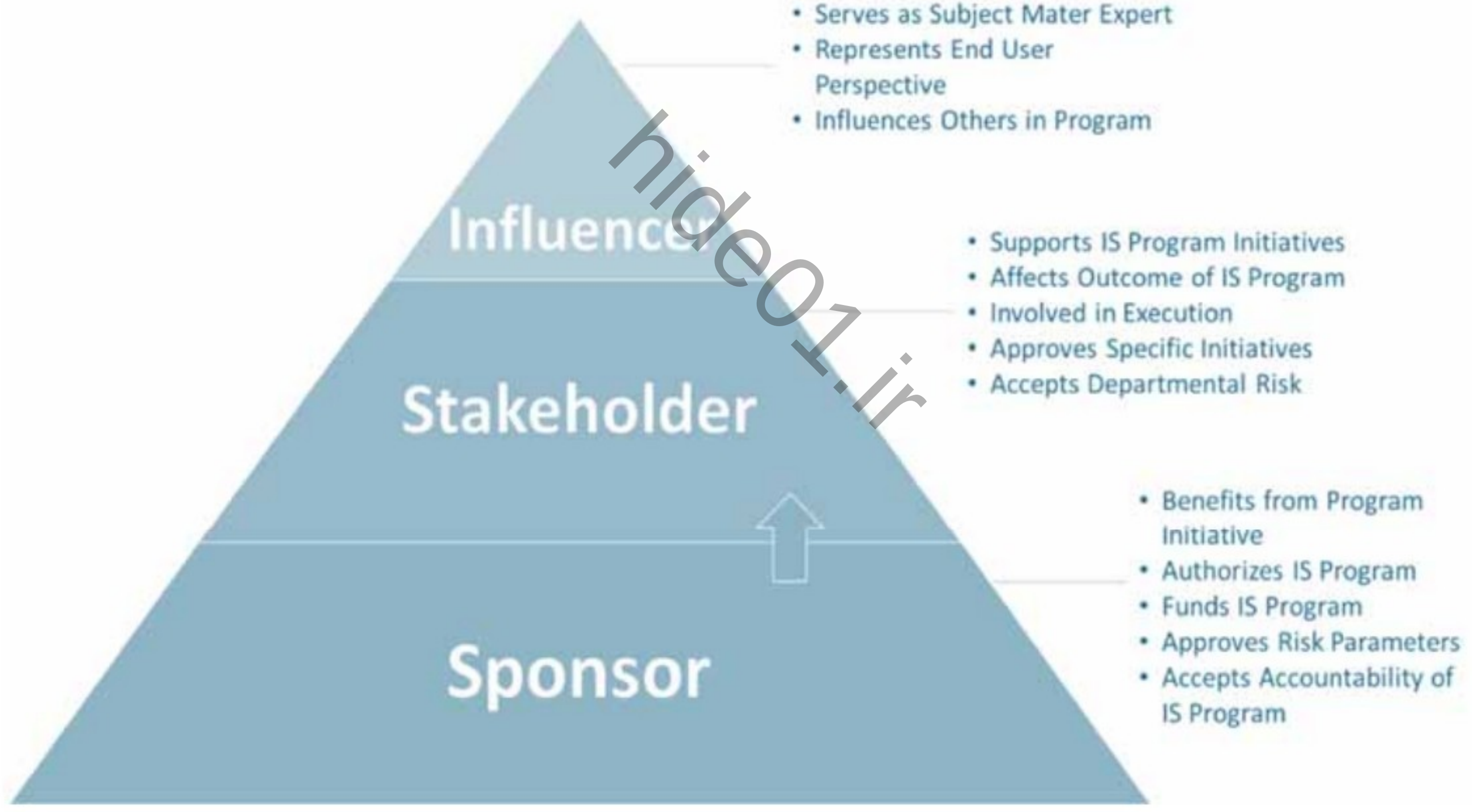
A **sponsor** typically has financial interest in outcomes. They fund projects, programs, and functions within the organization.

Stakeholders have interest in outcomes, but their influence is limited compared with that of sponsors.

Influencers are those within the organization with a respected opinion. They can be instrumental in promoting various information security program initiatives.

1.1.3 IDENTIFYING KEY SPONSORS, STAKEHOLDERS, AND INFLUENCERS - CONTINUED

The following summarizes the relative importance of the three roles.



Influencer

- Serves as Subject Mater Expert
- Represents End User Perspective
- Influences Others in Program

Stakeholder

- Supports IS Program Initiatives
- Affects Outcome of IS Program
- Involved in Execution
- Approves Specific Initiatives
- Accepts Departmental Risk

Sponsor

- Benefits from Program Initiative
- Authorizes IS Program
- Funds IS Program
- Approves Risk Parameters
- Accepts Accountability of IS Program

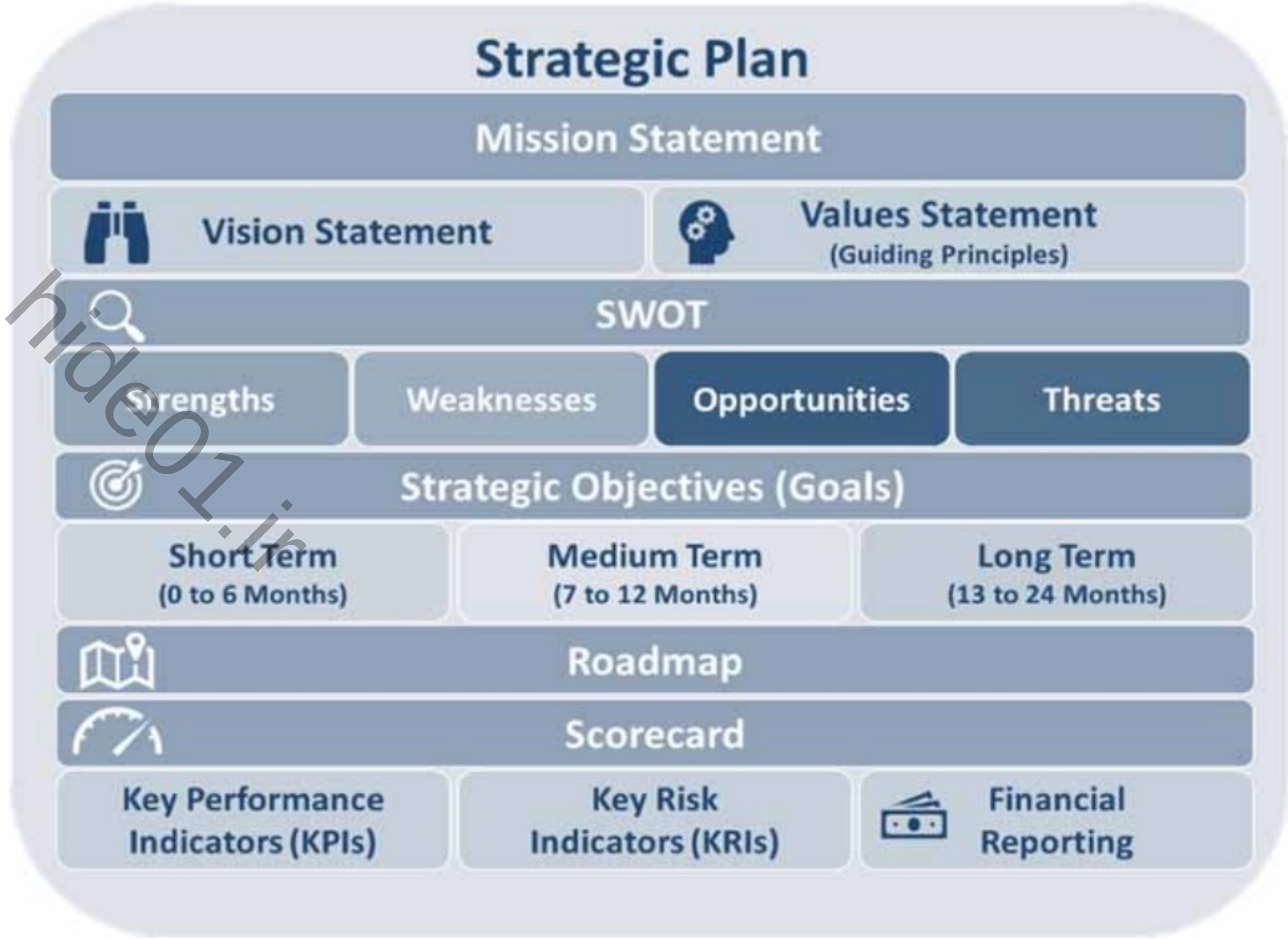
Information Security Program Support Pyramid

1.1.4 UNDERSTANDING ORGANIZATIONAL FINANCIALS

- Effective CISOs clearly understand the finances of their organization.
- They can converse with senior management and business unit owners on financial topics.
- There are four important financial statements common to every organization:
  1. **Balance sheets** show what a company owns and what it owes at a fixed point in time.
  2. **Income statements** show how much money an organization collected and spent over a given period.
  3. **Cash flow statements** show the exchange of money between an organization and external entities.
  4. **Shareholder equity statements** show changes in the vested interest of the company's shareholders during a specific period.

1.2 CREATING AN INFORMATION SECURITY STRATEGIC PLAN

The following framework provides guidance for the development of a strategic information security plan.



Strategic Plan

Mission Statement

Vision Statement

Values Statement
(Guiding Principles)

SWOT

Strengths

Weaknesses

Opportunities

Threats

Strategic Objectives (Goals)

Short Term
(0 to 6 Months)

Medium Term
(7 to 12 Months)

Long Term
(13 to 24 Months)

Roadmap

Scorecard

Key Performance Indicators (KPIs)

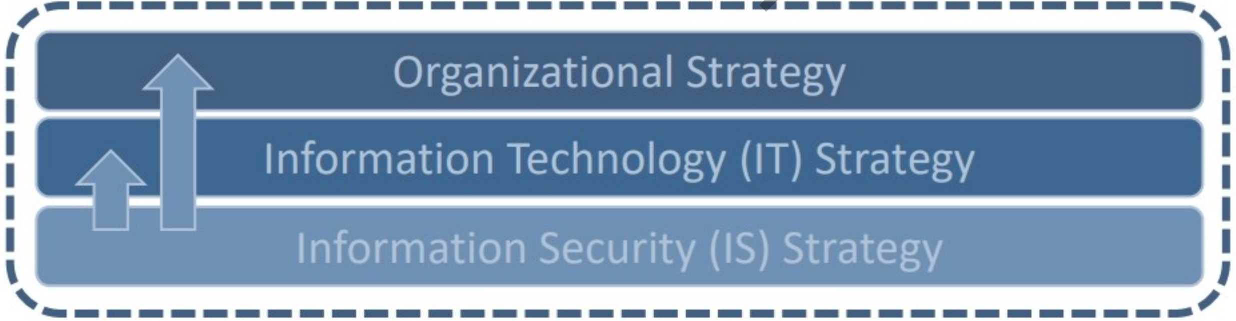
Key Risk Indicators (KRIs)

Financial Reporting

Strategic Information Security Plan Framework

1.2.2 ALIGNMENT TO ORGANIZATIONAL STRATEGY AND GOALS

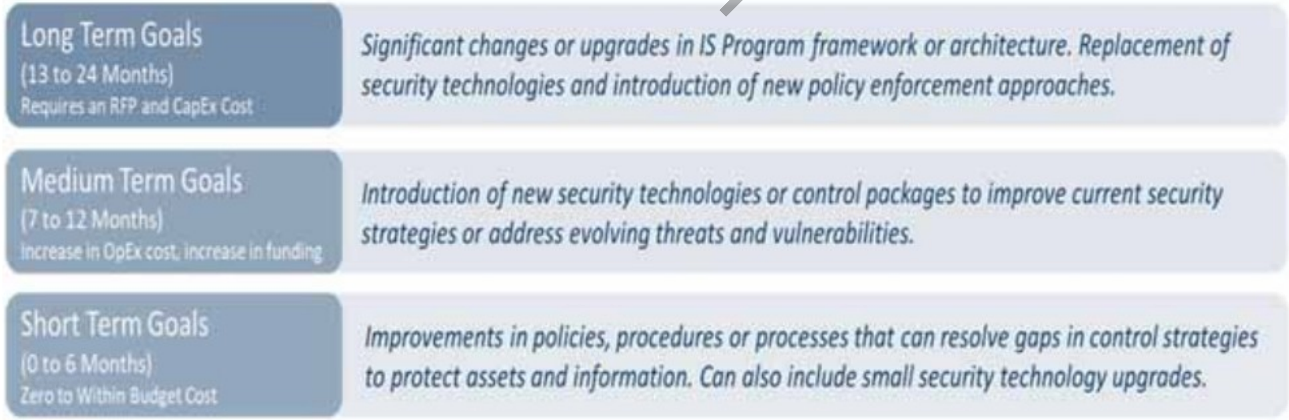
- One of the most important responsibilities of a CISO is to align the information security program to an organization's strategy and goals.
- However, it is not just the corporate strategy that the program must align with, but also with the IT organization goals and constraints.


Organizational Strategy
Information Technology (IT) Strategy
Information Security (IS) Strategy

Goals Alignment Relationship Model

1.2.3 DEFINING TACTICAL SHORT, MEDIUM, AND LONG-TERM INFORMATION SECURITY GOALS

- Information security goals are typically time bound to assure they are completed according to stated commitments.
- Tactical goals tend to occur within a shorter time period, such as 12 to 24 months, whereas strategic goals are accomplished in a longer time frame (3 to 5 years is common).
- The following are examples of tactical goals:



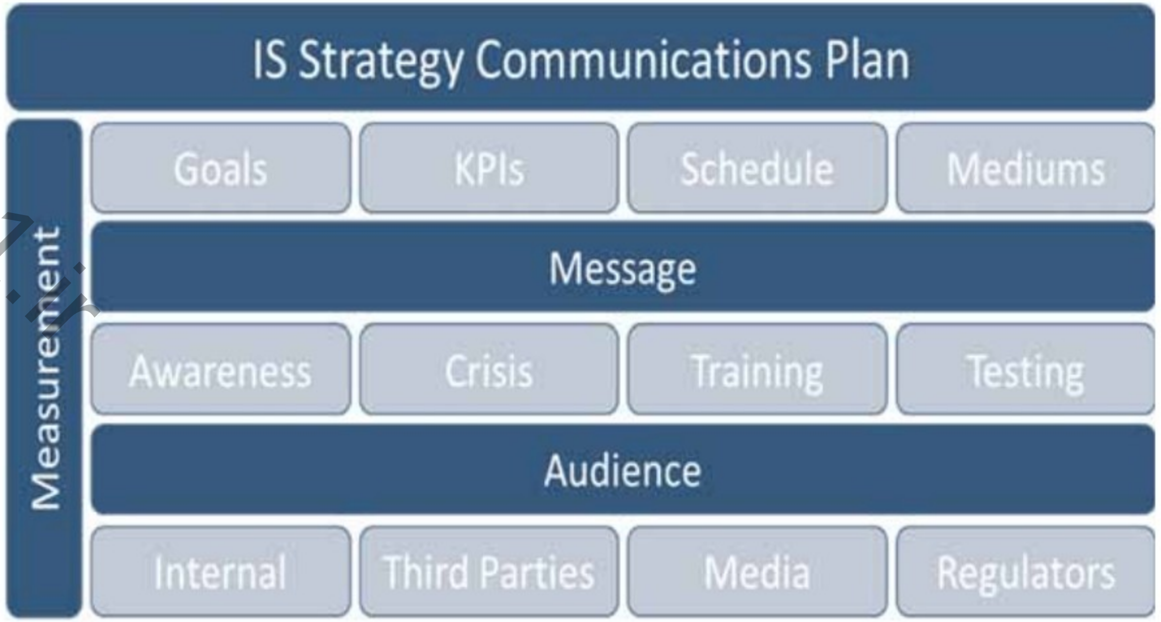
Long Term Goals (13 to 24 Months) Requires an RFP and CapEx Cost	*Significant changes or upgrades in IS Program framework or architecture. Replacement of security technologies and introduction of new policy enforcement approaches.*
Medium Term Goals (7 to 12 Months) Increase in OpEx cost, increase in funding	*Introduction of new security technologies or control packages to improve current security strategies or address evolving threats and vulnerabilities.*
Short Term Goals (0 to 6 Months) Zero to Within Budget Cost	*Improvements in policies, procedures or processes that can resolve gaps in control strategies to protect assets and information. Can also include small security technology upgrades.*

Tactical Time-Bound Goal Overview

1.2.4 INFORMATION SECURITY STRATEGY COMMUNICATION

- A communication plan is another important aspect of the information security strategy.
- It establishes the methods and processes defining what types of medium will be used for communicating the security mission, vision, values, and status.

Framework for developing a communications plan for an information security strategy.



Information Security Strategy Communications Plan

1.2.5 CREATING A CULTURE OF SECURITY

- Unless an organizational culture is security-aware, CISOs will have difficulty in protecting information and assets.
- Sociologists have defined culture as the collective customs, beliefs, and general attitude of a group.
- The following are four primary ways to influence the culture of an organization:
  - Emphasize what is important.
  - Reward good behavior.
  - Discourage bad behavior.
  - Model the behavior you want.

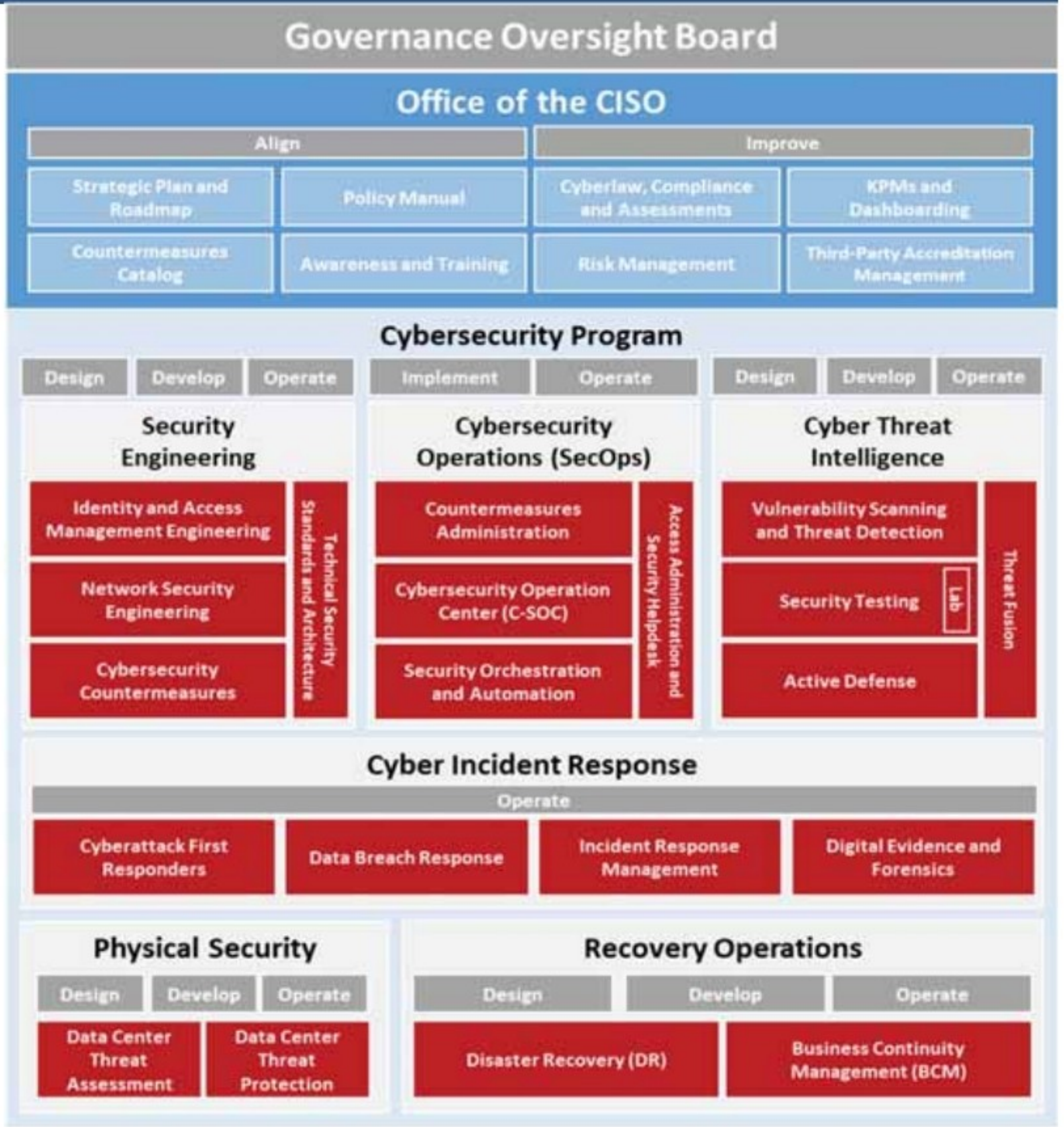
2. DESIGNING, DEVELOPING, AND MAINTAINING AN ENTERPRISE INFORMATION SECURITY PROGRAM

2. DESIGNING, DEVELOPING, AND MAINTAINING AN ENTERPRISE INFORMATION SECURITY PROGRAM

- Before construction begins on a new home, homeowners and contractors must agree on what the house will look like when finished, as well as the number of rooms and their sizes.
- Building a cybersecurity program should be no different.
- Many organizations use either ISO 27001 or NIST CSF as a security program framework to guide toward the program's finished state.
- The finished state (or blueprint) identifies the structure and components of your information security program.
  - It is a representation of the finished product.

2. IS PROGRAM BLUEPRINT

A blueprint is a guide for making something and consists of drawings, or pictures to represent the services and functions of an information security program.



Governance Oversight Board

Office of the CISO

Align | Improve

Strategic Plan and Roadmap | Policy Manual | Cyberlaw, Compliance and Assessments | KPMs and Dashboarding

Countermeasures Catalog | Awareness and Training | Risk Management | Third-Party Accreditation Management

Cybersecurity Program

Security Engineering (Design | Develop | Operate): Identity and Access Management Engineering; Network Security Engineering; Cybersecurity Countermeasures; Technical Security Standards and Architecture

Cybersecurity Operations (SecOps) (Implement | Operate): Countermeasures Administration; Cybersecurity Operation Center (C-SOC); Security Orchestration and Automation; Access Administration and Security Helpdesk

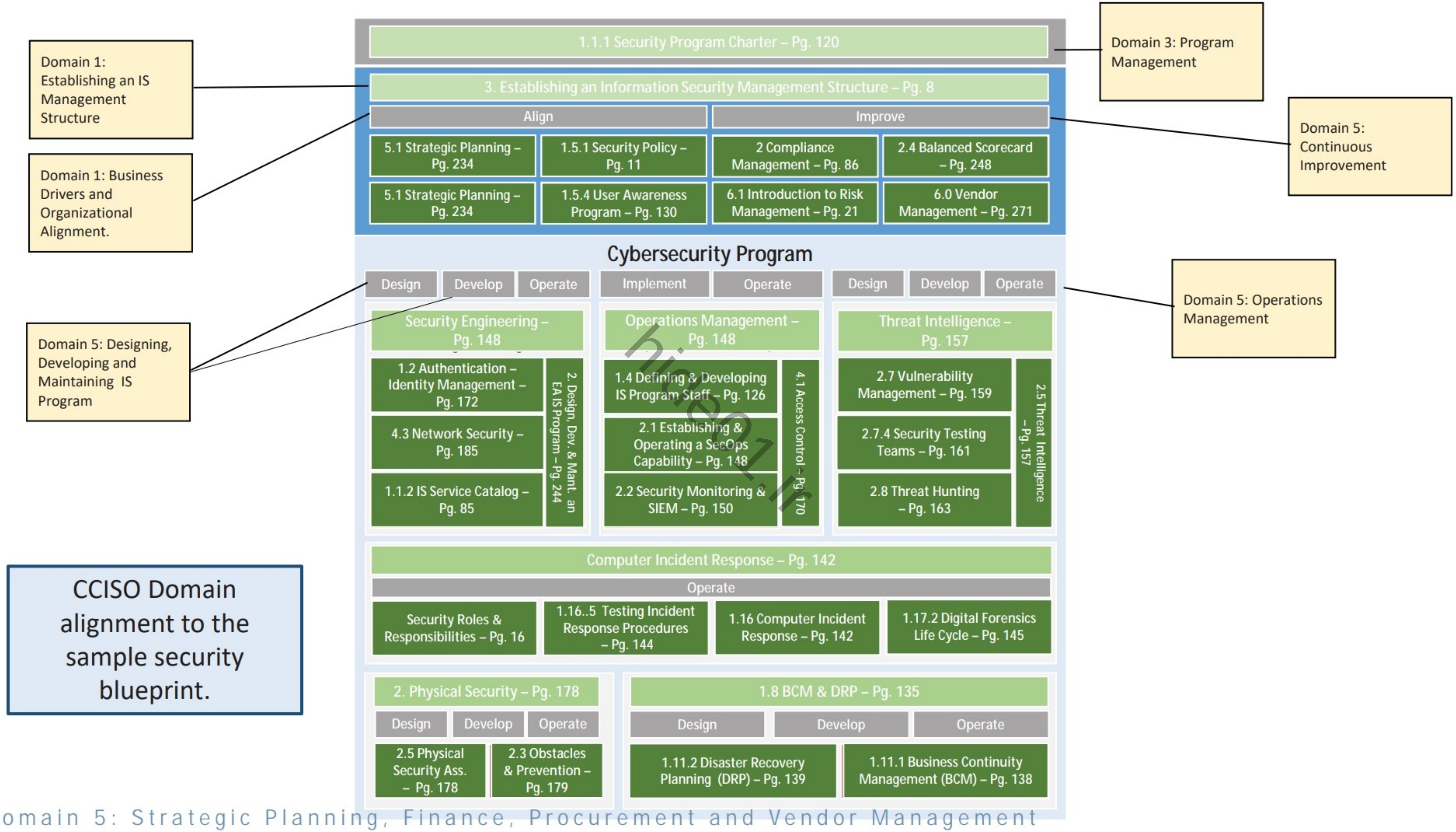
Cyber Threat Intelligence (Design | Develop | Operate): Vulnerability Scanning and Threat Detection; Security Testing; Lab; Active Defense; Threat Fusion

Cyber Incident Response (Operate): Cyberattack First Responders; Data Breach Response; Incident Response Management; Digital Evidence and Forensics

Physical Security (Design | Develop | Operate): Data Center Threat Assessment; Data Center Threat Protection

Recovery Operations (Design | Develop | Operate): Disaster Recovery (DR); Business Continuity Management (BCM)

Cybersecurity Program Blueprint.



1.1.1 Security Program Charter – Pg. 120

3. Establishing an Information Security Management Structure – Pg. 8

Align

Improve

5.1 Strategic Planning – Pg. 234

1.5.1 Security Policy – Pg. 11

2 Compliance Management – Pg. 86

2.4 Balanced Scorecard – Pg. 248

5.1 Strategic Planning – Pg. 234

1.5.4 User Awareness Program – Pg. 130

6.1 Introduction to Risk Management – Pg. 21

6.0 Vendor Management – Pg. 271

Cybersecurity Program

Design | Develop | Operate

Security Engineering – Pg. 148

1.2 Authentication – Identity Management – Pg. 172

4.3 Network Security – Pg. 185

1.1.2 IS Service Catalog – Pg. 85

2. Design, Dev. & Mant. an EA IS Program – Pg. 244

Implement | Operate

Operations Management – Pg. 148

1.4 Defining & Developing IS Program Staff – Pg. 126

2.1 Establishing & Operating a SecOps Capability – Pg. 148

2.2 Security Monitoring & SIEM – Pg. 150

4.1 Access Control – Pg. 170

Design | Develop | Operate

Threat Intelligence – Pg. 157

2.7 Vulnerability Management – Pg. 159

2.7.4 Security Testing Teams – Pg. 161

2.8 Threat Hunting – Pg. 163

2.5 Threat Intelligence – Pg. 157

Computer Incident Response – Pg. 142

Operate

Security Roles & Responsibilities – Pg. 16

1.16..5 Testing Incident Response Procedures – Pg. 144

1.16 Computer Incident Response – Pg. 142

1.17.2 Digital Forensics Life Cycle – Pg. 145

2. Physical Security – Pg. 178

Design | Develop | Operate

2.5 Physical Security Ass. – Pg. 178

2.3 Obstacles & Prevention – Pg. 179

1.8 BCM & DRP – Pg. 135

Design | Develop | Operate

1.11.2 Disaster Recovery Planning (DRP) – Pg. 139

1.11.1 Business Continuity Management (BCM) – Pg. 138

Domain 1: Establishing an IS Management Structure

Domain 1: Business Drivers and Organizational Alignment.

Domain 5: Designing, Developing and Maintaining IS Program

Domain 3: Program Management

Domain 5: Continuous Improvement

Domain 5: Operations Management

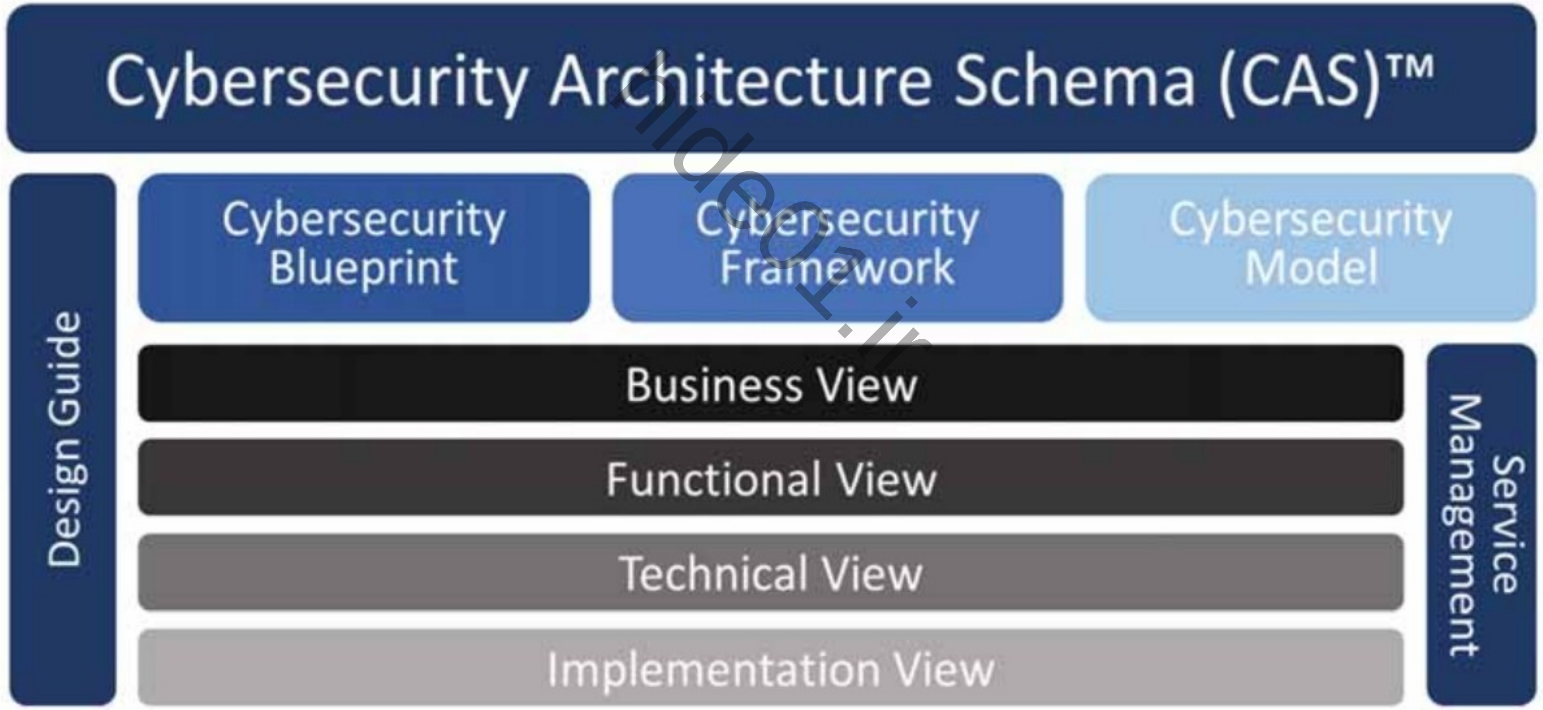
CCISO Domain alignment to the sample security blueprint.

2.1 ENSURING A SOUND PROGRAM FOUNDATION

- An information security program must have a sound architecture as its foundation.
- An architecture is comprised of the major components that make up a whole.
- CISOs should think in terms of architecture as a ‘full menu’
  - What does this program look like and functionally provide to the organization?

2.2 ARCHITECTURE VIEWS

The following provides a view of an information security architecture as a schema:



Cybersecurity Architecture Schema (CAS)™. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License)

2.2 ARCHITECTURAL VIEWS - CONTINUED

Four views are generally used in information security program designs to provide relevance, simplicity, and effectiveness.

Business should answer the question of why something is being done. It determines requirements and concerns of the users from their business perspective.

Functional answers the question of what should be done. This view focuses on the capabilities to be built within the cybersecurity program.

Technical answers the question how something is accomplished. The prime consideration in this view is establishing key capabilities.

Implementation answers the question of what will be used to accomplish goals. Determination is made regarding the resources that are required to implement the technical view.

2.3 CREATING MEASUREMENTS AND METRICS

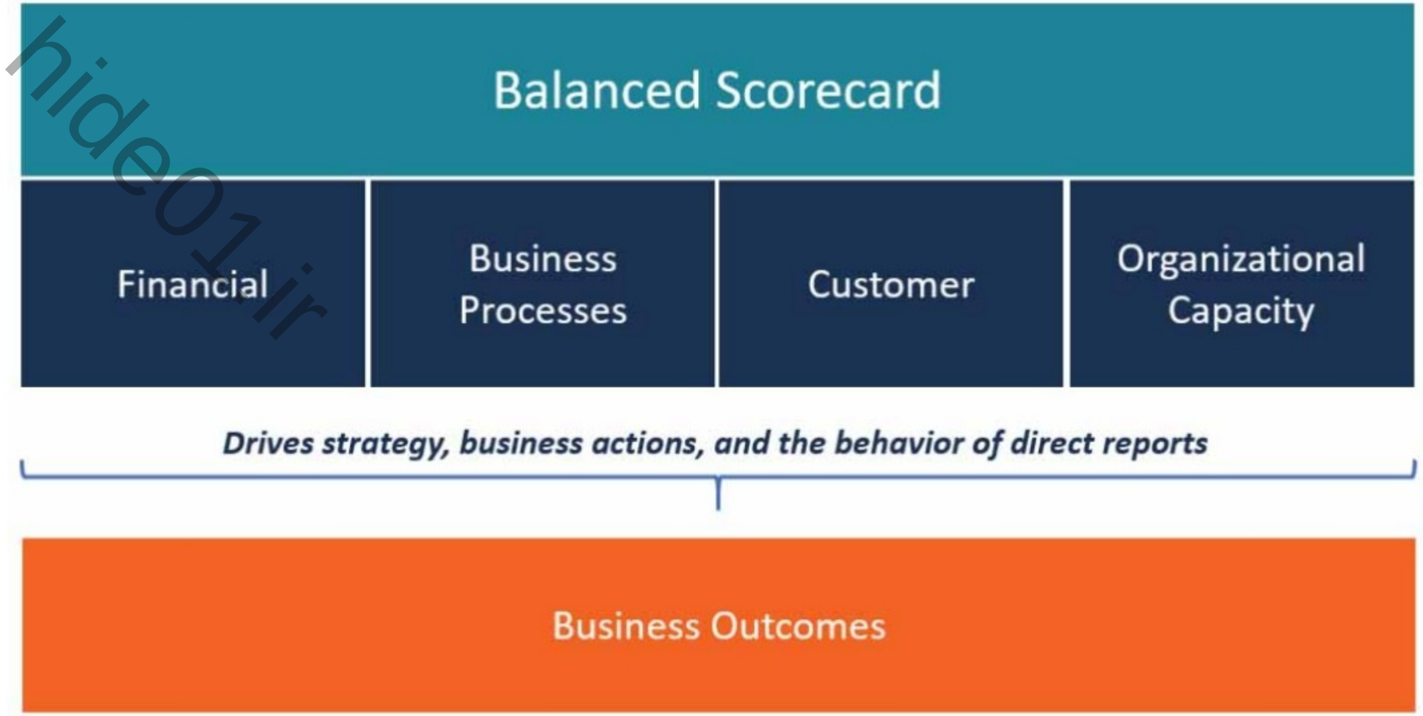
- Evaluation of goal attainment is a critical component of strategic planning.
- CISOs create metrics to measure the effectiveness of planning and performance during execution.
- Metrics can also be valuable for improving outcomes or performance.
- The most common evaluation tool for strategic planning is the Key Performance Indicator (KPI).
- KPIs are performance measures that indicate progress toward a desirable outcome.
- KPIs measure the effectiveness by highlighting gaps between actual and desired outcome.

2.4 BALANCED SCORECARD

A balanced scorecard semi-standard structured report that can be used by managers to keep track of the execution of activities by the staff.

A balanced scorecard:

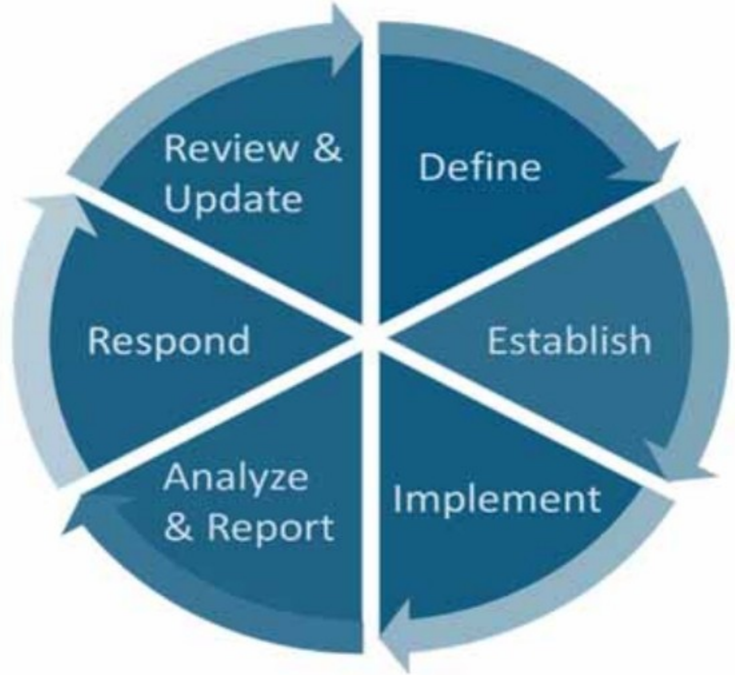
- Aligns business activities with the vision and strategy of the organization.
- Improves internal and external communications.
- Monitors the organization's performance against strategic goals.



2.5 CONTINUOUS MONITORING AND REPORTING OUTCOMES

NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) Federal Information Systems and Organizations.

The purpose of this guideline is to assist organizations in the development and implementation of continuous monitoring of the effectiveness of deployed security controls.

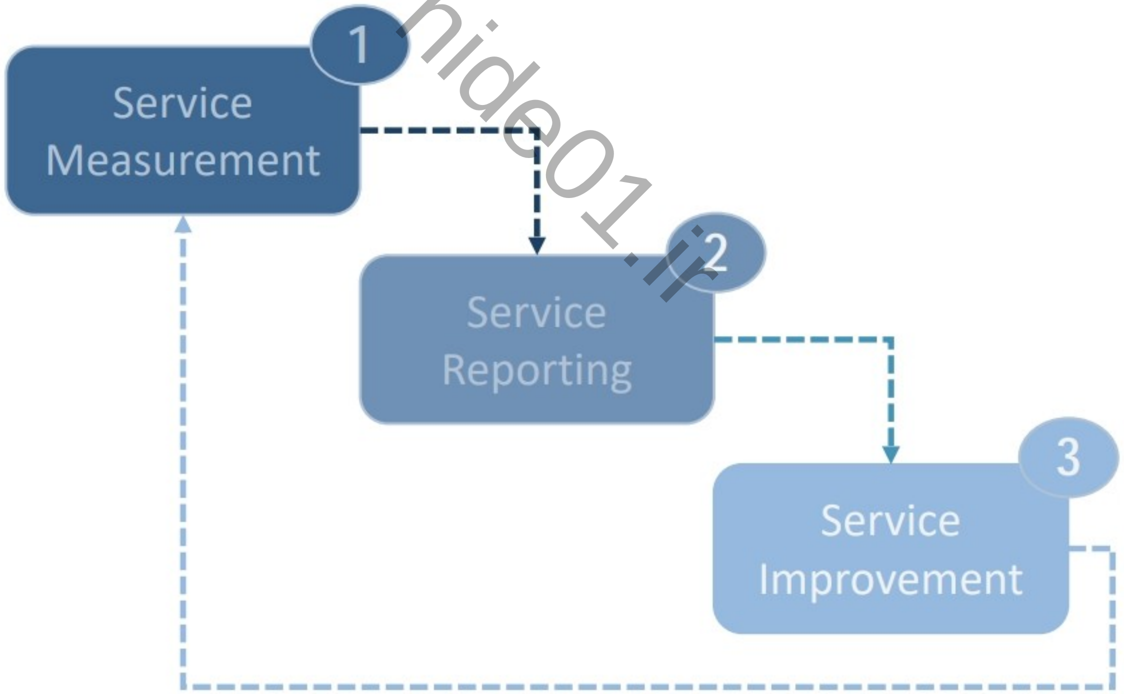


2.6 CONTINUOUS IMPROVEMENT

- Continuous Improvement Programs (CIP) provide a steady effort to assure the information security program is always available to protect information and assets.
- CISOs must continually seek incremental improvements in the information security program.
- CIP is a core part of an information security program improvement process and can be found throughout ITIL service management processes.

2.7 INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) CONTINUAL SERVICE IMPROVEMENT (CSI)

- Continual Service Improvement (CSI) processes are used to improve the effectiveness and efficiency of IT services and processes.
- The following main processes are part of the ITIL CSI:



3. UNDERSTANDING THE ENTERPRISE ARCHITECTURE (EA)

3. UNDERSTANDING THE ENTERPRISE ARCHITECTURE (EA)

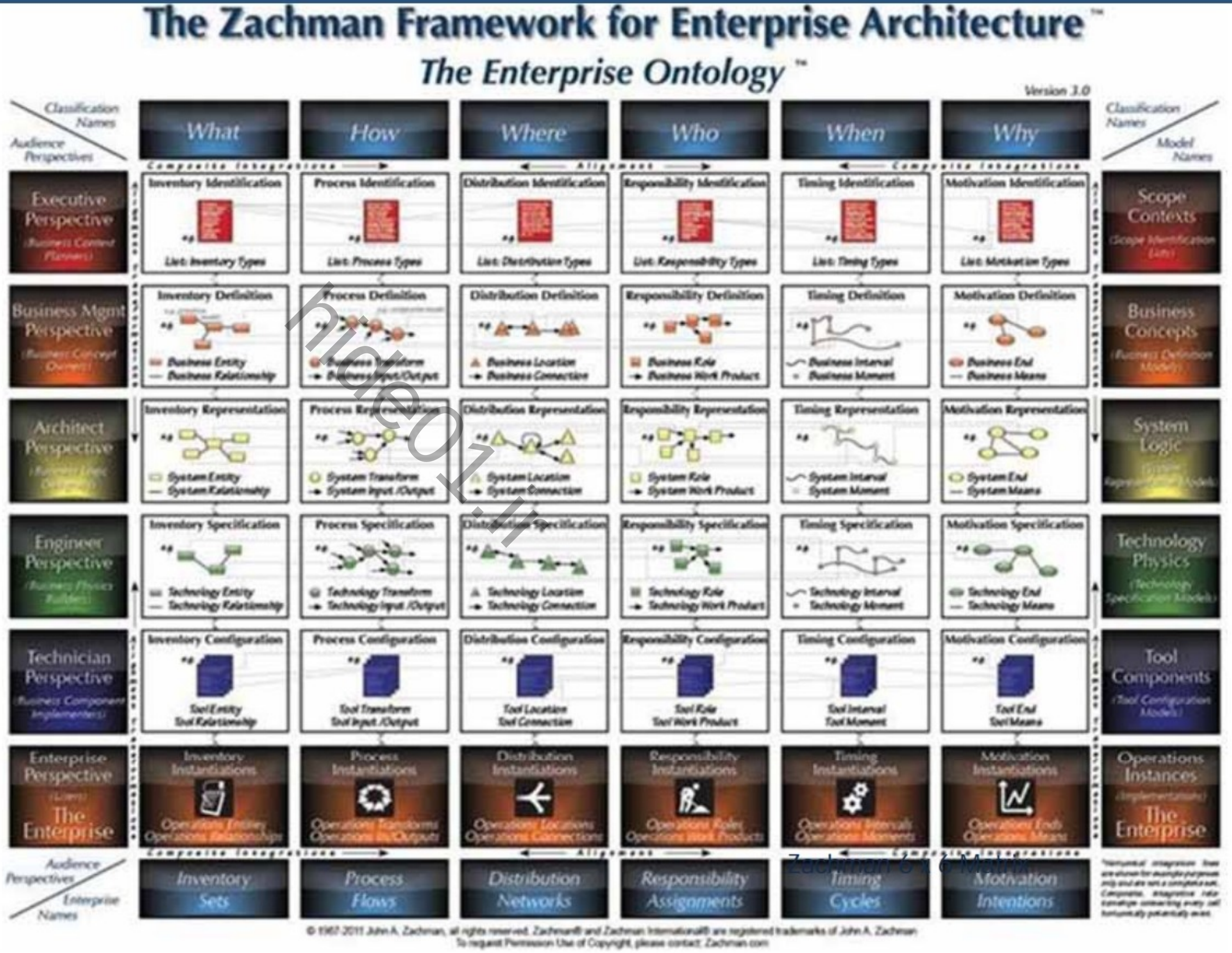
- An EA is both a result and a process.
- From a process perspective, it is a well-defined practice for performing analysis, design, planning, and implementation of technology.
- EA supports planning and decision making through documentation and information that provides an abstract view of an enterprise at various levels of scope and detail.
- EA provides a framework to define business requirements, business rules, and business cases that will lead the organization to successfully accomplish its mission, vision, and purpose.
- The purpose of EA is to optimize fragmented legacy processes into an integrated environment that is responsive to change and supports delivery of the business strategy.

3.1 EA TYPES

- An EA is both a result and a process.
- From a process perspective, it is a well-defined practice for performing analysis, design, planning, and implementation of technology.
- EA supports planning and decision making through documentation and information that provides an abstract view of an enterprise at various levels of scope and detail.
- EA provides a framework to define business requirements, business rules, and business cases that will lead the organization to successfully accomplish its mission, vision, and purpose.
- The purpose of EA is to optimize fragmented legacy processes into an integrated environment that is responsive to change and supports delivery of the business strategy.

3.1.1 THE ZACHMAN FRAMEWORK

- The Zachman Framework is an ontology providing a classification system that produces a working model of entities and interactions that create an agreed-upon vocabulary for exchanging information when specified.
- Many EAs use the Zachman Framework as a starting point.



The Zachman Framework for Enterprise Architecture™

The Enterprise Ontology™

Version 3.0

Composite Integrations → ← Alignment → ← Composite Integrations

Classification Names / Audience Perspectives	What	How	Where	Who	When	Why	Classification Names / Model Names
Executive Perspective (Business Context Planners)	Inventory Identification List: Inventory Types	Process Identification List: Process Types	Distribution Identification List: Distribution Types	Responsibility Identification List: Responsibility Types	Timing Identification List: Timing Types	Motivation Identification List: Motivation Types	Scope Contexts (Scope Identification Lists)
Business Mgmt Perspective (Business Concept Owners)	Inventory Definition Business Entity Business Relationship	Process Definition Business Transform Business Input/Output	Distribution Definition Business Location Business Connection	Responsibility Definition Business Role Business Work Product	Timing Definition Business Interval Business Moment	Motivation Definition Business End Business Means	Business Concepts (Business Definition Models)
Architect Perspective (Business Logic Designers)	Inventory Representation System Entity System Relationship	Process Representation System Transform System Input /Output	Distribution Representation System Location System Connection	Responsibility Representation System Role System Work Product	Timing Representation System Interval System Moment	Motivation Representation System End System Means	System Logic (System Representation Models)
Engineer Perspective (Business Physics Builders)	Inventory Specification Technology Entity Technology Relationship	Process Specification Technology Transform Technology Input /Output	Distribution Specification Technology Location Technology Connection	Responsibility Specification Technology Role Technology Work Product	Timing Specification Technology Interval Technology Moment	Motivation Specification Technology End Technology Means	Technology Physics (Technology Specification Models)
Technician Perspective (Business Component Implementers)	Inventory Configuration Tool Entity Tool Relationship	Process Configuration Tool Transform Tool Input /Output	Distribution Configuration Tool Location Tool Connection	Responsibility Configuration Tool Role Tool Work Product	Timing Configuration Tool Interval Tool Moment	Motivation Configuration Tool End Tool Means	Tool Components (Tool Configuration Models)
Enterprise Perspective (Users) The Enterprise	Inventory Instantiations Operations Entities Operations Relationships	Process Instantiations Operations Transforms Operations In/Outputs	Distribution Instantiations Operations Locations Operations Connections	Responsibility Instantiations Operations Roles Operations Work Products	Timing Instantiations Operations Intervals Operations Moments	Motivation Instantiations Operations Ends Operations Means	Operations Instances (Implementations) The Enterprise
Audience Perspectives / Enterprise Names	Inventory Sets	Process Flows	Distribution Networks	Responsibility Assignments	Timing Cycles	Motivation Intentions	*Horizontal integration lines are shown for example purposes only and are not a complete set. Composite, integrative relationships connecting every cell horizontally potentially exist.

Composite Integrations → ← Alignment → ← Composite Integrations

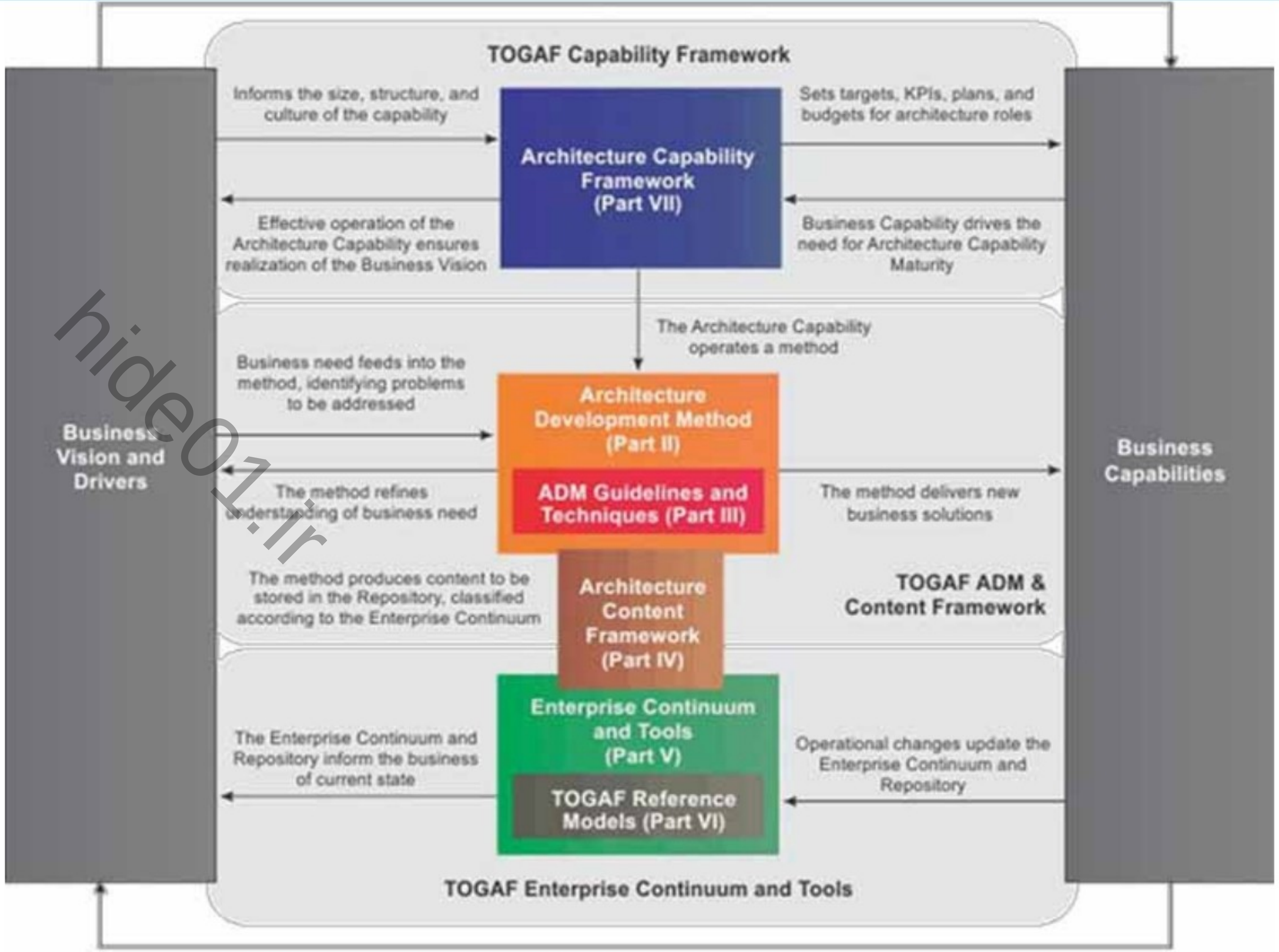
© 1987-2011 John A. Zachman, all rights reserved. Zachman® and Zachman International® are registered trademarks of John A. Zachman
To request Permission Use of Copyright, please contact: Zachman.com

Zachman 6 x 6 Matrix

3.1.2 THE OPEN GROUP ARCHITECTURAL FRAMEWORK (TOGAF)

The Open Group Architecture Framework (TOGAF)

- TOGAF is a business-centric EA framework that provides flexibility for formal definition of business activities.
- TOGAF provides a structured approach to organize and manage the implementation of technology in the enterprise.



TOGAF Capability Framework

Informs the size, structure, and culture of the capability

Architecture Capability Framework (Part VII)

Sets targets, KPIs, plans, and budgets for architecture roles

Effective operation of the Architecture Capability ensures realization of the Business Vision

Business Capability drives the need for Architecture Capability Maturity

Business Vision and Drivers

The Architecture Capability operates a method

Business need feeds into the method, identifying problems to be addressed

Architecture Development Method (Part II)

ADM Guidelines and Techniques (Part III)

The method refines understanding of business need

The method delivers new business solutions

Business Capabilities

The method produces content to be stored in the Repository, classified according to the Enterprise Continuum

Architecture Content Framework (Part IV)

TOGAF ADM & Content Framework

Enterprise Continuum and Tools (Part V)

TOGAF Reference Models (Part VI)

The Enterprise Continuum and Repository inform the business of current state

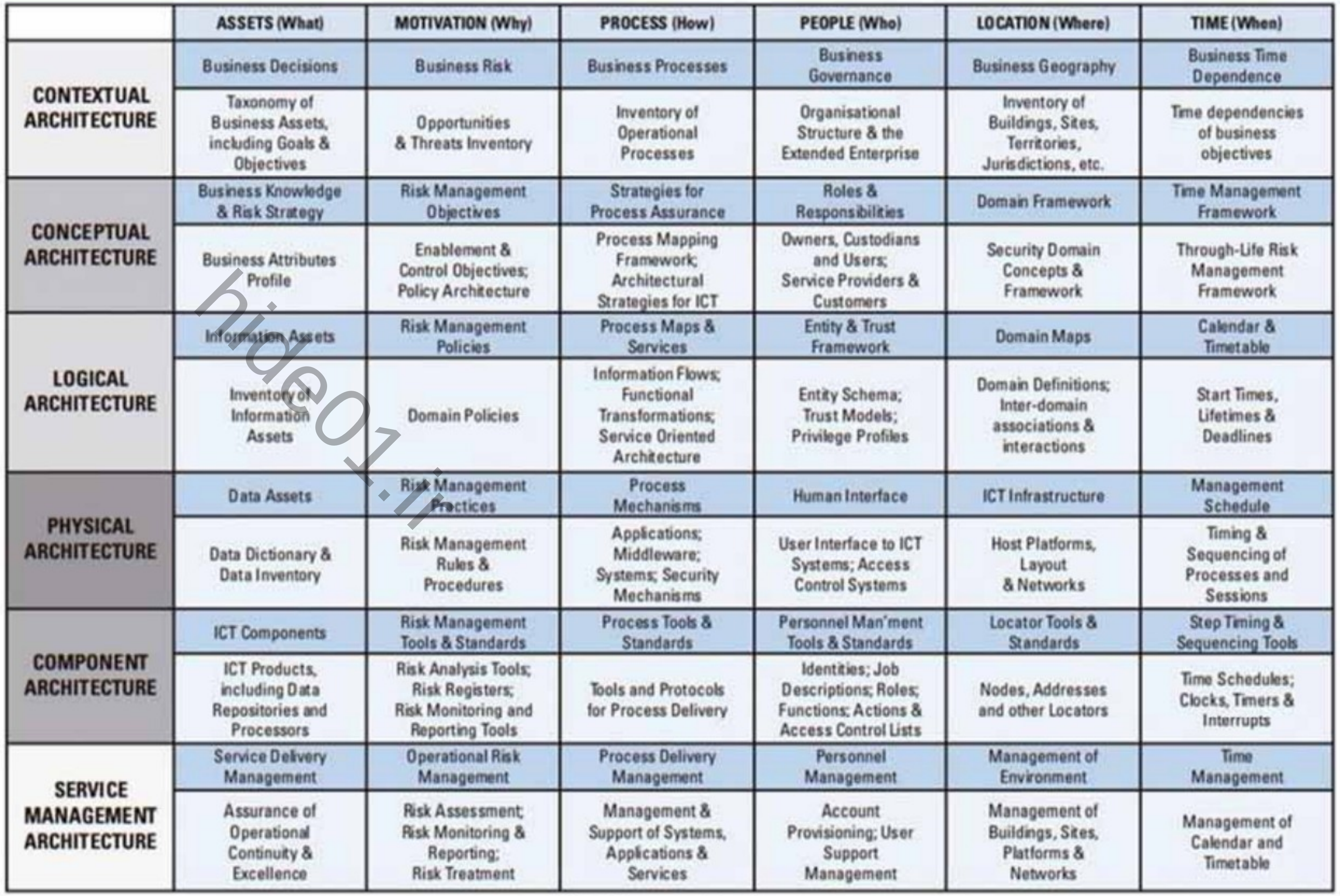
Operational changes update the Enterprise Continuum and Repository

TOGAF Enterprise Continuum and Tools

Structure of The Open Group Architecture Framework (TOGAF) Architecture

3.1.3 SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE (SABSA)

- The Sherwood Applied Business Security Architecture (SABSA) is a framework and methodology focused on enterprise needs.
- This includes risk management, information assurance, governance, and continuity management.

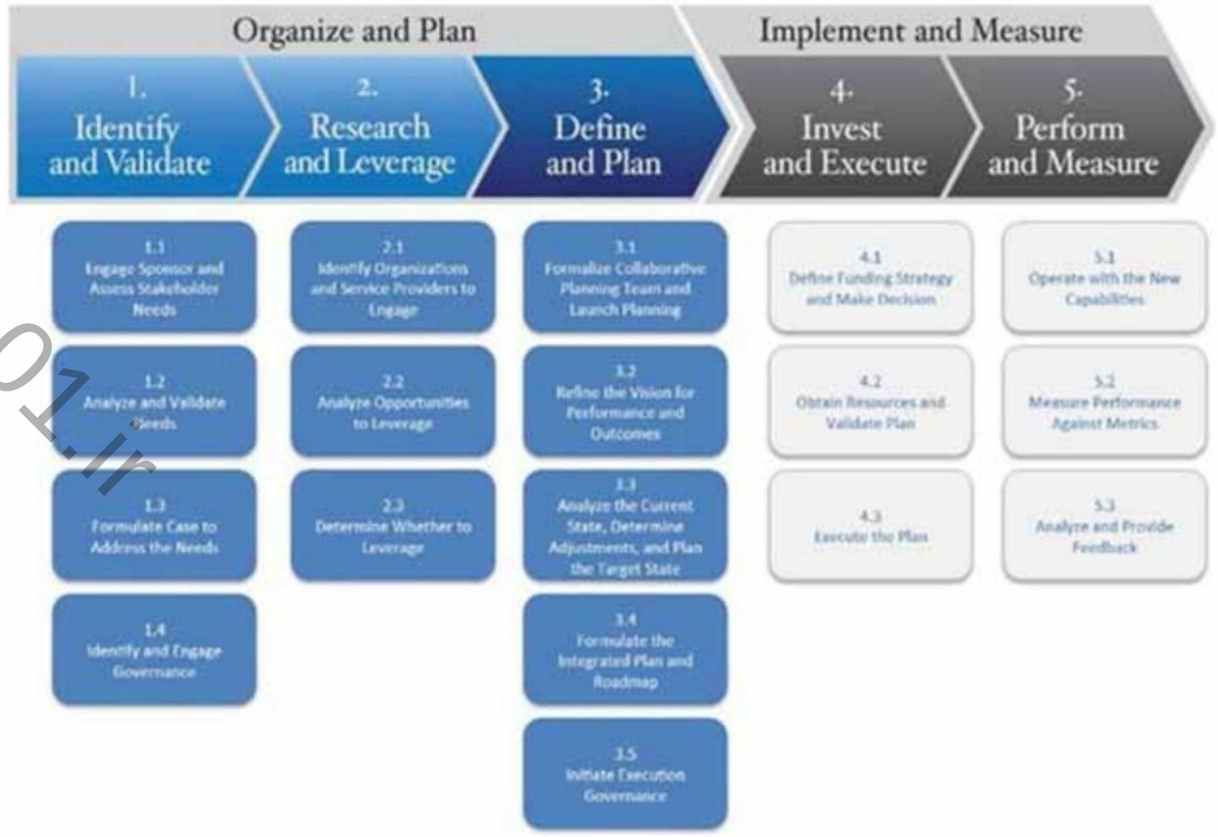


	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

SABSA 6 x 6 Matrix

3.1.4 FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK (FEAF)

- The Federal Enterprise Architecture Framework (FEAF) is a set of tools that help US federal agencies define the structure of EA within an organization.
- It helps the agencies describe the current enterprise, then identifies how the enterprise should look in the future.
- Organizations can then plan transition from the current state to the future state.


Organize and Plan
Implement and Measure
1. Identify and Validate
2. Research and Leverage
3. Define and Plan
4. Invest and Execute
5. Perform and Measure
1.1 Engage Sponsor and Assess Stakeholder Needs
1.2 Analyze and Validate Needs
1.3 Formulate Case to Address the Needs
1.4 Identify and Engage Governance
2.1 Identify Organizations and Service Providers to Engage
2.2 Analyze Opportunities to Leverage
2.3 Determine Whether to Leverage
3.1 Formalize Collaborative Planning Team and Launch Planning
3.2 Refine the Vision for Performance and Outcomes
3.3 Analyze the Current State, Determine Adjustments, and Plan the Target State
3.4 Formulate the Integrated Plan and Roadmap
3.5 Initiate Execution Governance
4.1 Define Funding Strategy and Make Decision
4.2 Obtain Resources and Validate Plan
4.3 Execute the Plan
5.1 Operate with the New Capabilities
5.2 Measure Performance Against Metrics
5.3 Analyze and Provide Feedback

Federal Enterprise Architecture Framework (FEAF)

4. FINANCE

- Because funding for the security program is typically allocated from organizational operating finances, the CISO has a fiduciary responsibility to be a good steward of the funds invested in the program.
- Achieving good stewardship requires an understanding of fundamental financial management concepts.
- This understanding will help to enable the financial success of the security program and its mission.

4.1 UNDERSTANDING SECURITY PROGRAM FUNDING

- Organizations spend an average of 5.6 percent of the overall IT budget on IT security and risk management (Gartner, Inc.).
  - There are many funding models, to include per-user cost averaging, historical budget alignment, or post-incident budget realignment.
- One of the top challenges for a CISO is identifying funding sources for an information security program.
- Most budget requests are accompanied by a Return on Investment (ROI) analysis.
- Understanding the budget language of your organization will allow you to speak in terms the organization understands.
- ROI analysis most often determines funding decisions.

4.2 ANALYZING, FORECASTING, AND DEVELOPING A SECURITY BUDGET

- The budgeting cycle is an essential financial management process used to estimate revenue and expenses over a specified period.
- Estimating expenses in relation to revenue (real or anticipated) determines whether enough money exists to fund operations or expand programs.
- Constant budget monitoring and management determines whether the budget has surplus, is balanced, or in deficit.
- Ultimately, the security program budget should do one (or more) of three things: increase revenue, reduce costs, or reduce risks.

4.2 ANALYZING, FORECASTING, AND DEVELOPING A SECURITY BUDGET - CONTINUED

The following suggestions will help CISOs secure proper funding.

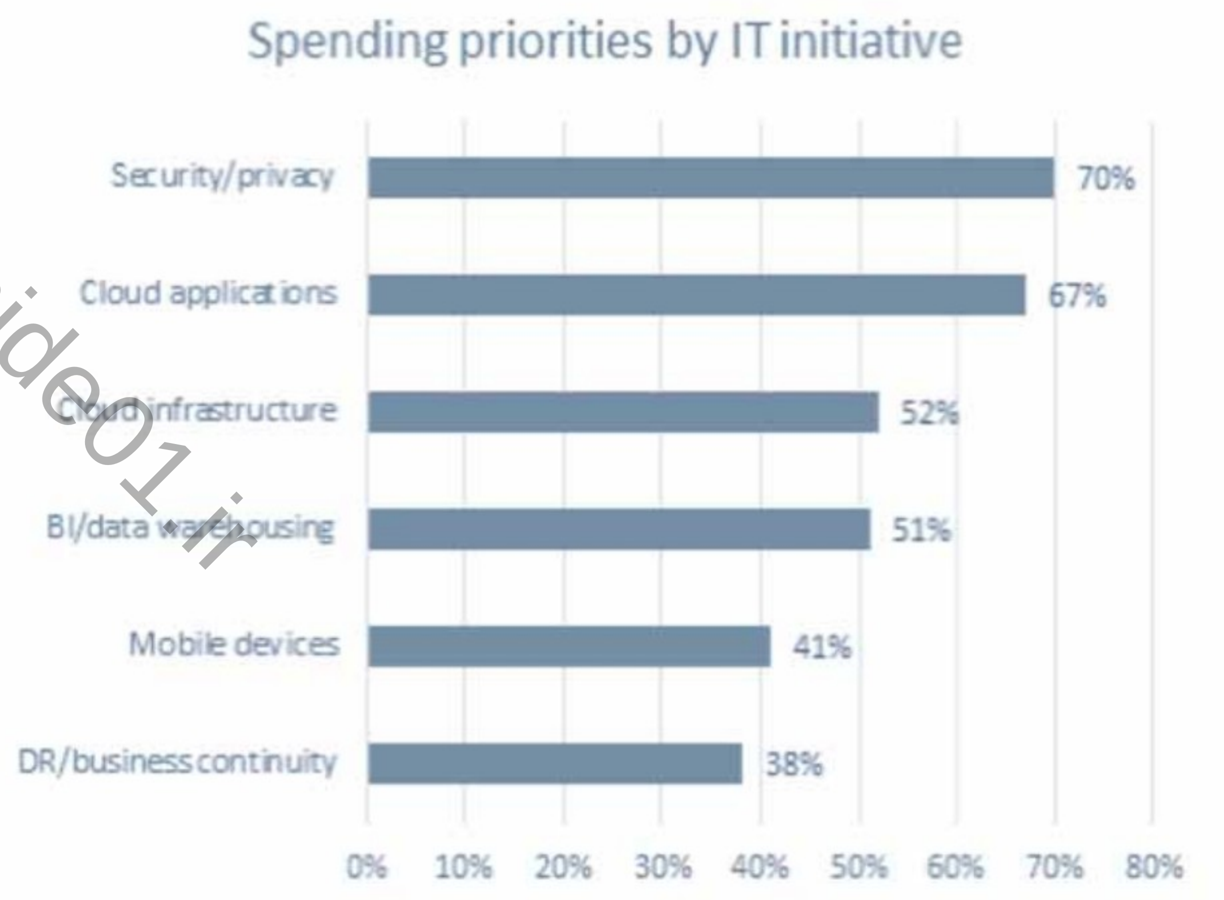
- Build a strong relationship with CFO to understand financial pressures within the organization.
- Understand organizational finance operations.
- Avoid the Fear, Uncertainty, and Doubt (FUD) approach – state needs in terms of risk and reward.
- Demonstrate financial stewardship and competence by being as accurate as possible with projections and spending.
- Articulate business value for investment (ROI) throughout the budgeting process.

4.2.1 RESOURCE REQUIREMENTS

- Financial estimation is a structured prediction of costs required to execute a task.
- The more accurate the estimation, the more reliable the information sources.
- By creating accurate financial estimates, a CISO can build organizational trust for the security program.

4.2.1 RESOURCE REQUIREMENTS - CONTINUED

- A properly documented resource plan will specify the quantities of human resources, equipment, and materials needed to obtain goals.
- The increasing frequency and scale of security breaches and cyberattacks has placed security/privacy at the top ofthe Computer Economics' spending priority ranking.



IT Spending and Staffing Benchmarks study for 2017/2018.

4.2.1 RESOURCE REQUIREMENTS - CONTINUED

The following provides a general guide for internal security program budget allocation.

Category	Total	North America	Europe
Recovering from cybersecurity events	17.0%	16.4%	18.4%
Responding to cybersecurity events	18.5%	17.7%	20.0%
Detecting cybersecurity events	20.2%	20.4%	19.8%
Protecting systems, assets, data, or capabilities from cybersecurity threats	24.30	24.6%	23.7%
Identifying cybersecurity risk	20.30	20.9%	18.1%

The Cyber Risk Alliance (CRA) 2020 Cybersecurity Resource Allocation and Efficacy (CRAE) Index.

4.2.2 DEFINE FINANCIAL METRICS

- Financial metrics provide insight into budget trends such as spending, surplus, deficits, and alignment to the budget plan cycle.
- Financial metrics are like descriptive statistics giving insight into the details of how well the budget is performing.
- The statistical average (arithmetic mean), for instance, reveals the typical value in a data set.
- Similarly, financial metrics reveal characteristics of the economic data set.

4.2.2 DEFINE FINANCIAL METRICS – CONTINUED

- Cash flow investment metrics, for instance, measure performance by evaluating cash inflows and outflows following a business outlay or investment.
- One of these metrics, the payback period, measures the time required for investment returns to cover the cost of the investment.
- Organizations usually compare payback periods of investments to help select the best investment options.

4.2.3 TECHNOLOGY REFRESH FUNDING

A technology refresh cycle establishes a predictable process for periodically replacing old technology with new assets.

- There are many benefits of creating a technology refresh calendar.
- CISOs should review security technology refresh using three methods:
  - **Technology Obsolesce**: CISOs should ensure they are not using security technology that has passed its useful life or introduces unwanted risk.
  - **Technology Innovation**: CISOs should monitor the cybersecurity technology landscape for innovative and effective ways of reducing risk, costs, and managing risks more efficiently.
  - **Decrease Failure Rate**: Using technology that has not exceeded the acceptable meantime-to-failure ratio increases uptime of critical security support.

4.2.4 NEW PROJECT FUNDING

- One of the key elements of a project proposal is the project budget.
- The project budget is a core metric that will be used throughout the project lifecycle.
  - The project manager will use this budget to determine whether the project is being delivered within constraints.
  - Project budget is typically analyzed and separated into project milestones.
  - The customer or sponsor will use it to determine the success of the effort.
- CISOs need accurate and reliable financial information to support project decisions that will impact the overall success of the security program.

4.2.5 CONTINGENCY FUNDING

CISOs often must create financial buffer in their budgets by identifying potential contingencies or exigent circumstances. These can be very diverse and numerous depending on the complexity of the organization.

Examples:

- **Cryptocurrency Wallet:** In the event your organization decides to pay a ransom request resulting from a ransomware attack, a cryptocurrency wallet may be needed.
- **Disaster Declarations:** If your organization uses a contracted disaster recovery facility, a disaster declaration fee might be required to activate the site.
- **License Creep:** It is common for security technology license costs to increase. For example, the number of monitored events per second could rapidly increase, causing the projected license costs of a SIEM product to exceed expectations.

4.3 MANAGING THE INFORMATION SECURITY BUDGET

Financial management is the processes of planning, organizing, directing, and controlling the monetary activities of an organization and the use of funds.

- Managing an information security budget requires that CISOs adhere to their organization's financial management standards and processes.
- A well-managed information security program budget allows for uninterrupted security services and establishes the CISO as a competent steward of organizational funds.

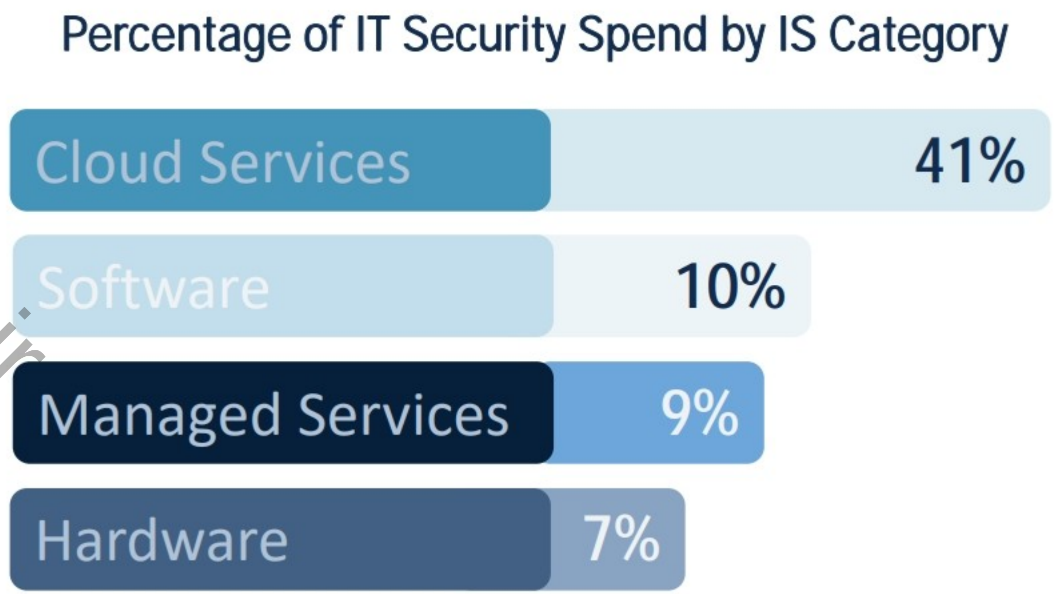
4.3.1 OBTAIN FINANCIAL RESOURCES

There are several methods that can be used to obtain security program funding.

- Capitalization – placing an expenditure on the balance sheet (direct funding).
- Chargeback – charging internal business units for security services provided.
- Market subsidy – typically funding or programs that are provided by a government or other outside entity.
- Value-added service pricing – this is an ROI approach for charging the business for security services.
- Vendor financing – some vendors will allow payments for services or products, distributing the spend over a longer period.

4.3.2 ALLOCATE FINANCIAL RESOURCES

- Accurate and timely allocation of financial resources can be very demanding for a CISO.
- Allocating too little or too much in certain security functions can put the program out of balance in relation to the risk profile.
- The CISO should pursue a risk-based approach to allocating their budget to assure the most critical areas of the organization receive priority funding.



4.3.4 DEVELOPING AN INFORMATION SECURITY PROGRAM BUDGET

CapEX

- Capital expenditure used to acquire, or upgrade fixed non-consumable assets:
  - Buildings.
  - Equipment.

OpEX

- Operational expenditure used to pay for ongoing costs related to a security program:
  - Salaries.
  - Maintenance.
  - Cloud services.
  - Training.

4.3.4 DEVELOPING AN INFORMATION SECURITY BUDGET – CONTINUED

- Budgeting is used to estimate revenue and expenses over a specified period.
- Estimating and matching expenses to revenue (real or anticipated) helps determine whether enough funding exists to pay for operations or expand programs.
- Security is typically not a revenue generator.
- CISOs can obtain IS program funding through a chargeback system that charges business units for the delivery of cybersecurity services.
- The security budget metrics measure the exchange of financial allocations for the security products and services supporting the organization.

4.3.5 MANAGING AN INFORMATION SECURITY PROGRAM BUDGET

- To be successful, the CISO should include these goals for efficient financial management:
  - Understand the details of how finances work in your organization.
    - How is the organization funded – what business units generate or obtain funding?
    - What areas of the business represent heavy investment?
    - What is the financial status of the company in relation to projections?
  - Assure that the cost of security controls do not exceed the value of the protected assets.
  - Understand and use standard financial management terms and tools.

4.3.5 MANAGING AN INFORMATION SECURITY PROGRAM BUDGET - CONTINUED

- There are two common methods of accounting for expenses and costs in a security program:

Top-Down ⬇

- Review the total budget.
- Determine the activities to be supported.
- Allocate the percentage for each activity from the budget.
- Inaccurate total budget can create insufficient activity funding.

Bottom-Up ⬆

- Determines cost of each program activity.
- Establish a budget for each activity.
- Sum of all activities equals total budget.
- Overstating activity funding can result in inaccurate budgeting.

4.3.6 MONITORING AN INFORMATION SECURITY BUDGET

- CISOs should clearly understand critical financial patterns within the organization and the supporting business units.

Cash Flow

- Measures the amount of money flowing into and out of the organization.
- Provides checks and balances of budget validity.
- Ideal for fixed budget analysis.

Burn Rate

- Measurement of the rate at which cash flows out of the program budget.
- Facilitates budget tracking.
- Compares actual verses planned spending.

4.3.7 REPORT METRICS TO SPONSORS AND STAKEHOLDERS

- One way to show transparency is to report financial metrics of the information security program in open forums such as security steering committee meetings.
- Deciding which financial metrics to use is part art and part science, as ROI is difficult to demonstrate for something intangible such as security.
- Regardless of the challenges (and at time angst), it is important for a CISO to openly report financial metrics.
- One of the best ways to communicate program budget is to create a spending baseline and show progress in relation to it.
- The cost of providing internal information security services versus outsourcing them should be communicated in terms of benefits and challenges with each approach.

4.3.8 BALANCING THE INFORMATION SECURITY BUDGET

Some final budget thoughts…

- As the CISO for your organization, you must deliver services within a balanced budget.
- You must also demonstrate that your information security program's expenses do not exceed the value of the investment.
- A successfully balanced budget tells senior management that you're properly managing the organization's investment.
- Managing a budget requires careful attention to monthly spending.
- CISOs should be prepared to make difficult decisions to reduce spending if the budget becomes unbalanced.

5. PROCUREMENT

5. PROCUREMENT

- Procurement consists of the requirements and processes related to how organizations source and acquire goods and services.
- CISOs need to clearly understand how their organization makes purchases.
- Procurement is always closely audited and monitored – be very careful not to intentionally or unintentionally break the rules.
- How purchasing works in an organization is another core management knowledge area - as important as financial and project or program management.

5.1 PROCUREMENT PROGRAM TERMS AND CONCEPTS

The fundamentals of purchasing are a critical part of an organization.

There are a wide range of standard procurement terms such as:

Statement of Objectives (SOO)

This is one part of a Request for Proposal (RFP), and often used in procurement situations. The SOO is an alternative to a Statement of Work. These are commonly used by governments.

Statement of Work (SOW)

This is a document that defines the scope of a purchase, specific deliverables, scheduling, and additional responsibilities by both parties.

Total Cost of Ownership (TCO)

This is a financial estimate intended to help buyers and owners determine the direct and indirect costs of a product or system.

PROCUREMENT PROGRAM TERMS AND CONCEPTS - CONTINUED

Additional common procurement terms include the following.

Request for Information (RFI)

Related to the Request For Proposal process (below), this document provides the opportunity to collect a wide range of information about a supplier or multiple suppliers and their capabilities. It is often the first step in finding a vendor solution.

Request for Proposal (RFP)

This document is basically a request for suppliers to bid on an equipment or services request from procurement.

Master Service Agreement (MSA)

An MSA is a contracting artifact that details the general responsibilities and obligations of two parties to each other. They are usually long term, spanning beyond individual contracts.

PROCUREMENT PROGRAM TERMS AND CONCEPTS - CONTINUED

Additional common procurement terms include the following.

Service Level Agreement (SLA)

An SLA is a contract that defines the quality and volume of specific deliverables and delivery schedules for one or both parties.

Terms and Conditions (T&Cs)

T&Cs are typically a set of legal requirements that must be agreed upon in order to initiate a contract.

5.2 UNDERSTANDING THE ORGANIZATION'S PROCUREMENT PROGRAM

- Purchasing processes usually have several steps, such as requisition, soliciting bids, purchase order, shipping advice, invoice, and payment.
- Sometimes these requirements can be perceived as unacceptably slow, expensive, and labor intensive.
- In some organizations, the same process is followed whether the item being purchased was a box of paper clips or a new bulldozer.
- Do not get frustrated with your procurement processes.
  - Learn to work within them and appreciate the financial controls and fiduciary protections they provide for your organization.

5.2.1 INTERNAL POLICIES, PROCESSES, AND REQUIREMENTS

Organizations will have policies, procedures, and processes to guide the procurement of information security products and services.

Some of the terms CISOs may encounter include:

- Procurement limits – how much can be spent on an acquisition.
- Purchase authority – purchase limits according to job title.
- Formal bidding – structured input of proposals and pricing.
- Informal bidding – unstructured process for submitting proposals and pricing.
- No bid – an unsuccessful attempt to fulfill a customer need.
- Sole source – removing competitive bids in the procurement process.
- Sealed bid – pricing for a solution is unknown among competing vendors.
- Public bid – bids can be submitted by any entity.

5.2.2 EXTERNAL OR REGULATORY REQUIREMENTS

- To prevent fraud or collusion in the procurement process, many organizations use stringent separation of duties matrices.
- CISOs should understand that not following proper procurement policies can lead to their dismissal or even arrest.
- CISOs need to understand the following external and regulatory aspects of procurement:
    - Commercial bribes (can be business-as-usual in some regions).
    - Ethical procurement.
    - Disadvantaged organization procurement.
    - Uniform Commercial Code (UCC) – US laws for commercial transactions.

5.2.3 LOCAL VERSUS GLOBAL REQUIREMENTS

- It has become common practice to offshore some security services to low-cost locations around the globe.
- Global resourcing of information security has not been popular due to the risks of providing sensitive data beyond an organization's borders.
- In some parts of the world the practice is more common.
- If contemplating using global security capabilities, considerations should include:
  - Value Added Taxes (VAT).
  - Cross-currency strength or weakness.
  - Communicating with foreign teams.
  - Traveling to suppliers.
  - Geo-political stability risks.

5.3 PROCUREMENT RISK MANAGEMENT

- In order to function properly, procurement demands high integrity.
- Irregularities in the purchasing process, or even the appearance of impropriety, can invalidate the entire process.
- As the CISO you must assure that your department is not the cause of fraud or ethical vendor issues.
- CISOs must clearly understand the legal ramifications of procurement requirement infractions and communicate them to the security team.
- CISOs need to closely adhere to organization procurement policies so their reputations remain intact.

5.3.1 STANDARD CONTRACT LANGUAGE

- CISOs should assist with reviewing an organization's contracts when the contract presents security risk to the organization.
- This is especially important considering the increasing incidents involving cyberattacks caused by 3rd party relationships and IT connectivity.
- A CISO should assure that general contract language exists to protect the organization from data or security breaches.
- This will help minimize incidents and provide legal recourse in the event of contract or security breach.

6. VENDOR RISK MANAGEMENT

6. VENDOR RISK MANAGEMENT

- Vendors can augment staff or provide technical or business skills not readily available within your organization.
- Vendors can be beneficial, but organizations must evaluate and understand the risks present when using vendors.
- The primary reason for performing vendor management is to understand the risk that a vendor will either introduce to, or mitigate for, the organization.
- To achieve effective vendor management, the CISO should work with the procurement function to assure vendor security requirements are integrated into MSAs and other contractual agreements.
- Vendors should be closely monitored for performance and proper security support throughout contract delivery.

6.1 UNDERSTANDING THE ORGANIZATION'S ACQUISITION POLICIES AND PROCEDURES

- Understanding the potential variety of risk introduced by vendors is an essential part of information security management.
- Vendor compromises lead to breaches of your organization's security posture – be cautious with the risk and reward aspect of when working with vendors.
- Integrate vendor risk management with enterprise risk management policies and procedures to help mitigate the potential for vendor security issues.

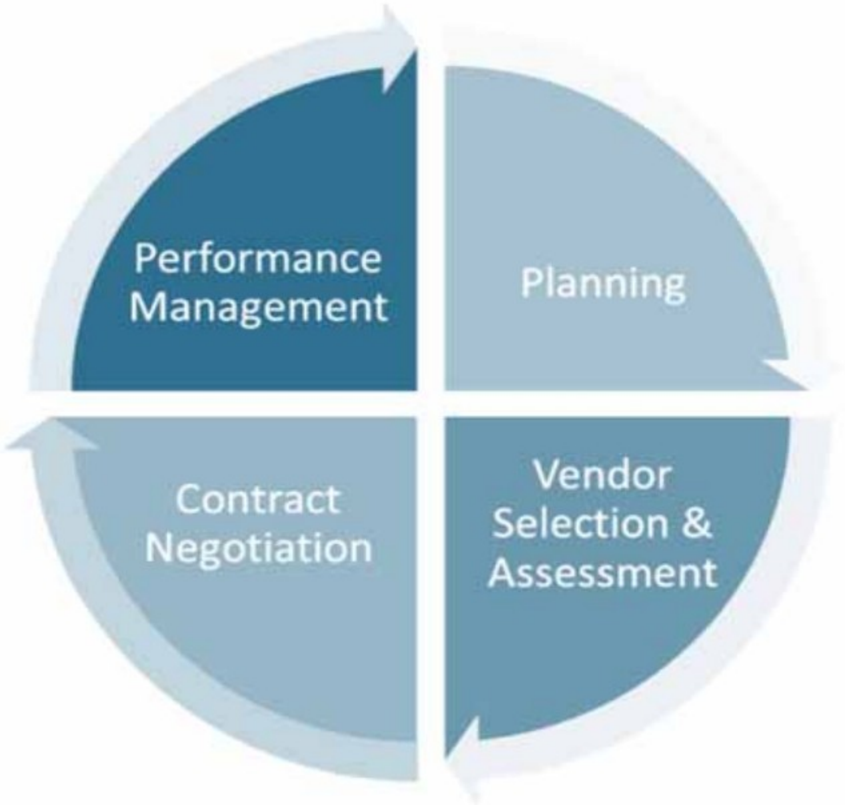
6.1.1 PROCUREMENT LIFECYCLE

- The procurement lifecycle consists of all processes the organization uses for vendor relationships.
- Common phases include planning, vendor assessment and selection, contract negotiation, and performance management.
- Security management within vendor relationships begins with the initial procurement process – make sure it is integrated very early in the procurement cycle.

6.1.1 PROCUREMENT LIFE CYCLE

- **Planning** sets prerequisites for vendor risk management. Define the scope of services, requirements to be met for vendors to be considered, and establish contractual language needs.
- **Vendor Assessment and Selection:** The RFP is generally regarded as a best practice to assist in the procurement of services. RFPs are beneficial because they can facilitate a competitive bidding process across several vendors.
- **Contract Negotiation** is an important component of vendor management. Everyone affected by the contract should be involved in evaluating the terms, expectations, and requirements outlined by the vendor.
- **Performance Management** is the ability to hold the vendor contractually accountable for the delivery of services and products as detailed in the contract.

Vendor Procurement Lifecycle



6.2 APPLYING COST-BENEFIT ANALYSIS (CBA) DURING THE PROCUREMENT PROCESS

- A Cost-benefit analysis (CBA) is a relatively simple calculation among financial comparison tools but can be somewhat imprecise.
- CBAs are often used to produce quick comparisons of multiple options.
- The outcome of a CBA will help determine whether a project is feasible and desirable, or if another project should be pursued.
- CBA analyzes decisions by identifying the benefits of a decision in terms of total value, and then subtracting the costs associated with taking that action.
- Total benefit - total cost = cost benefit.

6.3 VENDOR MANAGEMENT POLICIES

Third-party management policies and processes should include the following.

- Monitoring of delivery and the relationship - how the relationship will be monitored and at what frequency.
- Change management provides the procedure for requesting, approving, and documenting contract changes.
- Change in ownership or delivery personnel - requires the third party to notify the organization when vendor key personnel change or if the provider has been acquired.

6.3 VENDOR MANAGEMENT POLICIES - CONTINUED

- Material change in vendor bid requires notification in the event of a major change in the third party's financial condition, product certifications, or anything else that negatively affects bids, proposals, contracts, or delivery.
- Security auditing is used for performing risk assessments of the services or goods provider, with contract language including disposition of the results of the audit.

6.3 VENDOR MANAGEMENT POLICIES - CONTINUED

- Delivery auditing details how delivery will be assessed, how exceptions will be handled, and when these audits will be performed.
- Incident management provides third party requirements in the event of a security incident associated with contract delivery.
- Outage reporting requires notification of disruption of the provider's capability to deliver contractual requirements.
- Contract closure provides detailed contract termination requirements.

6.4 CONTRACT ADMINISTRATION POLICIES

Service and Contract Delivery Metrics - establishes measurements according to the product or services delivered. Commitments represented by the vendor in the contract can be used to create delivery metrics.

Contract Delivery Reporting provides consistent reporting on contract performance. Delivery performance reporting is particularly necessary in large or complex projects.

Contract Renewal events provide opportunities to make improvements in price, service, delivery or other sections of the original contract.

Contract Closure provides requirements for the contract close out period. Information previously provided, stored or processed by the vendor is destroyed, and assets are returned to the organization.

6.5 DELIVERY ASSURANCE

- Delivery assurance is an integral component of third-party vendor risk management.
- It provides a formal process for verifying delivery of services or products.
- Security policies and processes can be integrated with delivery assurance requirements.
- Delivery assurance typically integrates formal compliance checks against contractually committed goods and services.
- Delivery assurance provides the basis for a contractual gap assessment.

6.5.1 VALIDATION OF MEETING CONTRACTUAL REQUIREMENTS

Several methods can be used to verify delivery of contractual requirements.

- Delivery checklist – very good for larger, complex deliveries.
- Vendor commitment validation – the vendor verifies delivery to you.
- Work breakdown structure (WBS) analysis – typically used for services tc demonstrate the individual parts of the service were provided.
- Demonstration of delivery – can be used to assure the proper functioning of technologies, typically hardware and software.

6.5.2 FORMAL DELIVERY AUDITS

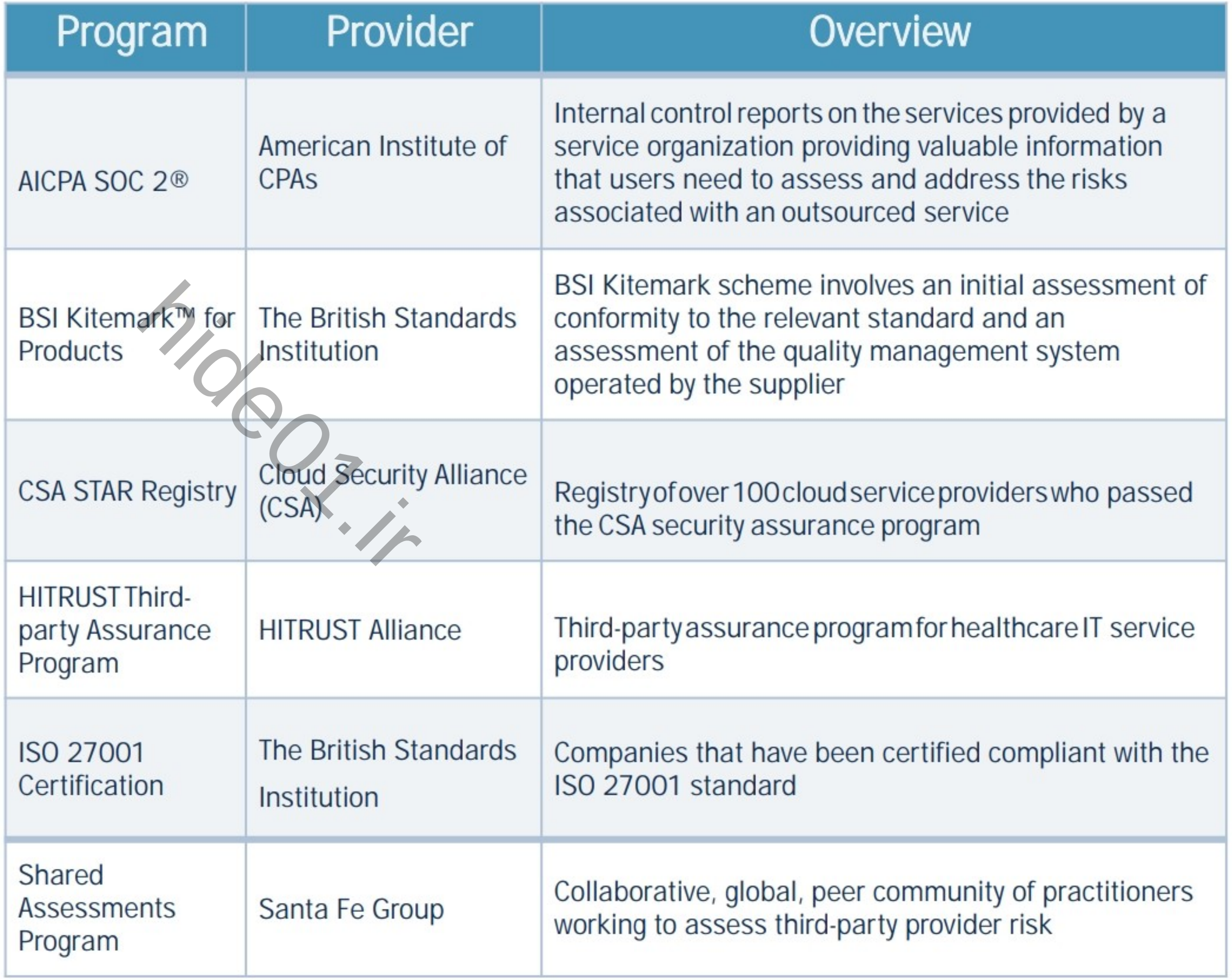
- A simple but effective delivery assurance tool is a delivery validation checklist. CISOs should create a checklist comprised of vendor commitments as provided in contracts, SOWs, and Work Breakdown Structures (WBSs).
- A formal delivery audit of a vendor or service provider is a common approach to delivery assurance.
- These requirements can be integrated early in the lifecycle as part of the vendor selection process
- Audits can be used for short term projects, long-term contracts, or contract closure processes.

6.5.3 PERIODIC DELIVERY AUDITS

- Delivery audits can be scheduled or randomly performed.
  - Contractual language is required in order to facilitate audits. They cannot simply be initiated without mutual consent.
- Periodic delivery audits can be difficult to negotiate and execute.
  - They are typically used to perform milestone analysis of contract delivery.
- Third-party attestation services can also be used.
  - o Due to the potential for high resource burden, you might consider using specialized organizations that independently assess and report on a third-party's delivery performance.

6.5.4 THIRD PARTY ATTESTATION SERVICES

There are several information resources available for assessing third party contractual delivery quality.



Program	Provider	Overview
AICPA SOC 2®	American Institute of CPAs	Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service
BSI Kitemark™ for Products	The British Standards Institution	BSI Kitemark scheme involves an initial assessment of conformity to the relevant standard and an assessment of the quality management system operated by the supplier
CSA STAR Registry	Cloud Security Alliance (CSA)	Registry of over 100 cloud service providers who passed the CSA security assurance program
HITRUST Third-party Assurance Program	HITRUST Alliance	Third-party assurance program for healthcare IT service providers
ISO 27001 Certification	The British Standards Institution	Companies that have been certified compliant with the ISO 27001 standard
Shared Assessments Program	Santa Fe Group	Collaborative, global, peer community of practitioners working to assess third-party provider risk

DOMAIN 5
END

DOMAIN 5 SUMMARY

DOMAIN 5: GENERAL

- This domain discussed the financial skills required of a CISO and how to effectively manage third party risk.
- CISOs need to recognize that although they do not personally pay information security program costs, they must act as if they do.
- CISOs will compete with other departments and programs for annual funding.
- Managing the risk introduced by third parties is a critical part of the overall security program.

DOMAIN 5: STRATEGIC PLANNING

- A strategic plan provides the direction and goals of an information security program.
- The plan outlines the actions required to achieve stated goals and the timeline for accomplishing them.
- Information security strategic plans must support IT and business strategic plans.
- Strategic plans generally provide a multi-year perspective.
- CISOs must identify the security program sponsors, stakeholders and influencers.
- A core outcome of a strategic plan is to improve the culture of security in an organization.

DOMAIN 5: DESIGNING, DEVELOPMENT, AND MAINTAINING AN ENTERPRISE IS PROGRAM

- CISOs should have a clear vision of the entire information security program and be able to clearly articulate the value of it.
- The most popular information security frameworks are ISO 27001 and the NIST CSF.
- CISOs should have a blueprint to serve as their master plan of how they will achieve the goals of the security strategy.
- CISOs will need to act as the security program architect by building out the services it provides to the organization.
- Metrics should be carefully defined and selected when designing a security program.
- Service management practices should be leveraged to build resiliency into the security program.

DOMAIN 5: UNDERSTANDING THE ENTERPRISE ARCHITECTURE (EA)

- The Enterprise Architecture (EA) provides the framework of how a business is managed.
- Certain aspects of the information security program architecture design can be borrowed from the organization's EA.
- The primary EA types you will likely experience include:
  - Zachman Framework
  - TOGAF
  - SABSA

DOMAIN 5: FINANCE

- Most funding for IS programs come from IT budgets.
- CISOs need to be good stewards of the financial aspects of the security program.
- The CISO should be the one person who can answer the question, "How much does security cost our organization?"
- CISOs need to understand how finances work within their organization.
- Organizations spend on average 5.6% of their IT budget on information security programs.
- CISOs need to understand CapEx and OpEx, and TCO and ROI.
- CISOs must create and manage an accurate budget to effectively manage an IS program.

DOMAIN 5: PROCUREMENT

- Security programs can consume many products and services.
- CISOs are involved in most, if not all, security purchasing decisions.
- To be an effective CISO, you must understand how your organization procures products and services.
- CISOs need to be able to select the best overall products and services as part of their financial stewardship.
- Understanding how to write an RFP and SOW is a critical skill.
- Most procurement decisions will be based on a CBA.

DOMAIN 5: VENDOR RISK MANAGEMENT

- It is not unusual to have hundreds if not thousands of vendors in use within an organization.
- Vendors can introduce unwanted risk for organizations.
- A growing percentage of data breaches originate through third party access to customer infrastructure.
- CISOs should avoid maintaining separate controls sets for internal and third-party connection to infrastructure systems.
- Vendor security expectations and requirements need to be clearly defined within contractual language.
- Delivery assurance checks and audits should be periodically made to verify compliance with contractual expectations.

DOMAIN 5 PRACTICE QUESTIONS

PRACTICE QUESTIONS

1. A CISO is considering a major security technology purchase and needs to understand product capabilities, corporate history, customer feedback, and cost and implementation effort.

What is the BEST way to collect this type of initial information?

A. Use a Request for Information (RFI) approach for gathering information.

B. Create a business case in order to communicate expected budget support requirements.

C. Create a Return on Investment (ROI) document for executive peer budget analysis and reviews.

D. Establish a competitive product review of a few selected technologies in a lab environment.

PRACTICE QUESTIONS

2. As CISO for a large corporation, you've outsourced your network security operations center to a service provider.

Which of the following are the two MOST important Key Performance Indicators (KPIs) you would include in your Service-Level Agreement (SLA)?

A. Incident response times and number of malicious events.

B. Incident reporting times and number of unmitigated network attacks.

C. Incident response times and number of unmitigated network attacks.

D. Incident reporting times and number of malicious events.

PRACTICE QUESTIONS

3. What is the MOST important thing to consider when writing the Statement of Work (SOW)?

A. The Service-Level Agreements (SLA).

B. Appropriate allocation of dedicated resources.

C. Reduction of the number of malicious attacks during the contract period.

D. Ensure payment terms are at least NET 30.

PRACTICE QUESTIONS

4. A CISO is required to create an annual security capital expense (CapEx) budget.

Which of the following would be INCLUDED in that part of her budget?

A. Fractional costs of employees from other business units who are required to periodically perform security duties.

B. Security equipment purchases which are amortized over a longer period than the calendar budget year.

C. Supporting business unit costs, such as legal advisement and auditing support for the program.

D. All labor expenses realized by employees directly assigned to the security organization.

PRACTICE QUESTIONS

5. A CISO observed that the organization's web filtering solution has been superseded by more effective and advanced versions and should be replaced.

Which of the following BEST describes this analysis?

A. Technology obsolescence.

B. Capital expense planning.

C. Return on investment.

D. Cost-benefit analysis.

EC-Council

www.eccouncil.org