



**Certified Network Defender v3**  
**MODULE 02**  
**ADMINISTRATIVE NETWORK SECURITY**

---

EC-Council Official Curricula

<https://t.me/offensiveSec>



This page is intentionally left blank.





## LEARNING OBJECTIVES

The learning objectives of this module are:

- LO#01: Obtain regulatory frameworks compliance
- LO#02: Discuss various regulatory frameworks, laws, and acts
- LO#03: Learn to design and develop security policies
- LO#04: Conduct security awareness training
- LO#05: Discuss other administrative security measures
- LO#06: Discuss asset management
- LO#07: Learn how to stay up to date on security trends and threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Learning Objectives

Compliance, policies, and governance are integral to an information security program for any organization. An organization needs to comply with certain regulatory standards to run its businesses. At the same time, it must also have strong security policies and governance in order to fulfill regulatory standards. The current module addresses this administrative aspect of an organization's network security.

The objectives of this module are to

- Obtain regulatory frameworks compliance
- Discuss various regulatory frameworks, laws, and acts
- Learn to design and develop security policies
- Conduct security awareness training
- Discuss other administrative security measures
- Discuss asset management
- Learn how to stay up to date on security trends and threats





## LO#01: Obtain regulatory frameworks compliance

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### **LO#01: Obtain Regulatory Frameworks Compliance**

This section explains the need for compliance and how to comply with a regulatory framework.



## Regulatory Frameworks Compliance



It is often required for the organizations to comply with some type of **security regulation**

Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary/mandatory **improvements** to cybersecurity

IT security regulatory frameworks contain a set of **guidelines** and **best practices**

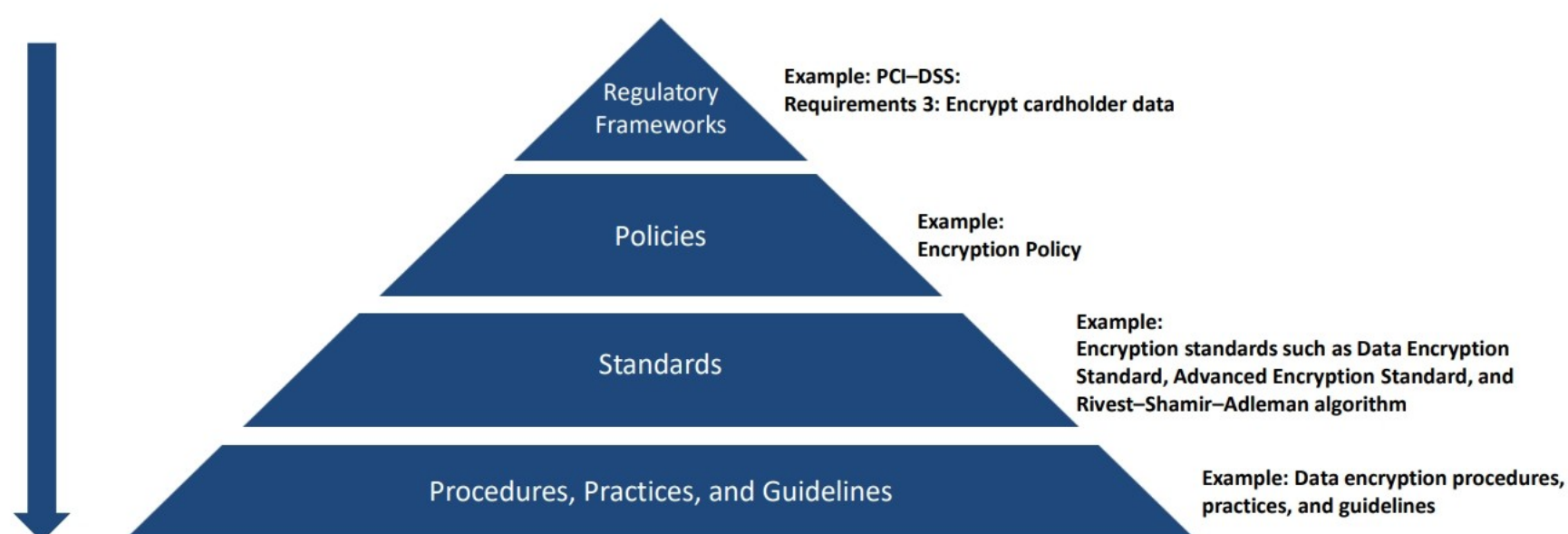
IT security regulatory frameworks **inform businesses** that they need to follow these guidelines and best practices to meet regulatory requirements, improve security, and achieve certain business objectives

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Regulatory Frameworks Compliance (Cont'd)



### Role of Regulatory Frameworks Compliance in an Organization's Administrative Security



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Regulatory Frameworks Compliance

Regulatory framework compliance is a set of guidelines and best practices established in order for organizations to follow and, thus, meet their regulatory needs, enhance processes, improve protection, and accomplish any other objectives based on the industry and data types maintained. Regulatory compliance prevents organizations from incurring large fines or being victim to data breaches. Most organizations comply with more than one regulatory framework. Deciding which framework, policies, and controls are best compatible with an organization's



compliance goals is a difficult task. At the same time, Regulatory framework compliance has an evolving nature because organizational environments are always in flux. Generally, these guidelines are leveraged by

- Internal auditors and other stakeholders who assess the controls an organization requires;
- External auditors who assess the controls an organization requires; and
- Others/third parties (private/governments) such as key customers and investors who assess risk before collaborating with an organization.

### **Role of Regulatory Frameworks Compliance in an Organization's Administrative Network Security**

To ensure cybersecurity, organizations must implement the following standards to meet regulatory framework compliance:

**Regulatory Frameworks:** Under a framework, an organization must document its policies, standards as well as procedures, practices, and guidelines. Each of these aspects have different purposes; hence, they cannot be combined into one document. Examples of regulatory frameworks include the Payment Card Industry—Data Security Standard (PCI-DSS) Requirement 3: Protect stored cardholder data

- **Policies**

Policies are high-level statements dealing with the administrative network security of an organization. These are leveraged by an organization's senior management. Organizations require at least one policy in place. A policy is viewed as a business mandate and has a top-down management. Some examples of policy include email and encryption policies. They generally outline the

- Security roles and responsibilities,
- Scope of information to be secured,
- Description of the required controls for securing information, and
- References to standards and guidelines that support the policies.

- **Standards**

Standards comprise specific low-level mandatory controls or controls related to the implementation of a specific technology useful for enforcing and supporting policies and ensuring consistent businesses security. As noted earlier, this includes password policy such as password standards for password complexity, or encryption policy, which include standards such as data encryption standard (DES), advanced encryption standard (AES), and Rivest–Shamir–Adleman algorithms.

- **Procedures, Practices, and Guidelines**

Procedures or standard operating procedures (SOP) comprise step-wise instructions useful for implementing the controls that are defined by multiple policies, standards, and



guidelines such as a procedure for secure Windows installation or data encryption procedure, practices, and guidelines.

Guidelines comprise recommendations, but non-mandatory controls, as well as general statements, administrative instructions, or best practices useful for supporting standards or acting as a reference when no are standards in place. Guidelines and best practices are interchangeable. These changes are environment-dependent and must be reviewed more often than standards and policies. For example, a standard may state that a password should be eight characters or more, while a supporting guideline may state that it is also a best practice to follow password expiration and data encryption guidelines.



## Why Organizations Need Compliance



### Improves Security

IT security **regulation** and **standards** improve overall security of an organization by meeting regulatory requirements

### Minimize Losses

Improved security, in turn, **prevents** security breaches, which can cost loss to company

### Maintain Trust

Customer trusts the organization in belief that their information is **safe**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Why Organizations Need Compliance

Information security compliance should be a requirement than a choice for organizations, since the money, time, and efforts invested in the compliance is worth more than the cost of risks. The advantages that regulatory framework compliance brings for an organization include

- **Improved Security:** IT security regulations and standards improve the overall security of an organization by meeting baseline regulatory requirements. These baseline requirements ensure consistent data security.
- **Minimized Losses:** Improved security can prevent security breaches, which otherwise can lead to losses, repair costs, legal fees, or hefty fines.
- **Maintenance of Trust:** Data breaches cause companies to lose their reputation and trust from customers. Compliance makes customers trust an organization with the belief that their information is safe.
- **Increased Control:** An organization's security increases with increased controls such as preventing employees from committing mistakes, implementing strong credential systems and encryption systems, or monitoring outside threats.



## Identifying Which Regulatory Framework to Comply



- An organization needs to **assess** itself to determine which regulatory framework applies to it best
- For example, following table shows different regulations and which organization would be subject to the **scope** of the regulatory framework

| Regulatory Framework  | Organizations within Scope  |
|---|---|
| Health Insurance Portability and Accountability Act (HIPAA) | Any company or office that deals with healthcare data, including, but not limited to, doctor's offices, insurance companies, business associates, and employers |
| Sarbanes Oxley Act  | U.S. public company boards, management, and public accounting firms   |
| Federal Information Security Management Act of 2002 (FISMA) | All federal agencies must develop a method of protecting information systems  |
| Gramm Leach Bliley Act (GLBA)                               | Companies that offer financial products or services to individuals such as loans, financial or investment advice, or insurance                                  |
| Payment Card Industry Data Security Standard (PCI-DSS)      | Companies handling credit card information  |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Identifying Which Regulatory Framework to Comply

An organization must perform a self-assessment to ascertain the regulatory frameworks that best applies to it. This compliance assessment involves identifying gaps between the existing control environment and an organization's requirements. However, this is a challenging task wherein an organization should fully understand its needs and function to understand which controls suit its size and complexity. When assessing compliance, an organization must consider the following:

- Financial institution letters;
- National Institute of Standards and Technology publications;
- Industry implementation guidance and recommendations—for example, international standards such as ISO 27002 or the National Institute of Standards and Technology Framework for cybersecurity enhancement; and
- Notice the cybercrimes, new exploits, and new trends to ascertain the possibility of a large-scope breach.



## Deciding on How to Comply to Regulatory Framework



- When an organization falls within scope of certain regulatory framework, it needs to correctly **interpret** regulatory requirements in the regulator framework to be complied with
- Based on those regulatory requirements, an organization needs to establish **policies, procedures**, and **security controls** to manage and maintain compliance

For example, the following table shows some of the PCI-DSS regulatory requirements:

|  | PCI-DSS   |
|--|---|
| Regulatory requirements  | <b>PCI-DSS requirement No 1.1.1:</b> "A formal process for approving and testing all network connections and changes to the firewall and router configurations."<br><b>PCI-DSS Requirement No 1.2.1:</b> "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." |
| Policies, procedures, and controls to satisfy the requirements | Provision for detecting all unauthorized network connections to/from an organization's IT assets  |

|  | PCI-DSS  |
|--|--|
| Regulatory requirements  | <b>PCI-DSS requirement no 1.1.6:</b> "Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure." |
| Policies, procedures, and controls to satisfy the requirements | Provision for looking insecure protocols and services running on systems   |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Deciding on How to Comply to Regulatory Framework (Cont'd)



|  | PCI-DSS   |
|--|---|
| Regulatory requirements  | <b>PCI-DSS requirement no 1.3.1:</b> "Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports."<br><b>PCI-DSS Requirement No 1.3.2:</b> "Limit inbound Internet traffic to IP addresses within the DMZ."<br><b>PCI-DSS Requirement NO 1.3.5:</b> "Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet." |
| Policies, procedures, and controls to satisfy the requirements | Provision for checking how traffic is flowing across the DMZ to/from the internal network   |

|  | PCI-DSS  |
|--|--|
| Regulatory requirements  | <b>PCI-DSS requirement no 5.1:</b> "Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)."<br><b>PCI-DSS requirement no 5.3:</b> "Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period." |
| Policies, procedures, and controls to satisfy the requirements | Provision for detecting malware infection when anti-virus protection is disabled on the machines   |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Deciding on How to Comply to Regulatory Framework

An organization needs to correctly interpret its regulatory requirements once it has confirmed its framework. Then, it must analyze and interpret the collected information to determine how the collected information is relevant to an organization's services. Next, discuss and sort all an organization's internal/external personnel ambiguities, uncertainties, and problems faced during the interpretation of the identified compliance information. Assess and determine the order for suitable compliance requirements such as important implications and risks of possible breaches.



Separate/group the compliance requirements that are perceived as, first, important and central; then, only important; and finally, pertinent, but incidental, for an organization's operations.

Based on the regulatory requirements, an organization needs to establish proper policies, procedures, and security controls to organize its information security.





## LO#02: Discuss various regulatory frameworks, laws, and acts


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### LO#02: Discuss Various Regulatory Frameworks, Laws, and Acts

This section explains the various regulatory frameworks, laws, and acts. It describes frameworks, laws, and acts such as the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Sarbanes–Oxley Act (SOX), Gramm–Leach–Bliley Act (GLBA), ISO Information Security Standards, Digital Millennium Copyright Act (DMCA), and Federal Information Security Management Act (FISMA).






## Payment Card Industry Data Security Standard (PCI-DSS)



- The PCI-DSS is a proprietary **information security standard for organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- It **applies to all entities involved in payment card processing**, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data
- High-level overview of PCI-DSS requirements are developed and maintained by **PCI Security Standards Council**:

### PCI Data Security Standard: High-Level Overview

|   |  |  |
|---|--|--|
| Build and Maintain a Secure Network         |   | Implement Strong Access Control Measures |
| Protect Cardholder Data                     |   | Regularly Monitor and Test Networks      |
| Maintain a Vulnerability Management Program |  | Maintain an Information Security Policy  |

Failure to meet the PCI-DSS requirements may result in fines or termination of payment card processing privileges

Source: <https://www.pcisecuritystandards.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


## Payment Card Industry Data Security Standard (PCI-DSS)

Source: <https://www.pcisecuritystandards.org>

The Payment Card Industry Data Security Standard (PCI-DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point-of-service (POS) cards. It offers robust and comprehensive standards and supporting materials to enhance the data security of payment cards. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI-DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data. It comprises a minimum set of requirements for protecting cardholder data. The high-level overview of the PCI-DSS requirements are developed and maintained by the PCI Security Standards Council.



## Health Insurance Portability and Accountability Act (HIPAA)



| HIPAA's Administrative Simplification Statute and Rules |  |
|---|--|
| Electronic Transaction and Code Sets Standards          | Requires every provider who does business electronically to <b>use the same health care transactions, code sets, and identifiers</b>   |
| Privacy Rule  | Provides <b>federal protections for personal health information</b> held by covered entities and empowers patients with an array of rights with respect to that information  |
| Security Rule   | Specifies a series of administrative, physical, and technical safeguards for covered entities to use as well as to assure the <b>confidentiality, integrity, and availability of electronic protected health information</b> |
| National Identifier Requirements                        | Requires that health care providers, health plans, and employers have standard national numbers that identify them on <b>standard transactions</b>   |
| Enforcement Rule  | Provides standards for enforcing all <b>Administration Simplification Rules</b>  |

Source: <http://www.hhs.gov>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Health Insurance Portability and Accountability Act (HIPAA)

Source: <http://www.hhs.gov>

The Health Insurance Portability and Accountability Act HIPAA of 1996 requires the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates; it gives patients an array of rights with respect to this information. The Privacy Rule permits the disclosure of health information needed for patient care and other important purposes as well. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to assure the confidentiality, integrity, and availability of electronic protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules is discussed below:

- **Electronic Transaction and Code Sets Standards**

Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. HIPAA names certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payments. Under HIPAA, if a covered entity conducts one of the adopted transactions electronically, it must use the adopted



standard—either from Accredited Standards Committee (ASC) X12N or National Council for Prescription Drug Programs (NCPDP) (for certain pharmacy transactions). Covered entities must adhere to the content and format requirements of each transaction.

- **Privacy Rule**

The HIPAA Privacy Rule establishes national standards to protect individual's medical records and other personal health information; it applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on non-patient authorized uses and disclosures of data. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

The HIPAA Security Rule establishes national standards to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity. It requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

HIPAA requires that employers have standard national numbers that identify them on standard transactions.

- **National Provider Identifier Standard**

The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. This standard is a 10-position, intelligence-free numeric identifier (10-digit number). That is, the numbers do not carry other information about health care providers such as the state in which they live or their medical specialty.

- **Enforcement Rule**

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.



## General Data Protection Regulation (GDPR)



- The GDPR is a regulation in European Union law on **data protection and privacy for all individuals within the European Union** and the European Economic Area; it also addresses the export of personal data outside these areas

The GDPR replaces the Data Protection Directive 95/46/EC and is designed to:

- Harmonize data privacy laws across Europe
- Protect and empower all European Union citizens data privacy
- Reshape the way organizations across the region approach data privacy

Source: <https://gdpr.eu>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## General Data Protection Regulation (GDPR)

Source: <https://eugdpr.org>

The GDPR is a regulation in European Union (EU) law on data protection and privacy for all individuals within the EU and the European Economic Area. It also addresses the export of personal data outside the EU and European Economic Area. It simplifies the regulatory environment for citizens and businesses in the EU for the benefit of the digital economy. Organizations with the terms of GDPR ensure the legal collection and management of personal data, or risk facing serious penalties. As per GDPR terms, organizations should hire a data protection officer if they deal with special category of large-scale data processing.

There are two types of data handlers the GDPR applies to:

- **Controllers:** Person/public authority/agency/other body that alone, or jointly with others, determines the purposes and means of the personal data process.
- **Processors:** Person/public authority/agency/other body that processes personal data on behalf of the controller.

The EU GDPR replaces the Data Protection Directive 95/46/EC and is designed to:

- Harmonize data privacy laws across Europe,
- Protect and empower all EU citizens data privacy, and
- Reshape the way organizations across the region approach data privacy.



## Sarbanes–Oxley Act (SOX)

The infographic is titled "Sarbanes–Oxley Act (SOX)" and features the CND logo in the top right corner. It contains two main sections: a list of general SOX Act facts and two detailed sections, Section 302 and Section 404, each with its own list of requirements.

- The SOX Act is a U.S. federal law that sets new or enhanced standards for all U.S. public company **boards, management,** and **accounting firms**
- The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation on **security regulations**

### Section 302

- A mandate that requires senior management to certify the accuracy of the reported financial statement
- CEOs and CFOs of accounting company's clients must sign statements verifying the completeness and accuracy of the financial reports

### Section 404

- A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls
- CEOs, CFOs, and auditors must report on, and attest to the effectiveness of, internal controls for financial reporting

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sarbanes–Oxley Act (SOX)

Source: [www.soxlaw.com](http://www.soxlaw.com)

Enacted in 2002, the SOX Act aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This Act does not explain how an organization needs to store records, but describes records that organizations need to store and the duration of the storage. The Act mandates a number of reforms to enhance corporate responsibility, improve financial disclosures, and combat corporate and accounting fraud.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board**

Title I consists of nine sections and establishes the Public Company Accounting Oversight Board for independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

Title II consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.



- **Title III: Corporate Responsibility**

Title III consists of eight sections and mandates whereby senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the Securities and Exchange Commission (SEC) or its agents of corporate reports.

- **Title V: Analyst Conflicts of Interest**

Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions to bar a person from practicing as a broker, advisor, or dealer.

Given below is the continuation of SOX titles:

- **Title VII: Studies and Reports**

Title VII consists of five sections and requires the Comptroller General and SEC to perform various studies and report the respective findings. These studies and reports include the effects of consolidation of public accounting firms, role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.



- **Title IX: White Collar Crime Penalty Enhancement**

Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

Title X consists of one section and states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

Title XI consists of seven sections. Section 1101 recommends the following name for this title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This allows the SEC to temporarily freeze "large" or "unusual" transactions or payments.



## Gramm-Leach-Bliley Act (GLBA)



- The objective of the **Gramm-Leach-Bliley Act** was to ease the transfer of **financial** information between **institutions** and **banks** while making the rights of the individual more specific through **security** requirements

### Key Points include:

- Protecting consumer's **personal financial information** held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than **\$10,000 for each violation**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Gramm-Leach-Bliley Act (GLBA)

Source: <https://www.ftc.gov>

The Gramm-Leach-Bliley Act (GLB Act or GLBA) is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. The Act requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data. The objective of the GLBA is to ease the transfer of financial information between institutions and banks, while making the rights of the individual through security requirements more specific.

In this regard, the key points include:

- Protecting consumer's personal financial information held by financial institutions and their service providers are the key points of the financial privacy provisions of the GLBA. Companies should give consumers privacy notices that explain the GLBA's information-sharing practices, while customers can limit the sharing of their information.
- If an organization violates GLBA, then
  - It is subject to a civil penalty of not more than \$100,000 for each violation;
  - Officers and directors of an organization shall be subject to, and personally liable for, a civil penalty of not more than \$10,000 for each violation; and
  - The organization and its officers and directors shall also be subject to fines or imprisonment for not more than five years, or both.
- The top information protection requirements of GLBA include



- Financial Privacy Rules to be provided for consumers with privacy notice after the relationship is established with the consumer; and
- Safeguards Rules, which require organizations to develop a written information security plan describing its processes and procedures for protecting clients' NPI.
- The Security and Encryption Requirements for GLBA include
  - Organizations to establish required standards that related to the administrative, technical, and physical security of customer records and information; and
  - Organizations to implement encryption to reduce the risk of disclosure or alteration of information—for example, strong key management practices, robust reliability, and securing the encrypted communication's endpoints.



ISO Information Security Standards



Table with 3 columns: Sr. No., Standards, Objective. Rows 1-16 listing ISO/IEC standards from 27000 to 27017.

Table with 3 columns: Sr. No., Standards, Objective. Rows 17-32 listing ISO/IEC standards from 27018 to 27042.

Source: http://www.iso27001security.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO Information Security Standards (Cont'd)



Table with 3 columns: Sr. No., Standards, Objective. Rows 33-48 listing ISO/IEC standards from 27043 to 27570.

Table with 3 columns: Sr. No., Standards, Objective. Rows 49-50 listing ISO/IEC standards 27701 and 27799.

Source: http://www.iso27001security.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## **ISO Information Security Standards**

### **ISO/IEC 27000**

Source: <https://www.iso27001security.com>

ISO/IEC 27000 provides an overview of information security management systems (ISMS) and defines related terms. The overview of ISMS introduces risk and security management, information security, and management systems. The vocabulary or glossary covers most of the specialist information security-related terms used in the ISO27k standards.

### **ISO/IEC 27001**

Source: <http://www.iso27001security.com>

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which an organization identifies, analyzes, and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities, and business impacts—an important aspect in such a dynamic field and a key advantage of ISO27k's flexible risk-driven approach compared with, for example, PCI-DSS.

### **ISO/IEC 27002**

Source: <http://www.iso27001security.com>

ISO/IEC 27002 is relevant to all types of organizations, including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, government departments, and quasi-autonomous bodies, or any organization that handles and depends on information. The specific information security risk and control requirements may differ in detail, although there is common ground—for instance, most organizations need to address the information security risks relating to their employees plus contractors, consultants, and the external suppliers of information services.

### **ISO/IEC 27003**

Source: <http://www.iso27001security.com>

ISO/IEC 27003 guides the design of an ISO/IEC 27001-compliant ISMS, leading up to the initiation of an ISMS implementation project. It describes the process of ISMS specification and design from inception to the production of implementation project plans, covering the preparation and planning activities *prior* to the actual implementation.

### **ISO/IEC 27004**

Source: <http://www.iso27001security.com>

ISO/IEC 27004 concerns the measurements relating to information security management; these are commonly known as “security metrics”.

### **ISO/IEC 27005**

Source: <http://www.iso27001security.com>



The standard provides guidelines for information security risk management and supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

### **ISO/IEC 27006-n**

Source: <http://www.iso27001security.com>

ISO/IEC 27006 is the **accreditation standard** that guides certification bodies on the formal processes they must follow when auditing their client's Information Security Management Systems (ISMSs) against ISO/IEC 27001 in order to certify or register them compliant. The accreditation processes laid out in the standard give assurance that ISO/IEC 27001 certificates issued by accredited organizations are valid.

### **ISO/IEC 27007**

Source: <http://www.iso27001security.com>

ISO/IEC 27007 provides guidance for accredited certification bodies, internal auditors, external/third-party auditors, and others auditing ISMSs against ISO/IEC 27001 (i.e., auditing the *management system* for compliance with the standard).

ISO/IEC 27007 reflects and largely refers to ISO 19011, the ISO standard for auditing quality and environmental management systems—with “management systems” being the common factor linking it to the ISO27k standards. It provides additional ISMS-specific guidance.

### **ISO/IEC TR 27008**

Source: <http://www.iso27001security.com>

This standard provides guidance for all auditors regarding ISMS controls selected through a risk-based approach (e.g., as presented in a statement of applicability) for information security management. It supports the information security risk management process as well as internal, external, and third-party audits of ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which the required ISMS controls are implemented. Further, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements and as a strategic platform for information security governance.

### **ISO/IEC 27009**

Source: <http://www.iso27001security.com>

This standard is intended to guide those who would develop ‘sector-specific’ standards based on or relating to ISO/IEC 27001, where ‘sector’ means “domain, application area or market sector”.

### **ISO/IEC 27010**

Source: <http://www.iso27001security.com>

This standard provides guidance in relation to sharing information about information security risks, controls, issues, and/or incidents that span the boundaries between industry sectors and/or nations, particularly those affecting “critical infrastructure.”



### **ISO/IEC 27011**

Source: <http://www.iso27001security.com>

This ISMS implementation guide for the telecom industry was developed jointly by ITU Telecommunication Standardization Sector (ITU-T) and ISO/IEC JTC1/SC 27, with the identical text being published as *both* ITU-T X.1051 *and* ISO/IEC 27011.

### **ISO/IEC 27013**

Source: <http://www.iso27001security.com>

This standard provides guidance on implementing an integrated information security and IT service management system based on both ISO/IEC 27001:2005 (ISMS) and ISO/IEC 20000-1:2011.

### **ISO/IEC 27014**

Source: <http://www.iso27001security.com>

ISO/IEC JTC1/SC 27, in collaboration with the ITU-T, has developed a standard specifically aimed at helping organizations govern their information security arrangements.

### **ISO/IEC TR 27015**

Source: <http://www.iso27001security.com>

This is a guideline intended to help financial services organizations (e.g., banks, insurance companies, and credit card companies) implement ISMSs using the ISO27k standards.

Although the financial services sector already labors under a vast swathe of risk and security standards (such as ISO TR 13569 "Banking Information Security Guidelines," SOX and Basel II/III), the ISMS implementation guidance developed by SC 27 reflects ISO/IEC 27001 and 27002, along with various general-purpose security standards such as Control Objectives for Information and Related Technologies(COBIT) and the PCI-DSS requirements.

### **ISO/IEC TR 27016**

Source: <http://www.iso27001security.com>

This standard helps management appreciate and understand the financial impacts of information security in the context of an ISO27k ISMS, along with political, social, compliance, and other potential impacts on an organization that collectively influence how much it needs to invest in protecting its information assets.

### **ISO/IEC 27017**

Source: <http://www.iso27001security.com>

This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of a cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards.

### **ISO/IEC 27018**

Source: <http://www.iso27001security.com>



This standard provides guidance aimed at ensuring that cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them. The standard will be followed by ISO/IEC 27017, covering the wider information security angles of cloud computing, other than privacy.

### **ISO/IEC TR 27019**

Source: <http://www.iso27001security.com>

This standard (a Technical Report) is intended to help organizations in the energy industry interpret and apply ISO/IEC 27002:2005 in order to secure their electronic process control systems.

### **ISO/IEC TR 27021**

Source: <http://www.iso27001security.com>

In order to stabilize and standardize the market for training and certifying professionals for ISO27k implementation and audits, this standard lays out the competence expected of ISMS professionals.

### **ISO/IEC TS 27022**

Source: <http://www.iso27001security.com>

The standard (a Technical Specification) "provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them and describes the ISMS processes implied by ISO/IEC 27001."

### **ISO/IEC 27031**

Source: <http://www.iso27001security.com>

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

The standard

- Suggests a structure or framework (actually a set of methods and processes) for any organization, whether private, governmental, or non-governmental;
- Identifies and specifies all relevant aspects including performance criteria, design, and implementation details for improving information and communications technology (ICT) readiness as part of an organization's ISMS; thus, it helps ensure business continuity; and
- Enables an organization to measure its ICT continuity, security, and, hence, readiness to survive a disaster in a consistent and recognized manner.

### **ISO/IEC 27032**

Source: <http://www.iso27001security.com>



ISO/IEC 27032 addresses “cybersecurity” or “cyberspace security,” defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace.” In turn “the cyberspace” is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.”

### **ISO/IEC 27033-n**

Source: <http://www.iso27001security.com>

ISO/IEC 27033 provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their security, network applications/services and users of the network, in addition to security of information being transferred through communications links. It is aimed at network security architects, designers, managers, and officers.

### **ISO/IEC 27034 -n**

Source: <http://www.iso27001security.com>

ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, and implementing and using application systems, that is, business and IT managers, developers and auditors, and ultimately the end-users of ICT. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of an organization’s ISMS, adequately addressing many ICT security risks.

### **ISO/IEC 27035-n**

Source: <http://www.iso27001security.com>

Information security controls are imperfect in various ways: controls can be overwhelmed or undermined (e.g., by competent hackers, fraudsters, or malware), fail in service (e.g., authentication failures), work partially or poorly (e.g., slow anomaly detection), or be more or less completely missing (e.g., not [yet] fully implemented, not [yet] fully operational, or never even conceived because of failures upstream in risk identification and analysis). Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously.

### **ISO/IEC 27036 -n**

Source: <http://www.iso27001security.com>

ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information security risks involved in the acquisition of ICT products (goods and services) from suppliers.

The standards prevent mentioning to selling and buying since the issues are much the same whether the transactions are commercial or not.

### **ISO/IEC 27037**

Source: <http://www.iso27001security.com>



This standard provides guidance on identifying, gathering/collecting/acquiring, handling, and protecting/preserving digital forensic evidence, that is, “digital data that may be of evidential value” for use in court. The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

### **ISO/IEC 27038**

Source: <http://www.iso27001security.com>

Digital data sometimes have to be revealed to third parties, occasionally even published to the public, for reasons such as disclosure of official documents under Freedom of Information laws or as evidence in commercial disputes or legal cases. “Redaction” is the conventional term for the process of denying file recipients’ knowledge of certain sensitive data within the original files.

### **ISO/IEC 27039**

Source: <http://www.iso27001security.com>

Intrusion detection systems (IDSs) are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. Intrusion prevention systems (IPSs) take automation a step further by automatically responding to certain types of identified attack—for example, by closing off specific network ports through a firewall to block identified hacker traffic. Intrusion detection and prevention systems combine features of both IDSs and IPSs.

### **ISO/IEC 27040**

Source: <http://www.iso27001security.com>

The proposers of this standard claim that the information security aspects of data storage systems and infrastructures have been neglected because of misconceptions and limited familiarity with the storage technology, or in the case of (some) storage managers and administrators, a limited understanding of the inherent risks or basic security concepts.

### **ISO/IEC 27041**

Source: <http://www.iso27001security.com>

The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.



## **ISO/IEC 27042**

Source: <http://www.iso27001security.com>

The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for the forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

## **ISO/IEC 27043**

Source: <http://www.iso27001security.com>

The fundamental purpose of the digital forensics standards ISO/IEC 27037, 27041, 27042, 27043, and 27050 is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

## **ISO/IEC 27050-n**

Source: <http://www.iso27001security.com>

The fundamental purpose of the ISO27k digital forensics standards is to promote good practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls in compliance with local laws, regulations and established practices, it is hoped that standardization will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

## **ISO/IEC 27070**

Source: <http://www.iso27001security.com>

The integrity and hence value of some security functions and subsystems (particularly those relating to cryptography) relies on their being based on trustworthy foundations known as the Root of Trust. Special RoT security arrangements are necessary to negate threats involving low-level exploitation of data-processing chips, devices or systems, in turn compromising the higher-level firmware, device drivers, operating system and application software that build upon the RoT. Whereas trusted computing generally involves some form of Hardware Security Module (e.g. an ISO/IEC 11889 Trusted Platform Module) providing various cryptographic functions and key storage in a physically secure tamper-resistant enclosure, that architecture is not well suited



to cloud computing. In the cloud, systems are virtualized, hence they cannot readily access and rely directly upon hardware-based RoT in the conventional manner.

### **ISO/IEC 27799**

Source: <http://www.iso27001security.com>

This standard provides guidance to health care organizations and other custodians of personal health information on how best to protect the confidentiality, integrity, and availability of such information by implementing ISO/IEC 27002. Specifically, it addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions, and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, adaptability, and availability of personal health information.

### **ISO/IEC 27100**

Source: <http://www.iso27001security.com>

Cybersecurity is a broad term used differently throughout the world. This document defines cybersecurity, establishes its context, and describes relevant concepts, including how cybersecurity is related to and different from information security. Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

### **ISO/IEC 27102**

Source: <http://www.iso27001security.com>

There is a global market for 'cyber-insurance', providing options for the transfer of some information/commercial risks to commercial providers. At present, the focus is primarily on sharing risk and providing compensation for the business costs and consequences arising from 'cyber-incidents' (such as serious privacy breaches caused by hacks and malware infections) that have not been entirely avoided, mitigated, or simply accepted by the organization.

### **ISO/IEC 27103**

Source: <http://www.iso27001security.com>

It provides guidance for those implementing the ISO27k standards, covering the management system aspects. Its scope is simply to provide explanation and guidance on ISO/IEC 27001:2013. The standard supplements and builds upon other standards, particularly ISO/IEC 27000 and ISO/IEC 27001 plus ISO/IEC 27004, ISO/IEC 27005, ISO 31000 and ISO/IEC 27014.

### **ISO/IEC TS 27110**

Source: <http://www.iso27001security.com>

This Technical Specification offers guidance for those within organizations who are creating cybersecurity frameworks, defined as basic sets of concepts used to organize and communicate cybersecurity activities.



## **ISO/IEC 27400**

Source: <http://www.iso27001security.com>

The standard provides guidance on the principles, [information] risks, and the corresponding information security and privacy controls to mitigate those risks associated with the Internet of Things.

## **ISO/IEC TR 27550**

Source: <http://www.iso27001security.com>

Privacy engineering involves taking account of privacy during the entire cradle-to-grave lifecycle of IT systems and the associated processes, such that privacy is and remains an integral part of their function.

## **ISO/IEC 27553-n**

Source: <http://www.iso27001security.com>

This standard provides high-level requirements for biometric authentication on mobile devices, including functional components and communications. Biometrics are increasingly used for user authentication on mobile devices. They are easier to use and harder to steal or fake than conventional passwords and tokens. However, proliferating devices and approaches are fragmenting the market, hence standardization offers advantages for users and manufacturers.

## **ISO/IEC 27555**

Source: <http://www.iso27001security.com>

This standard gives guidance on the deletion of Personally Identifiable Information using a systematic approach supporting ISO/IEC 29100's "Privacy framework".

## **ISO/IEC 27556**

Source: <http://www.iso27001security.com>

This standard lays out a "user-centric framework" (an architecture) to handle personal information in a controlled manner in accordance with the privacy-by-design and other requirements of applicable privacy laws and regulations. The standard outlines a mechanism for organizations handling personal data to comply with the data subject's privacy requirements, even as the organizations share and collaborate on processing the data.

## **ISO/IEC 27557**

Source: <http://www.iso27001security.com>

This standard advises on managing privacy risks (risks relating to or arising from the processing of personal information) that could impact the organization and/or individuals (data subjects) as an integral part of the organization's overall risk management. It supports the requirement for risk management as specified in management systems such as ISO/IEC 27001 (ISMS) and ISO/IEC 27701 (PIMS), plus risk management standards - particularly ISO 31000, ISO/IEC 29134 and ISO/IEC 27005. The standard distinguishes information risks (with the potential to harm the



organization directly) from privacy risks (with the potential to harm individuals directly and the organization indirectly), emphasizing difference in the respective risk management activities.

### **ISO/IEC 27559**

Source: <http://www.iso27001security.com>

This standard proposes a 'principles-based' framework/structure for identifying and mitigating privacy-related risks such as re-identification etc. during the lifecycle of supposedly de-identified data. It advises on properly de-identifying (anonymizing) personal data in order to build trust with data subjects and comply with applicable obligations under GDPR and other privacy laws and regulations.

### **ISO/IEC TS 27570**

Source: <http://www.iso27001security.com>

Smart cities are emerging from the confluence of public wireless networks, mobile/portable devices, the Internet of Things (both industrial and consumer), automation, cloud computing, smart devices with advanced automation and artificial intelligence/machine learning, big data and more. As disparate ICT system are increasingly and dynamically communicating within our cities, both opportunities and risks are opening for individuals plus the commercial and governmental agencies providing various services (such as communications, energy, transportation, healthcare and law enforcement).

### **ISO/IEC 27701**

Source: <http://www.iso27001security.com>

This standard explains how to 'enhance' (adapt and extend) an ISO/IEC 27001 Information Security Management System and the associated ISO/IEC 27002 controls to manage privacy as well as information security.

### **ISO 27799**

Source: <http://www.iso27001security.com>

This standard offers guidance on information security management and information security controls in the context of the healthcare industry and medical organizations of various kinds - hospitals, labs, surgeries, medical insurers etc.



## DMCA and FISMA

### The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization**
- It defines **legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the **removal** or **alteration** of copyright management information

Source: <http://www.copyright.gov>

### Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support federal operations and assets
- It includes
  - Standards for **categorizing** information and information systems by mission impact
  - Standards for minimum **security requirements** for information and information systems
  - Guidance for selecting appropriate **security controls** for information systems
  - Guidance for **assessing security controls** in information systems and determining security control effectiveness
  - Guidance for the security authorization of information systems

Source: <http://csrc.nist.gov>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## DMCA and FISMA

### The Digital Millennium Copyright Act

Source: <http://www.copyright.gov>

The **Digital Millennium Copyright Act** (DMCA) is a U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information in order to implement US treaty obligations. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

Title I implements the WIPO treaties. First, it makes certain technical amendments to U.S. law in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and another on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications
- System caching



- Storage of information on systems or networks at direction of users
- Information location tools

The new section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

▪ **Title III: COMPUTER MAINTENANCE OR REPAIR**

Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

▪ **Title IV: MISCELLANEOUS PROVISIONS**

Title IV contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office. The second provision grants exemption for the making of “ephemeral recordings.” The third provision promotes the distance education study. The fourth provision provides exemption for Nonprofit Libraries and Archives. The fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors, and screen actors to obtain residual payments for the exploitation of motion pictures in situations in which the producer is no longer able to make these payments.

▪ **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

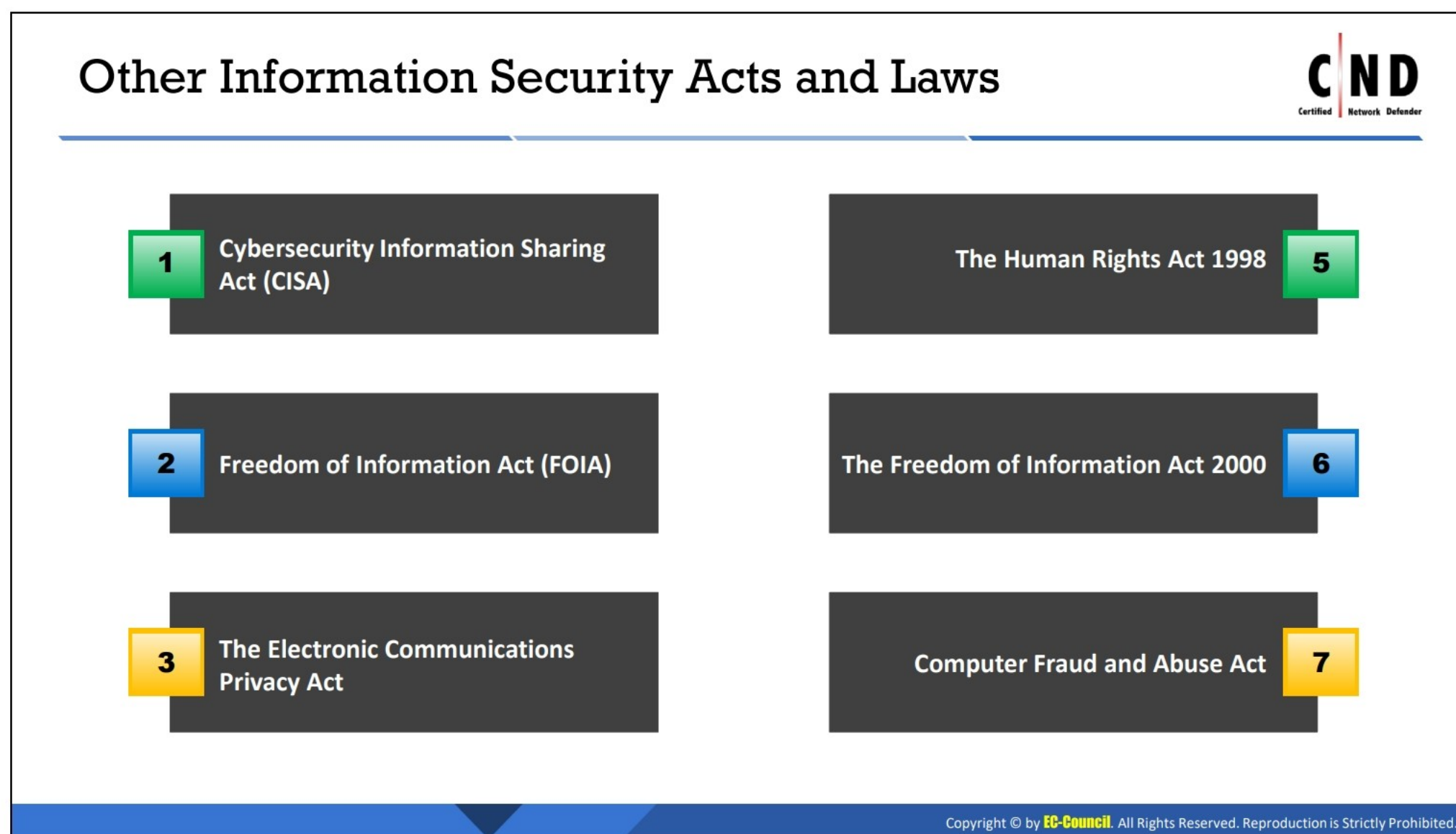
Title V of the DMCA entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, “useful articles” are limited to the hulls (including the decks) of vessels no longer than 200 ft.

**Federal Information Security Management Act**

Source: <http://csrc.nist.gov>

**Federal Information Security Management Act (FISMA)** of 2002 produces several key security standards and guidelines required by Congressional legislation. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.





## Other Information Security Acts and Laws

### Cybersecurity Information Sharing Act (CISA)

Source: <https://www.cisa.gov/>

As mandated by the Cybersecurity Information Sharing Act of 2015 help non-federal entities share cyber threat indicators with the Federal Government. There are policies and procedures relating to the receipt and use of cyber threat indicators by federal entities, guidelines relating to privacy and civil liberties in connection with the exchange of those indicators, and guidance to federal agencies on sharing information in the government's possession.

### Freedom of Information Act

Source: <http://www.foia.gov>

The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens informed about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions that protect interests such as personal privacy, national security, and law enforcement.

### The Electronic Communications Privacy Act

Source: <https://it.ojp.gov>

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and



other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA in order to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

### **The Human Rights Act 1998**

Source: <http://www.legislation.gov.uk>

This Act buttresses the rights and freedoms guaranteed under the European Convention on Human Rights; it makes provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights, and for other related purposes.

### **The Freedom of Information Act 2000**

Source: <http://www.legislation.gov.uk>

This Act makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958, and for related purposes.

### **Computer Fraud and Abuse Act**

Source: <https://ilt.eff.org>

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is an amendment made in 1986 to the Counterfeit Access Device and Abuse Act 1984, and essentially states that, whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, and if the conduct involves an interstate or foreign communication, shall be punished under the Act. In 1996 the CFAA was, again, broadened by an amendment that replaced the term “federal interest computer” with the term “protected computer” 18 U.S.C. § 1030. While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and address federal computer offenses, an amendment in 1994 allows civil actions to be brought under the statute as well.



# Cyber Laws in Different Countries



|               | Laws/Acts  | Website   |
|---------------|--|---|
| United States | Section 107 of the Copyright Law mentions the doctrine of "fair use" | <a href="http://www.copyright.gov">http://www.copyright.gov</a>   |
|               | Online Copyright Infringement Liability Limitation Act               |   |
|               | The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)                   | <a href="http://www.uspto.gov">http://www.uspto.gov</a>           |
|               | The Electronic Communications Privacy Act                            | <a href="https://www.fas.org">https://www.fas.org</a>             |
|               | Foreign Intelligence Surveillance Act                                | <a href="https://www.fas.org">https://www.fas.org</a>             |
|               | Protect America Act of 2007  | <a href="http://www.justice.gov">http://www.justice.gov</a>       |
|               | Privacy Act of 1974  | <a href="http://www.justice.gov">http://www.justice.gov</a>       |
|               | National Information Infrastructure Protection Act of 1996           | <a href="http://www.nrotc.navy.mil">http://www.nrotc.navy.mil</a> |
|               | Computer Security Act of 1987  | <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>           |
|               | Federal Information Security Management Act (FISMA)                  | <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>           |
|               | The Digital Millennium Copyright Act (DMCA)                          | <a href="http://www.copyright.gov">http://www.copyright.gov</a>   |
|               | Sarbanes Oxley Act (SOX)   | <a href="https://www.sec.gov">https://www.sec.gov</a>             |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Cyber Laws in Different Countries (Cont'd)



| Country Name   | Laws/Acts   | Website   |
|----------------|---|---|
| Australia      | The Trade Marks Act 1995  | <a href="http://www.comlaw.gov.au">http://www.comlaw.gov.au</a>           |
|                | The Patents Act 1990  |   |
|                | The Copyright Act 1968  |   |
|                | Cybercrime Act 2001   |   |
| United Kingdom | The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002                          | <a href="http://www.legislation.gov.uk">http://www.legislation.gov.uk</a> |
|                | Trademarks Act 1994 (TMA)   |   |
|                | Computer Misuse Act 1990  |   |
| China          | Copyright Law of People's Republic of China (Amendments on October 27, 2001)                    | <a href="http://www.npc.gov.cn">http://www.npc.gov.cn</a>                 |
|                | Trademark Law of the People's Republic of China (Amendments on October 27, 2001)                | <a href="http://www.saic.gov.cn">http://www.saic.gov.cn</a>               |
| India          | The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957               | <a href="http://www.ipindia.nic.in">http://www.ipindia.nic.in</a>         |
|                | Information Technology Act  | <a href="http://www.dot.gov.in">http://www.dot.gov.in</a>                 |
| Germany        | Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage | <a href="http://www.cybercrimelaw.net">http://www.cybercrimelaw.net</a>   |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Cyber Laws in Different Countries

Countries enact cyber laws depending on their requirements. Already, most countries in the world have laws in place to deal with cybercrimes. Cyber laws are designed based on the framework principles of the UNCITRAL Model Law on Electronic Commerce.





### LO#03: Learn to design and develop security policies


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## LO#03: Learn to Design and Develop Security Policies

Organizations need to design and develop security policies and procedures to ensure availability, confidentiality, and integrity across the network. This section explains how to design and develop security policies. It also describes the design and development considerations for various security policies.



## Security Policy



- A security policy is a **well-documented** set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization
- Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources.
- The security policy is an **integral** part of an information security management program for any organization

### Need for a Security Policy

- Provide consistent application of **security principles** throughout the organization
- Ensure **information security standards** compliance
- Limit the organization's **exposure** to external information threats
- Outline senior management's commitment in maintaining a **secure environment**

- Provide **legal protection**
- Quickly respond to security incidents
- Reduce the **impact** of a security incident
- Minimize the risk of a **data breach**
- Enhance the overall data and network security

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Security Policy

A security policy is a high-level document, or set of documents, describing the security controls to implement in order to protect a company. It maintains confidentiality, availability, integrity, and asset values. Security policies form the foundation of a security infrastructure. Without them, it is impossible to protect the company from possible lawsuits, lost revenue, and bad publicity, or even basic security attacks. Such policies accomplish three goals:

- Reduce or eliminate the legal liability to employees and third parties;
- Protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification; and
- Prevent computing resource waste.

A security policy comprises objectives, rules for behavior, and requirements to secure an organization's network and computer systems. Security policies function as a connecting medium between the objectives and security requirements, as well as to help users, staff, and managers protect technology and information assets. The policy provides a baseline to acquire, configure, and audit computer systems and networks.

A security policy defines a set of security tools for preventing attacks on the entire network in order to keep malicious users away from an organization and provide control over perilous users within an organization.

The security policy should ensure the confidentiality, privacy, integrity, and availability of the company's assets.



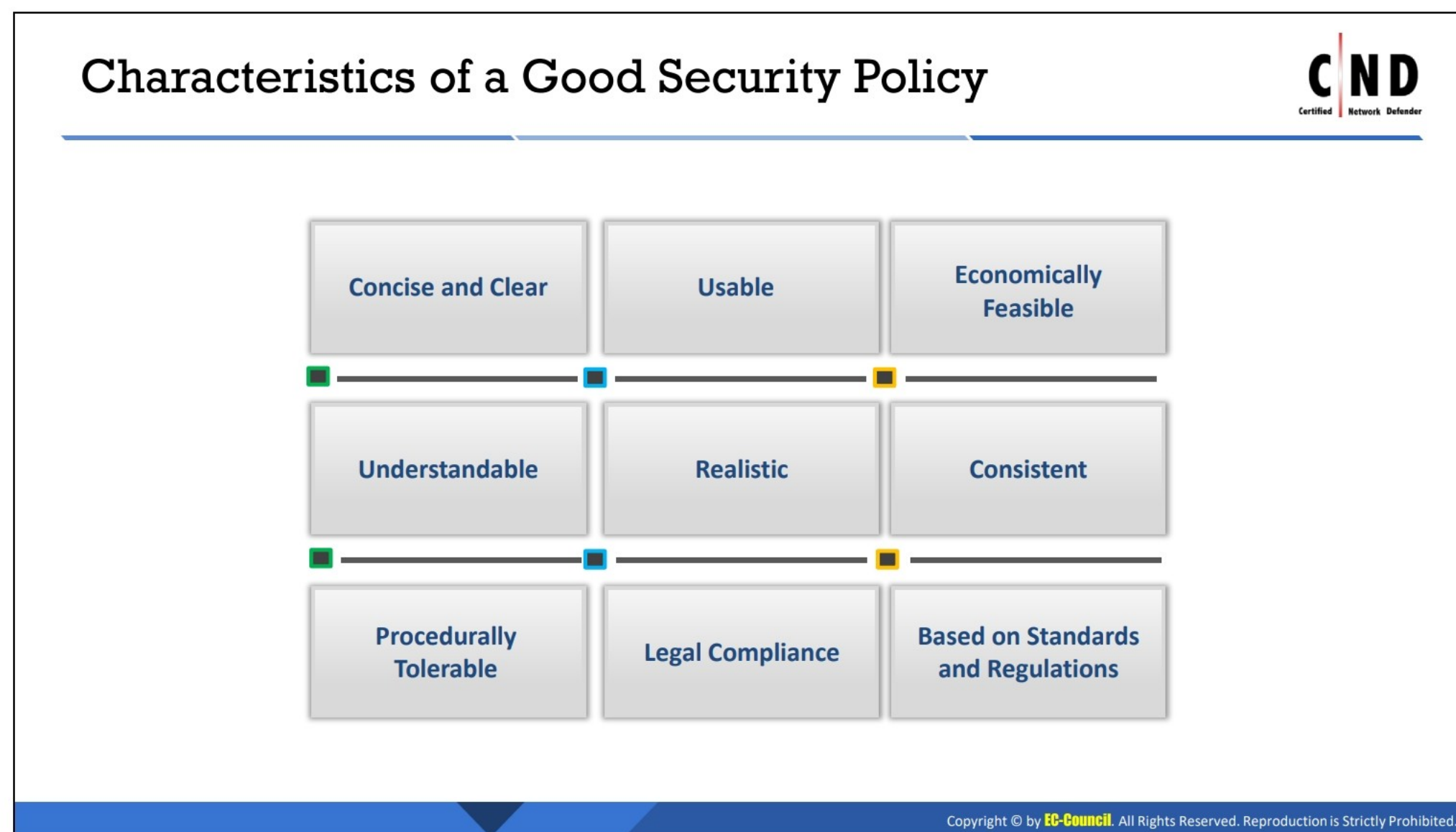
## Need for Security Policy

- The number of devices used across an organization is increasing, which is, in turn, increasing the size and complexity of the information being transferred, networks being used, and storage space. At the same time, the likelihood of security threats originating from various vulnerabilities is increasing. A security policy enables an organization to combat such threats and protect it from losing information.
- A security policy provides consistent application of security principles throughout the company to ensure secure functioning of services. It ensures compliance to information security industry standards, building a trust-based relationship with clients. It helps limit a company's exposure to external information threats, while indicating senior management's commitment to maintaining a secure environment.
- Further, security policy provides legal protection by defining what rules to use on the network, how to handle confidential information, and the proper use of encryption, which together reduce liability and exposure of an organization's data.
- Security policies reduce the risk of damaging security incidents by identifying the vulnerabilities and predicting the threats before they occur.
- They also comprise procedures and techniques to minimize the risk of an organization's data leak or loss by adopting backup and recovery options.

## Advantages of Security Policies

- **Enhanced Data and Network Security:** Organizations implement a policy based on their network, which enhances their data security. It facilitates protection when sharing information among other systems on a network.
- **Risk Mitigation:** The risks involved from external sources are reduced by implementing and deploying security policy. If an employee follows the policy exactly, it becomes nearly impossible for an organization to lose its data and resources.
- **Monitored and Controlled Device Usage and Data Transfers:** Although policies are being implemented thoroughly by employees, administrators should regularly monitor the traffic and external devices used in the system. Monitoring and auditing the incoming and outgoing traffic should always be done on regular intervals.
- **Better Network Performance:** When security policies are implemented correctly and the network is monitored regularly, no unnecessary loads exist. The data transmission speed in the system increases, providing an overall performance enhancement.
- **Quick Response to Issues and Lower Downtime:** Policy deployment and implementation enables faster response rates when resolving network issues.
- **Reduction in Management Stress Levels:** The role of management becomes less stressful when policies are implemented. Every policy must be followed by every employee in an organization. If this occurs, management will be less burdened by potential malicious attacks on the network.
- **Reduced Costs:** If employees follow the policies correctly, the cost of each intrusion is reduced as well as the impact on an organization.





## Characteristics of a Good Security Policy

### Features of a Good Security Policy

- **Concise and Clear:** A security policy needs to be concise and clear, which ensures easy deployment in the infrastructure. Complex policies become hard to understand and employees may not implement them as a result.
- **Usable:** Policies must be written and designed, so they may be used easily across various sections of an organization. Well-written policies are easy to manage and implement.
- **Economically Feasible:** Organizations must implement policies that are economical and enhance the security of an organization.
- **Understandable:** Policies must be easy to understand and follow.
- **Realistic:** Policies must be practical based on reality. Using fictional items in a policy will only hurt an organization.
- **Consistent:** Organizations must have consistency when implementing their policies.
- **Procedurally Tolerable:** Procedural policies should be employer–employee friendly.
- **Cyber and Legal Laws, Standards, Rules, and Regulations Compliance:** Any policy that is implemented must comply with all rules and regulations regarding cyber laws.

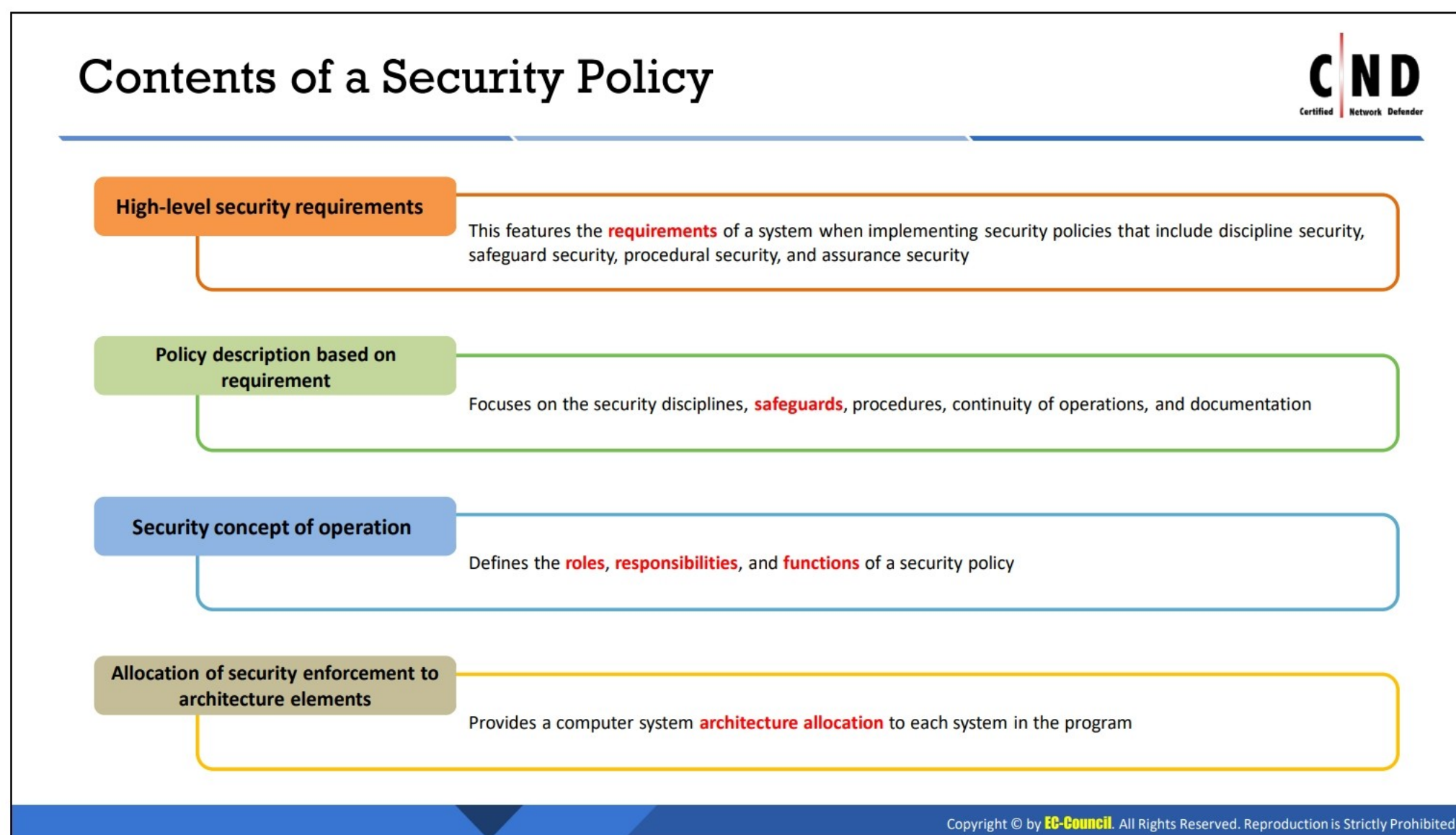
### Key Elements of Security Policy

- **Clear Communication:** Communication must be clear when designing a security policy. A communication gap leads to undesirable results. At the same time, some policies may be infeasible for users or a network. Keep communication channels clear.



- **Brief and Clear Information:** Any information provided to developers regarding the creation of the network policy must be clear and understandable. Failure to do so would hamper network security expectations.
- **Defined Scope and Applicability:** The scope identifies the items that must be covered, hidden, protected, or public, and how to secure them. The network policy addresses a wide range of issues from physical to personal security.
- **Enforceable by Law:** The security policy must be enforceable by law. Penalties should be imposed in the event of a policy breach. Penalties for a violation must be addressed when the policy is created.
- **Recognizes Areas of Responsibility:** The network policy must recognize the responsibilities of employees, the organization, and third parties.
- **Sufficient Guidance:** A good network policy must have proper references to other policies; this helps guide and redefine the scope and the objectives of the policy.





## Contents of a Security Policy

### Security Policy Implementation

There are four aspects in security policy implementation: security requirements, policy description, security concept of operation, and architecture element allocation. We explain these further below:

#### Security Requirements

Security requirements include all requirements for a system to implement security policies. These are further divided into four types:

- **Discipline Security Requirements:** Actions to be taken for various components that need to be secured such as computer security, operations security, network security, personnel security, and physical security
- **Safeguard Security Requirements:** Protective measures required such as protective measures for access control, malware protection, audit, availability, confidentiality, integrity, cryptography, identification, and authentication
- **Procedural Security Requirements:** Access policies, accountability, continuity of operations, and documentation
- **Assurance Security Requirements:** Policies used with the compliance of various standards, certifications, and accreditations



## **Policy Description**

Policy description mainly focuses on the security disciplines, safeguards, procedures, continuity of operations, and documentation. Each subset of this policy describes how the system's architecture elements will enforce security.

## **Concept of Operation**

This concept defines the roles, responsibilities, and functions of a security policy. It focuses on the mission, communications, encryption, user and maintenance rules, idle time management, privately owned versus public domain, shareware software rules, and virus protection policy.

## **Architecture Element Allocation**

This policy allocates computer system architecture to each system in the program.





## Typical Policy Document Content

Next, the important policy sections are as follows:

- **Overview** of a security policy provides background information that the policy needs to address.
- **Purpose** is a detailed explanation of why the policy needs to be framed.
- **The scope** includes information about who and what the policy covers.
- **Definitions** are the terms used in the policy.
- **Roles and Responsibilities** are defined for the employees and management.
- **Target Audience** is the users and clients the policy is being created for.
- **Policies** are statements on each aspect of the policy.
- **Sanctions and Violations** defines the allow/deny process clients and users must follow.
- **Contact Information** includes information about who to contact in case there is a policy sanction and/or violation.
- **Version** number ensures all changes/updates to the policy are tracked correctly.
- **Glossary/Acronyms** list the different terms and abbreviations used in the policy.



## Policy Statements



■ A policy is only as **effective** as the policy statements it contains; policy statements must be written in a very **clear** and **formal** style

Several good examples of a policy statement are:

- |           |  |           |   |
|-----------|--|-----------|---|
| <b>01</b> | All computers must have <b>anti-virus protection</b> activated to provide real-time, continuous protection | <b>04</b> | All computer software must be purchased by the IT department in accordance with the organization's <b>procurement policy</b>                          |
| <b>02</b> | All servers must have the <b>minimum services configured</b> to perform their designated functions         | <b>05</b> | A copy of all backup and restoration media must be kept with the <b>off-site</b> backup media   |
| <b>03</b> | All access to data is based on a <b>valid business need</b> and subject to a formal approval process       | <b>06</b> | While using the Internet, no user is permitted to abuse, defame, stalk, harass, threaten anyone, or violate local and international <b>cyber laws</b> |

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

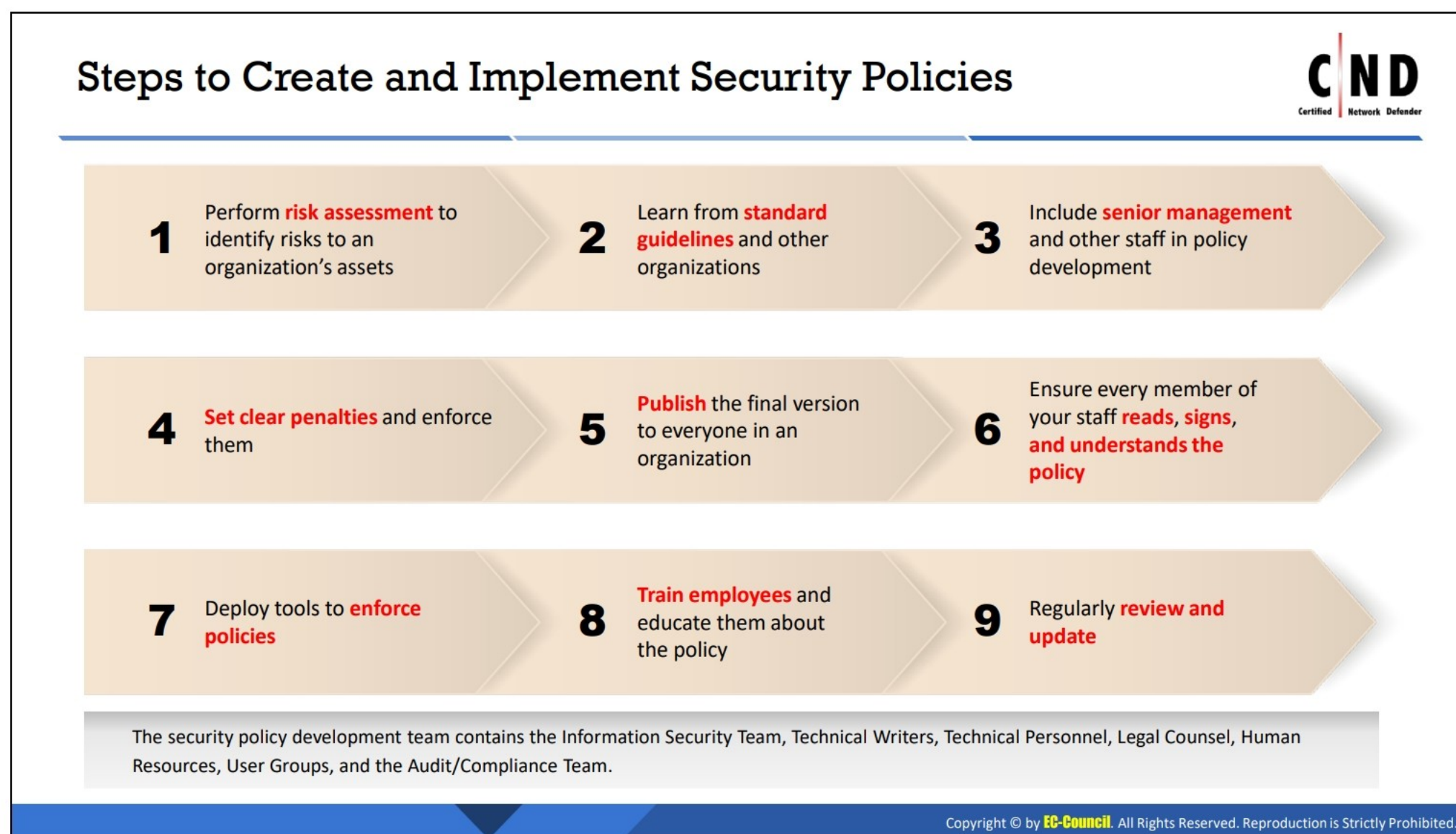
### Policy Statements

An organization's security policy is said to be successful if it consists of clear and concise policy statements. A policy statement is an outline that defines the in-depth structure of an organization's policy. Every policy draft should have a valid policy statement that defines an organization's course of action during a circumstantial situation. The policy statement helps employees understand the preventive measures they are permissible to take. An example of an ideal policy statement is:

**"All access to data will be based on a valid business need and is subject to a formal approval process."**

The above policy statement example clearly states employees can access data only on approval from management. Thus, if any employee does not adhere to the policy statement, an organization has the right to take required action.





## Steps to Create and Implement Security Policies

The steps below are used to create and implement an effective security policy:

- 1. Risk Assessment:** An organization needs to perform a risk assessment of its assets before drafting a policy. During a risk assessment, risks are identified, and their severity and criticality determined.
- 2. Standard Guidelines:** An organization sets up guidelines before drafting its own security policy. Clear standard guidelines are helpful to an organization and its employees.
- 3. Management Input:** Management is involved in the process of drafting a new policy or adding a policy to the existing one. Employees will only adhere to the drafted policy if management legally sanctions and approves it. Any policy drafted without management consent is illegal and will cause serious consequences.
- 4. Penalties:** Certain organizations have strict policies. If an employee does not follow these policies, severe actions can be taken against them. An organization should always state the penalties that an employee may be subjected to if he or she does not follow the rules.
- 5. Final Draft:** Once management approves the completed policy document, this document is distributed throughout an organization.
- 6. Accepted by Employees:** Employees are required to accept all policies set by an organization. Employees are expected to carefully read the document, and then sign it.
- 7. Deployment of Policies:** To enforce policies in an organization you may need additional deployment tools.



8. **Training the Employees:** Employees should be periodically trained in understanding organizational policies. Even if the policies in an organization have been functional over time, new employees should be trained. This is a critical task.
9. **View and Update:** Even if an organization has been in business for a long time, reviewing its policies is still important. With the introduction of new technologies and new security breaches, updating policies is a necessity. Policies that no longer protect the current technology and/or scenarios are not useful to an organization.



## Considerations Before Designing a Security Policy



|   |  |
|---|--|
| ✓ | What is the <b>purpose</b> of the policy? Is it a value addition or a mere formality?                |
| ✓ | Is the policy in line with the <b>training programs</b> ?  |
| ✓ | Does the policy <b>comply</b> with the organization's objectives?                                    |
| ✓ | Is the policy a guideline for best practices or does it need to be <b>based on a some standard</b> ? |
| ✓ | How many people fall under the scope of the policy, and who are they?                                |
| ✓ | What is the least amount of information each employee must know in order to do his or her job?       |
| ✓ | Are all details required in the policy?  |
| ✓ | Can the policies be <b>linked</b> ? What is the best method?   |
| ✓ | What does the <b>staff need</b> to understand from the policies?                                     |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Considerations Before Designing a Security Policy

Organizations should not deploy a policy without knowing the purpose first.

Before designing a security policy, answer the following questions:

- **What is the purpose of the policy? Is it a value add or a mere formality?**

An organization or management should be aware of the policy's purpose when it is deployed. If management understands the purpose of the policy, it will be easier to make employees adhere to it.

- **Is the policy in line with any training program?**

Usually, an organization introduces a policy without training or conducting workshops for the employees. It is necessary to deploy only those policies employees have been trained for. Policies without training or workshops will not effectively serve an organization, as employees would not be aware of its pros and cons.

- **Does the policy comply with an organization's objectives?**

While documenting the policy, it should be noted that the policy runs parallel to the objectives of an organization. Policy implementation cannot be successful if it does not meet organizational objectives.

- **Is the policy a guideline for a better practice or does it need to be based on a standard?**

The purposes of introducing policies may differ. It is important to know why the policies are being introduced. Usually, certain policies are formed as per the regulations by the government and some are implemented for an organization's personal security.



- **How many people fall under the purview of this policy, and who are they?**

While designing a policy, there may be situations where only some employees, or a particular group of them, needs to adhere to it. It is important to categorize these types of policies in order to simplify implementation in an organization.

- **What is the least every employee needs to know?**

All an employee should know regarding the policy is how it is routinely implemented. The training session conducted for the employees should inform them about the action taken against them in case of compliance issues.

- **Do I really need all details written into this policy, or is this better written in System-Specific Security Policies for the IT professional?**

While a policy is documented, it is important to understand its target. Every policy might not necessarily be part of the same document—for example, the document for security policy will not include the human resource policy.

- **What do the staff need to understand from the policy?**

Management should keep the main objective clear and use user-friendly language. For example, if the policies apply to all members of an organization, management should arrange training sessions or workshops to help employees fully understand them without uncertainty. With the introduction of these policies, an organization clarifies to employees the level of awareness required for securing the data and resources in the network.



## Design of a Security Policy



Guidelines should cover the following **policy structure** points:

- Detailed description of **policy issues**
- **Functionalities** of those affected by the policy
- **Compatibility level** of the policy is necessary
- Consequences of **non-compliance**
- **Applicability** of policy to the environment
- **Description** of policy status

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Design of a Security Policy

The security policy structure provides an overview of the functionalities of security aspects. The security policy structure should ensure that the following are in place:

- Description of the issue pertaining to the policy;
- Details of the policy status and description of the domains where the policy has been applied;
- Functions and responsibilities of employees involved in the policy;
- Extent to which the policy is compatible with an organization's standards;
- The tasks and procedures involved and not involved in the policy; and
- End consequences will be encountered if the policy is not compatible with an organization's standards.

The security policy must contain all information required for successful implementation of an organizational work process. Consider the following key points while designing security policies:

- **Develop Policies to Enforce:** Not enforcing a policy has no purpose. Real-time implementation of all statements mentioned in the policy is necessary for limiting network access.
- **Explain the Policy Purpose:** Based on the functions of an organization, develop the policies for a specific network objective.
- **Develop Security Policies Not Requiring Frequent Updates:** To avoid frequent amendments, the overall network issues should be pre-estimated.



- **Differentiate between Policies, Standards, and Recommendations:** The network policies should be comprehensive and thorough, but should not be too specific.
- **Represent Basic Organizational Goals:** Depending on the information, the assets of an organization represent the range of the network security.
- **Ensure your Policies are Understood:** Network policies should be straightforward and not too complicated.
- **Include Policies in Security Awareness Training:** At least one policy has to be included in the security awareness training.
- **Identify Basic Risks Expected:** The basic risk factors of the network are to be pre-estimated by the network admin.

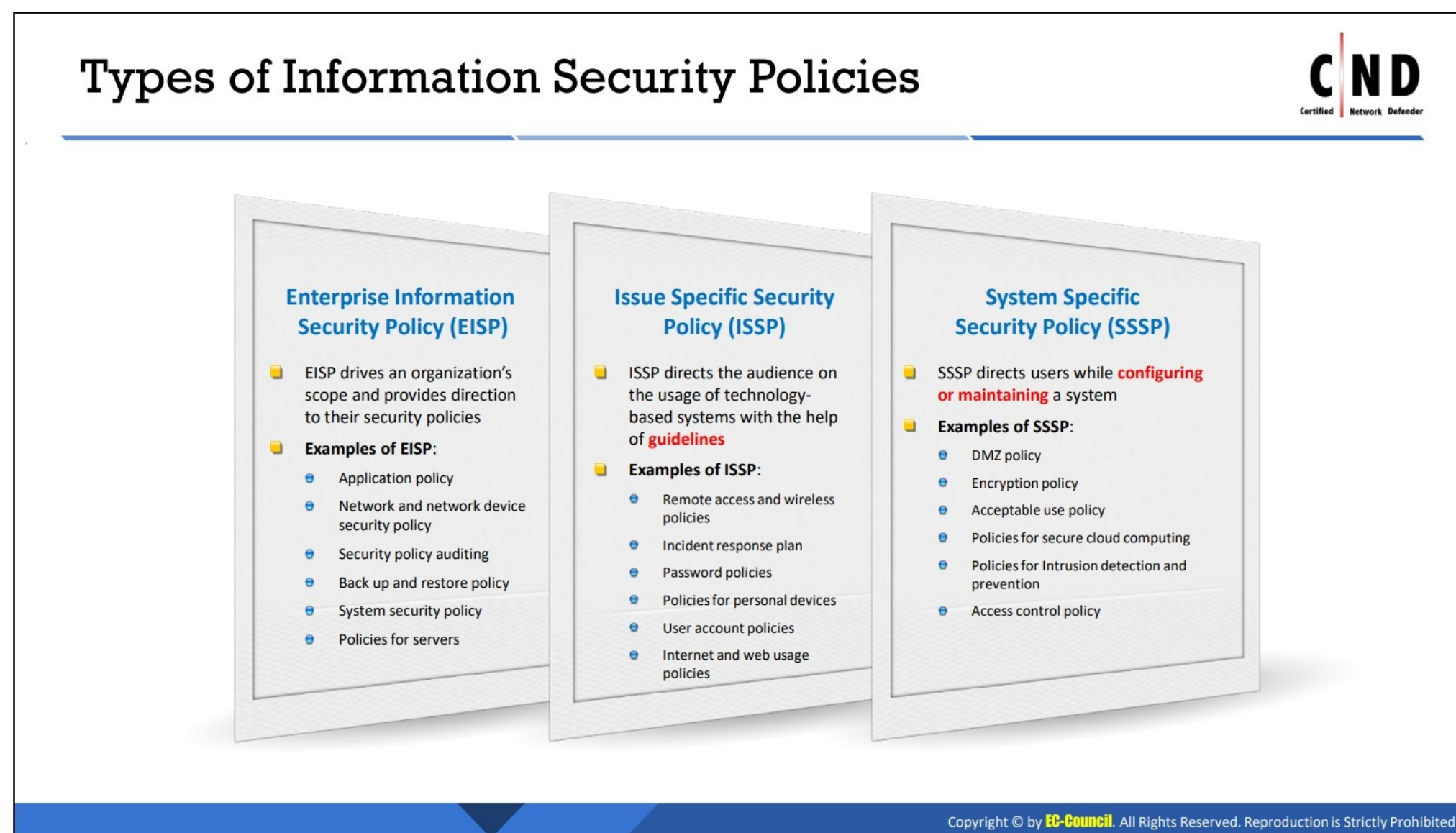
**Some of the measures to develop security policies are as follows:**

- Every company and client should identify its roles and responsibilities and its tasks should be described in detail. That is, the knowledge of the structure of an organization, responsibilities of individuals, tasks performed by all organization members, and who tackles the security policies is essential. It is important to ensure the policies address the problems, requirements, and objectives of an organization. The representation of each problem should be to the maximum extent. It should also include data security, legal issues, and human resources. The development and operations of an organization should be represented in the policies.
- The basic goals of the business are represented. Business knowledge is essential to improve security and build a good security policy. Consider an organization that needs extensive auditing, monitoring, and a recovery system that requires regular data backups. This may not be the case for the rest of the company. Therefore, the policies of an organization differ according to its requirements. Some policies may be cost effective, whereas others may be expensive. Thus, security policies are specific to each organization.
- The next step in developing policies is to identify the security principles that represent the company's security objectives. These goals are to be checked regularly and introduced into the development process whenever necessary. The aim of security policies is to describe the policies and principles of an organization with less technical details and in a simple way.
- The assets and data that need security are recognized and categorized. The valuable data are focal to all security policies. Data identified as more vulnerable to threats are secured. Cataloging the data and assets makes it easy for management to make decisions with respect to their value and use. This helps effectively control resources.
- As the data are collected and analyzed, it should also be classified. Data are critical to any policy. Data flow analysis is important to any and all issues related to data. For example, during a transaction, data flows through the browser, web, and other media such as telephone lines, servers, and firewalls. The data are stored in databases or on disks, tapes, or paper. If the flow of data is tracked through a media, where there are potential data vulnerabilities and data corruption locations can be detected, and control mechanisms can be implemented to prevent the vulnerabilities and corruption.



- The expected risks are identified. Developing a profile for possible threats helps enable a decision-making process for any threats within that area. The chance of risk associated with issues and the amount of capital needed to recover from that loss can be recognized. The nature of threats differs depending on different areas. For instance, the result of attacking financial transactions would be different from an attack on an art website.
- The services that guard the system are to be identified. Once the data resources and flow of data are identified, a risk profile is created. The security services that apply to such an area are then recognized and identified. The services for security include responsibilities, authentication, accessibility, recognizing, integrity, secrecy, and non-duplication. Knowledge of the security needs of a particular environment is essential for choosing the security policy to be employed over that area.





## Types of Information Security Policies

In an organization, policies are crucial for information security planning, design, and deployment. These policies provide measures to handle issues and the technologies that could help users accomplish their security goals. The policy also explains how the software or equipment functions in an organization. Information technology enterprises deploy security policies such as:

### Enterprise Information Security Policies

These policies support organizations by offering ideology, purpose, and methods to create a secure environment for enterprises. It establishes a method for development, implementation, and management of security programs. These policies also ensure the proposed information security framework requirements are met.

### Issue-Specific Security Policies

These policies address specific security issues in an organization. The scope and applicability of these security policies are completely dependent on the type of issue and the methods used by them. It specifies the necessary technologies along with preventive measures such as authorization of user access, privacy protection, and fair and responsible use of technologies.

### System-Specific Security Policies

The implementation of these policies focuses on the overall security of a particular system in an organization. An organization often develops and manages this type of policy, including the procedures and standards, for system maintenance. The technologies used by an organization should also be included in system-specific policies. It addresses the implementation and configuration of technology and user behavior.



| Internet Access Policies  |  | CND<br>Certified Network Defender  |   |
|---|--|--|---|
| Promiscuous Policy  | Permissive Policy  | Paranoid Policy  | Prudent Policy  |
| <ul style="list-style-type: none"> <li>No restrictions on Internet/remote access</li> <li>Nothing is blocked</li> </ul> | <ul style="list-style-type: none"> <li>Known dangerous services/attacks blocked</li> <li>Policy begins with no restrictions</li> <li>Known holes plugged; known dangers stopped</li> <li>Impossible to keep up with current exploits; administrators always play catch-up</li> </ul> | <ul style="list-style-type: none"> <li>Everything is forbidden</li> <li>No Internet connection, or severely limited Internet usage</li> <li>Users find ways around overly severe restrictions</li> </ul> | <ul style="list-style-type: none"> <li>Provides maximum security while allowing known, but necessary, dangers</li> <li>All services are blocked</li> <li>Safe/necessary services are enabled individually</li> <li>Nonessential services/procedures that cannot be made safe are not allowed</li> <li>Everything is logged</li> </ul> |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Internet Access Policies

Internet access policies define the restricted use of the Internet. It is important for employees to know which of their actions is restricted while accessing the Internet. The Internet access policy helps keep employees informed on acceptable browsing. An Internet policy includes guidelines for permissible use of the Internet, system security, network setup, and IT service.

Internet access policies broken down into the four categories below:

- Promiscuous Policy:** This policy does not impose any restrictions on the usage of system resources. For example, with a promiscuous Internet policy, there is no restriction on Internet access. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people travel or work at branch offices and need to access an organizational network, it also opens the computer to threats such as malware, viruses, and Trojans. Because of free Internet access, this malware can come in the form of attachments without user knowledge. Network defenders must be extremely alert while choosing this type of policy.
- Permissive Policy:** This policy is wide open, and only known dangerous services/attacks or behaviors are blocked. For example, in a permissive Internet policy, the majority of Internet traffic is accepted, except for several well-known and dangerous services/attacks. Because only known attacks and exploits are blocked, it is impossible for network defenders to monitor current exploits. They are always playing catch-up with new attacks and exploits.
- Paranoid Policy:** A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage. There is either no Internet



connection or severely limited Internet usage. Users often try to circumvent such severe restrictions.

4. **Prudent Policy:** A prudent policy starts with all services blocked. The Network defender enables safe and necessary services individually. This provides maximum security and logs all activity such as system and network activities.



## Acceptable Use Policy



- An **acceptable use policy** defines the proper use of an organization's information, electronic computing devices, system accounts, user accounts, and network resources

### Design Considerations:

- Should users **read and copy** files that are not their own, but are accessible?
- Should users modify files they have read and write access to, but do not own?
- Should users be permitted to use **.rhosts** files, even when the entries are acceptable?
- Should users be **allowed** to share accounts?
- Should users make **copies** of system configurations for personal use or provide them to other people?
- Should users be allowed to make **duplicates** of copyrighted software?

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Acceptable Use Policy

Acceptable use policies (AUPs) comprise rules decided by network and website owners. This type of policy defines the proper use of computing resources. It states the responsibilities of users to protect the information available in their accounts. The users must accept the policy restrictions while accessing a computer on the network or the Internet. An AUP covers principles, prohibitions, reviews, and penalties, while prohibiting the user from using the corporate resources for personal reasons.


An AUP is an integral part of information security policies. Generally, an organization asks its new members to sign an AUP before they are permitted to access the information systems. An AUP should cover all major aspects about permissible and forbidden activity in the IT infrastructure.

To ensure adherence to AUP, network defenders should conduct regular security audits.

The majority of AUPs describe the penalties of a policy breach. These penalties range from temporarily disabling the user's account to extreme measures such as legal actions.



## User Account Policy



The user account policy defines the creation process of **user accounts** and includes user rights and responsibilities

### Design Considerations

- Who has the authority to **approve** account requests?
- Who (employees, spouses, children, or company visitors) are permitted to use the computing resources?
- Can users have **multiple accounts** on a single system?
- Can users **share accounts**?
- What are the rights and responsibilities of the user?
- When should an account be **disabled and archived**?

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## User Account Policy

The user account policy is a document specifying the requirements for requesting and maintaining an account on an organization's network. It mentions the processes for creation, deletion, and operation of user accounts by defining the type of accounts created under a specific network.

The user account policy defines the process of account authorization, user responsibilities as well as Internet services for both internal and external users. It also defines the creation of a username and password, encryption standards, type of verifications in case the user forgets the password, and the devices used for accessing or linking to the account.

**Example Wording:** "Employees shall only request/receive accounts on systems they have a true business need to access. Employees may only have one official account per system and the account ID and login name must follow the established standards. Employees must read and sign the AUP prior to requesting an account."

Network defenders as well have responsibilities when implementing a user account policy. These include:

- Types of Accounts:** As per an organization's policy, administrators are asked to create two types of accounts in the network—administrator and standard. The administrator account is for the network administrators only. Standard accounts are for employees irrespective of the department in which they are working.
- Account Permissions:** Administrators are required to set the level of permissions to every employee in an organization. Although a team leader may not have access to administrator privileges, the level of permission will differ with the reporting member of this team.



Administrators should assign permissions according to employee designation. Permissions can also be set for a group. All human resource group members have a standard set of permissions, for example.

3. **Account Auto-Lock:** An administrator sets a length of time an account will automatically lock. This feature is present in mobile phones as well and prevents others from accessing the device without the log in code.

The user account policy should mention certain important characteristics, operations, and maintenance. The policy content should state the following:

- Who has the authority to approve account requests?
- Who is allowed to use the resources (e.g., employees or students only)?
- Are users allowed to share accounts or are they allowed to have multiple accounts on a single host?
- User's rights and responsibilities
- When the account should be disabled and archived
- How long can the account remain inactive before it is disabled?
- Password construction and aging rules



## Remote Access Policy



■ **Remote access policy** defines who can have remote access, access mediums, and remote access security controls

### Design Considerations

- Who is allowed **remote access**?
- What **specific methods** (such as cable modem/DSL or dial-up) does the company support?
- Are **dial-out modems** allowed on the internal network?
- Are there any **extra requirements** such as **mandatory anti-virus** and security software on the remote system?
- Can other family members of an employee use the **company network**?
- Do any restrictions exist on the data that can be **accessed remotely**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Remote Access Policy

The remote access policy document defines the acceptable guidelines for remote access to the network and resources. A remote employee should follow the policy when connecting to the internal network. The remote access policy is helpful to organizations with a geographically dispersed network. Implementing the remote access policy helps minimize potential damage that can occur from unauthorized external network traffic. Implementing remote access includes dial-in modems, frame relay, integrated services digital network, digital subscriber line, virtual private network (VPN), secure shell (SSH), and Wi-Fi.

Points to consider in the policy:

- **User Authentication:** Organizations should have a strict user authentication policy for remote users. An organization has the right to deny access to users with a weak password or user credentials. The policy should also state the action taken against employees if they share their remote credentials with others.
- **Information Encryption:** Employees working as a remote user should include encryption of their data while working on a shared infrastructure. This maintains the confidentiality and integrity of the data. An organization must educate remote users on the encryption policy to be followed.
- **Usage of Network and Network Devices:** The policy should restrict employees from reconfiguring their network devices. Employees should not perform any unauthorized activities on an organization's network and should not connect to any other third-party network.



- **Antivirus and Patches:** The systems used by remote users should meet an organization's requirement. Users should have an up-to-date antivirus installed on their system. They should proactively install updates for the antivirus and patches for the OS.
- **Data Access:** Administrators should assign privileges to the remote user according to the users' roles and responsibilities in an organization.

The network defender's responsibilities in enforcing remote access include:

1. Ensure remote system has an approved version of antivirus, firewall, and malware;
2. Enforce an authentication method for the remote virtual private network;
3. Enforce access control on the remote system when connected through remote access; and
4. List a set of devices which can be used for remote access.



## Information Protection Policy



■ **Information protection policy** defines guidelines for processing, storing, and transmitting sensitive information

### Design Considerations

- What are the information sensitivity levels?
- Who can access the sensitive information?
- How is the sensitive information stored and transmitted?
- What level of sensitive information can be printed on public printers?
- What is the process for removing sensitive information from storage media (paper shredding, scrubbing HDDs, or degaussing disks)?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Information Protection Policy

The information security policy is a document that guides employees to defend their data or physical devices from unauthorized access. The main aim of the policy ensures the information is not shared or modified by any external sources. An organization should define the level of sensitive information. Organizations should make it a practice to ask new employees to sign the information security policy.

Lack of an information security policy can lead to vulnerabilities in the network and system. With no information security policy in place, employees can knowingly or unknowingly share the data with external sources.

The information security policy should be drafted based on the following points:

- Create a list of authenticated users who can have access to sensitive information.
- The process and method of saving sensitive information should be outlined. This can include data that is either archived or encrypted.
- The policy should mention the location where the sensitive information is stored. The authorized users should be asked to save the information in this location. Saving the data at any other location can potentially cause data theft or exposure of information to other sources.

Implementation of information security assures the data will be protected throughout the functioning of an organization.



## Firewall Management Policy



■ **Firewall management policy** defines access, management, and monitoring of firewalls in the organization

### Design Considerations

- Who has **access** to the firewall systems?
- Who can receive requests to make changes to the **firewall configuration**?
- Who can **approve** requests to change the firewall configuration?
- Who can see the firewall configuration rules and access lists?
- How often should the firewall configuration be **reviewed**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Firewall Management Policy

A network defender's responsibilities when configuring firewall security policies include:

- **Service or Application Authentication:** Administrators should verify the applications or services before they choose the default "Allow" setting. A service that does not seem legitimate should not be added.
- **Setting up a Dashboard:** Administrators should set up a dashboard that will include all threats and vulnerabilities an organization's network can encounter. This creates a strong rule base.
- **Enable Anti-Spoofing Protection:** To ensure the source Internet protocol (IP) address is the same as the security gateway interface, it is important to enable anti-spoofing protection.
- **Telnet Access:** Telnet is insecure by nature. Administrators should not allow Telnet access for the secure functioning of the network.
- **FTP Connection:** File transfer protocol (FTP) connections should only be allowed if administrators have to upload error logs for the vendor. In other scenarios, it is advisable to prohibit FTP.
- **Avoid Direct Connection:** Administrators should avoid setting up a direct connection between an internal client and external service. If an organization needs a connection to be established, it can be done through proxy servers.



## Special Access Policy



- **Special Access Policy** defines the terms and conditions of granting special access to system resources

### Design Considerations:

- Who can **receive requests** for special access?
- Who can **approve requests** for special access?
- What are the **password rules** for special-access accounts?
- How often are **passwords changed**?
- What **reasons** or **situations** can lead to revocation of special access privileges?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Special Access Policy

Regulating the special access policy allows certain employees to access the data in the network. Before implementing a special access policy in the network, an administrator should consider the following items:

- **Authorized Users:** Special access to resources can only be given to privileged users. Usually these users are top management employees or administrators.
- **Approval:** Employees can be given privileged access only if it is authorized by management or the administrator.
- **Password Rules:** The policy should have a policy statement regarding password rules. This may include the strength of the password and the validity of the password.
- **Revoking Privileges:** Users provided with special privileges should be notified of the circumstances under which their privileges can be revoked.

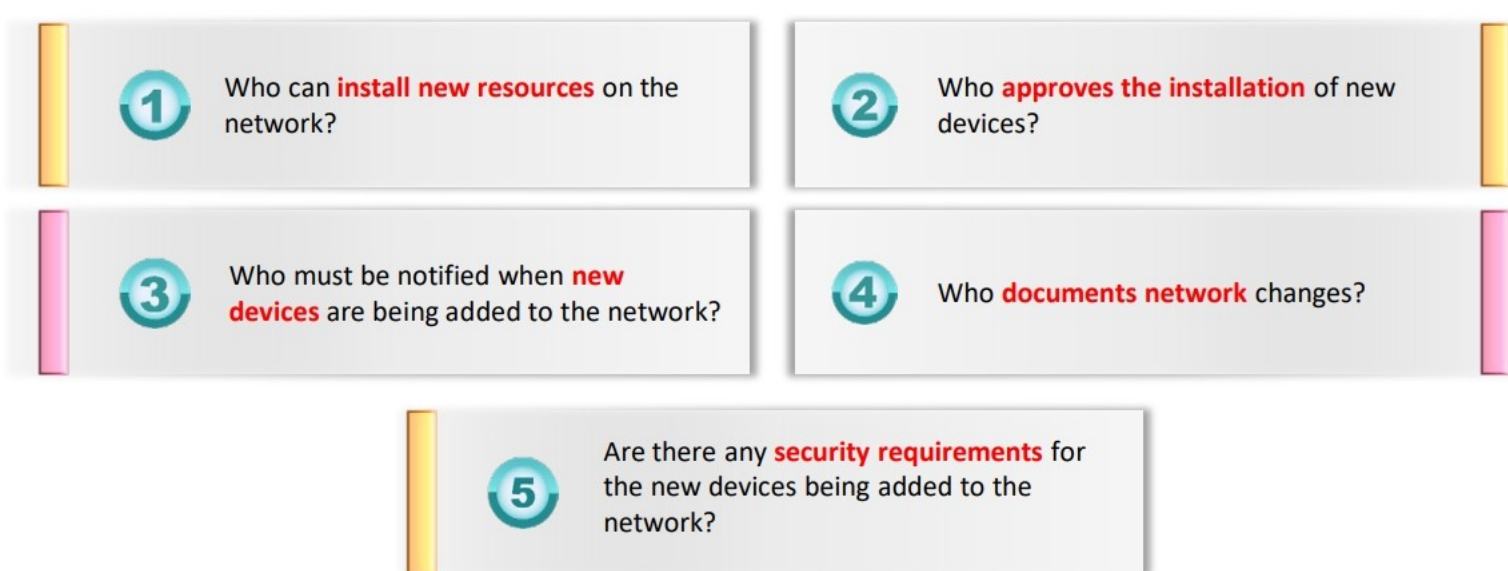


## Network Connection Policy



- Network connection policy defines the standards for establishing the **connection** for computers, servers, or other devices to the network

### Design Considerations:



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Connection Policy

A network connection policy is drafted to secure an organization's network. The network connection policy defines regulations to be followed and implemented on the systems, servers, and other electronic devices used in an organization. An effective network connection policy involves securing the devices from potential intrusion an organization can experience.

The following points should be included in the network connection policy:

- Connection of Devices:** The policy should include the normal rules for connecting their electronic devices, including their personal mobile phones. Employees should be restricted from making any changes in the network through their devices, as it may cause network fluctuations or loss of connectivity.
- Authenticating:** For a better security service, employees should be asked to authenticate their device every time it is connected to the network. Although it might be a frustrating task for some, the security of the network is the main priority.
- Employee Responsibility:** Every employee using his or her personal devices on an organization's network is responsible for his or her systems to meet the security standards. An organization will have full authority to deny the device that does not meet their security standards.



## Business Partner Policy



- Business partner policy defines the **agreements, guidelines, and responsibilities** for business partners to run business securely

### Design Considerations

|   |  |
|---|--|
| ✓ | Is it mandatory for a company to have a <b>written security policy</b> ?                       |
| ✓ | Should each company have a <b>firewall</b> or other <b>perimeter security device</b> ?         |
| ✓ | How will one <b>communicate</b> (VPN over the Internet or leased line)?                        |
| ✓ | How will access to the <b>partner's resources</b> be requested?                                |
| ✓ | Should <b>each partner</b> keep accurate accounts, books, and records related to the business? |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Business Partner Policy

Organizations working in partnership follow certain guidelines that are drafted under a business partner policy. It defines the guidelines partners are required to follow in order to run their business securely. There can be geographical and cultural differences between the two business partners, which requires care when drafting sensitive policies. Business partner policies should address the following questions:

- Need of Policy:** The business partner policy defines the rules and regulations of the respective organizations. Certain policies followed by employees in company A may not necessarily be followed in company B. Organizations should work out a third way for drafting the policy in order to not affect how both the companies function.
- Security:** Encouraging employees to follow common security rules is the biggest challenge when drafting a business partner policy. The policy should mention the common security boundaries for both partners and how it will be regulated if employees do not follow it.
- Resource Sharing:** Although both organizations are in a partnership, it does not mean the companies will have access to each other's data. The policy should state the amount of data that both parties can share and access. Data breaches by either partner will result in legal actions.
- Record Maintenance:** In a partnership, an organization should maintain a log for every transaction. This maintains a healthy partnership between each company.



## Email Security Policy



- An email security policy defines the **proper usage** of corporate email

### Design Considerations

- Define prohibited use
- Define personal use, if allowed
- Employees should know if their emails are reviewed and/or archived
- What types of emails should be kept and for how long
- When to encrypt emails
- Consequences of violating email security policy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Email Security Policy

Email security policies are developed to ensure the corporate email is used properly. A simple personal email from a corporate account can result in unintended information disclosure.

Implementation of an email security policy lets an organization achieve:

1. **Competitive Accomplishment:** Through an email security policy, organizations train their employees in email etiquette, including, but not limited to, drafting effective emails and learning about the reply in target duration. This helps an organization maintain its respective competition in the market.
2. **Employee Productivity:** Email security policies state what the normal use of corporate email is. This restricts employees from using emails for their personal use, thus increasing the overall productivity of an organization.
3. **Less Employer Liability:** Organizations should state the consequences, or actions, taken against the employee if the normal use policies are not followed. The liability of the employer is reduced as a result.

The following include the responsibilities of network defenders:

1. **Email Use and Limitations:** The policy should state the scenarios and domains wherein employees cannot use their corporate email addresses in general and specifically. The policy should also instruct employees not to open malicious attachments.
2. **Defining Extent of Personal Use:** The policy should set boundaries for employees when using corporate email for their personal use.



3. **Monitoring of Emails:** The policy should mention if an organization reviews all employee emails.
4. **Duration of Emails:** Employees should be notified about the duration for keeping email in their mailbox. Employees should be informed of the administrators' right to archive emails after a certain period of time.
5. **Encryption:** Employees should be aware of the encryption policy of an organization when sensitive information is being sent or received.
6. **Actions Against Compliances:** The policy should clearly state the action taken against an employee if he or she fails to follow the policy set by an organization.

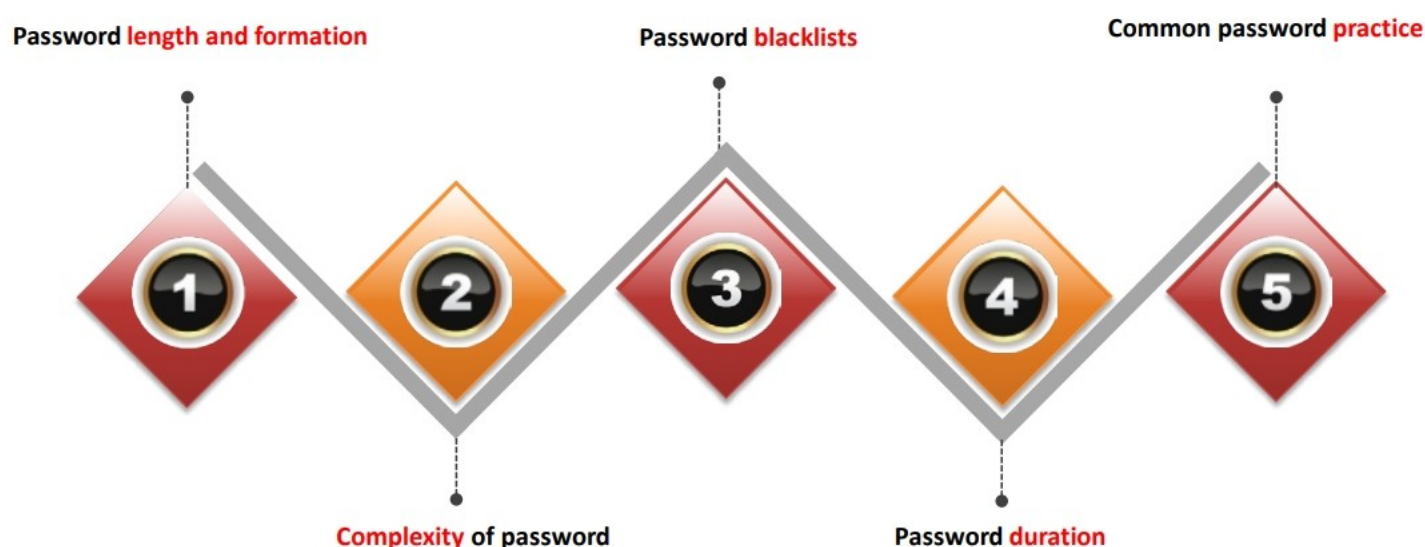


## Password Policy



■ **Password policy** provides guidelines for using strong passwords for an organization's resources

### Design Considerations



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Password Policy

A password policy is a set of rules to increase system security by encouraging users to employ strong passwords to access an organization's resources and to keep them secure. The purpose of the policy is to protect an organization's resources by creating robust protected passwords. The policy statement should include a standard practice for creating a robust password. For example, the password should

- Have a length between 8 and 14 characters;
- Include both uppercase and lowercase letters, numerical digits, and special characters;
- Special characters (@, %, \$, &, or ;);
- Be case sensitive, whereas username or login ID may not be; and
- Be unique when changing the old password. Thus, regarding password history, old passwords cannot be reused.
  - Maximum password age: 60 days
  - Minimum password age: No limit

Some of the components of a password policy include:

- **Password Length and Formation**

This policy includes the length of the password. The password length varies according to an organization. The formation of a password includes:

- One or more numerical digits;
- Special characters such as @, #, and \$;



- Use uppercase and lowercase letters;
- Avoid using personal information; and
- Use of company name in the password is prohibited.

■ **Password Duration**

This policy suggests users change their passwords regularly—usually every 90 or 180 days. Changing a memorized password is hard for the user, but it is necessary to avoid password stealing.

■ **Common Password Practices**

The password policy statement should include guidance or best practices on creating, storing, and managing passwords. For example, it should include guidelines such as

- Do not share your computer user account details.
- Do not keep a common password for all accounts.
- Do not share passwords.
- Never write the password anywhere, instead remember it.
- Employees should not communicate their password through email, phone, or instant messages even to the administrator.
- Do not leave the machine unattended. Always log off or lock the system when leaving the desk.
- Keep different passwords for the OS and frequently used applications.

The password policy should include a disclaimer that informs all users of the consequences of not following the guidelines stated in the password policy. The disclaimer should involve all employees, including top management. Disclaimers can include verbal or written warnings or termination.



## Physical Security Policy



■ **Physical security policy** defines guidelines to ensure that adequate physical security measures are in place

### Design Considerations

- Is the **building protection deficiency** reviewed regularly?
- Is there a process to **identify outsiders** such as visitors, contractors, and vendors before giving them access to the premises?
- Are there adequate **lighting systems** in place?
- Are each of the **entry points** properly blocked?
- Are the badges, locks, keys, and authentication controls audited regularly?
- Is **video surveillance** footage monitored regularly?
- Is a proper **inventory** of an organization's assets maintained regularly?

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Physical Security Policy

Physical security is the security provided in terms of physical assets, which can be damaged physically. In IT organizations, where large amounts of physical assets are handled, the assets are prone to damage during installations or a transfer of assets from offshore to local locations. Care must be taken in terms of how frequently the risks are being monitored and analyzed, and the training provided to the people handling or working with the physical assets must be monitored. Designing a physical security policy helps an organization maintain certain norms, which can be followed by employees, thus reducing the probability of loss.



## Information System Security Policy



- Information system security policy defines guidelines to **safeguard** an organization's information systems from malicious use

### Design Considerations:

- Are the information systems **protected** with anti-malware?
- Is the anti-malware **updated** regularly?
- Is the **OS** updated and patched regularly?
- Are they **secured** using strong password policies?
- Are they secured with strong **physical security policies**?

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Information System Security Policy

The information security policy helps maintain the integrity and confidentiality of the information system.

Information system security policy statements are often focused on:

1. Installation of antivirus
2. Regular updates of software
3. Applying a firewall
4. OS upgrades
5. Password policy
6. Physical security standards



## Bring Your Own Devices (BYOD) Policy



- A BYOD policy provides a set of guidelines to **maximize business benefits** and **minimize risks** while using an employee's personal device on an organization's network

### Design Considerations:

- What **personal devices** are allowed for use under BYOD ?
- Which **resources** can be accessed through BYOD devices?
- What features need to be **disabled** in BYOD devices?
- What are the **data storage considerations** for BYOD devices?
- What **security measures** are required for data and BYOD devices?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Bring Your Own Devices (BYOD) Policy

The existence of a Bring Your Own Device (BYOD) policy is important. The policy provides a set of guidelines to maximize business benefits and minimize risks while using employee personal devices on an organization's network.

Aspects of a BYOD policy:

1. **Permissible Devices:** The policy should state the names of the devices an employee is allowed to use. The list of devices may differ based on the designation of each employee in an organization.
2. **Permissible Resources:** The policy should clearly state the resources an employee can use while using his or her own device. The policy should mention the actions taken if an employee does not adhere to these policies.
3. **Disabled Services:** Before an employee connects their device to the corporate network, administrators should verify the services and applications running on the device. If certain services or applications are a source of vulnerabilities, administrators should disable those services immediately.
4. **Data Storage:** It is necessary to document the location of data storage for BYOD. Administrators should provide a separate location for data on employee devices. Storing the data in existing drives can be a threat to the data. Administrators must provide a separate drive to employees.
5. **Security Measures for Data and BYOD Device:** Employees should be made aware of threats and vulnerabilities that may arise when they use their devices in the corporate network. It



is the responsibility of the administrator to monitor these devices along with all corporate devices.

While BYOD is emerging as a new trend in organizations, it is the responsibility of the administrator to enforce the BYOD policy. A few administrator responsibilities associated with a BYOD policy are:

1. **List of Devices:** Administrators can prepare a list of devices and software in the BYOD policy document—for example,
  - Smart phones (with model number)
  - Laptops (with model number)
  - OS (with version)
  - Any other process specific software or app
2. **Resources to be Accessed:** Depending on the designation of the employee, administrators can allow the following resources on BYOD:
  - Email
  - Contact
  - Calendar
  - Process specific documents
3. **Disable Use of the Following on BYOD devices:**
  - Storage or transmission of illicit materials
  - Using another company's proprietary information
  - Harassing
  - Engaging in other business activities
4. **Store Data on BYOD Devices with Proper Security Measures using:**
  - The device
  - Organization server
  - Cloud
5. **To Secure Data on BYOD Devices, Follow these Steps:**
  - Password (BYOD device also) and encryption policies
  - Monitor data transferred



## Software/Application Security Policy



- Application security policy mandates proper measures that **enhance the security** of **in-house** and **purchased** applications

| Design Considerations                  |                             |   |
|--|-----------------------------|---|
| Configuration Management               | Authentication              | Error Handling and Exception Management |
| Data Protection in Storage and Transit | User and Session Management | Logging and Auditing                    |
| Authorization                          | Data Validation             | Encryption                              |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Software/Application Security Policy

Application security involves securing the inbuilt and purchased applications running on the system. The security policy covers the application throughout its complete life cycle. The threat to an application is caused by software tampering, parameter manipulation, authorization, or cryptography.

Drafting the guidelines for application security mandates the proper functioning of the application, further enhancing how the system works.

The key factors in documenting a software/application security policy are:

1. Data validation
2. Session Management
3. Authentication
4. Authorization
5. Encryption

A network defender's role in enforcing application policies is:

1. **Criteria for Data Validation:** It is required to set measures to validate data flowing in and out of the application.
2. **Authentication Process:** Network defenders should set up an authentication policy for all systems. If a user is attempting to install a third-party application, the system will prompt for an administrator password. This will restrict users from installing such applications without administrator rights.



3. **Authorization Standards:** Network defenders should authorize application use for only those who need it. The authorization can also be limited to certain parts of the application's data.
4. **Encryption Policy:** Network defenders can encrypt the sensitive application data, preventing users from gaining access to it.
5. **Monitoring:** Every employee application session should be monitored.



## Data Backup Policy



- The backup policy helps an organization **recover and safeguard** information in the event of a security incident/network failure

### Design Considerations:

|   |  |
|---|--|
| ✓ | Location of data backup  |
| ✓ | Name and contact of authorized personnel who can <b>access</b> backups |
| ✓ | Backup schedule  |
| ✓ | Type of backup method used   |
| ✓ | <b>Hardware</b> and <b>software</b> requirements for taking backups    |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Data Backup Policy

Creating a backup policy is one of the most important things you can do for your data security plan. Optimized backup policies and procedures will save your organization time and money. One important reason for this policy is to bring the backup and recovery process in line with actual requirements. It will also ensure a smooth recovery process in the event of a hard drive failure, virus attack, or natural disaster.

Backup policies and procedures vary according to the needs of an organization and industry. There are certain elements of a data backup and restore process that every company should identify:

- **Determining What Files Should Be Backed Up:**

Before implementing a backup policy on a system, network defender should identify the important files for business activity. Data that help run the business should be backed up. Data that include financial, tax, or personal employee information are important and should be backed up.

- **Determine Who Can Access Backups:**

Administrators should assign privileges to access backups to only those employees who work on the data. It is important to keep track of the backup data. Keep the backup logs updated regularly.



- **Determine How Often to Backup:**

An organization backup policy should define the backup schedule employees must use. Informing employees beforehand helps them prioritize their data for this requirement. The schedule should be created by considering the business of an organization and the criticality of the data on the machines. It is not necessary to run a backup on all devices simultaneously. Certain files or databases have to be backed at a different time. The backup policy should also mention the time the backups should run. Usually an organization prefers to perform backups after business hours. Based on the backup policy, the backup process can be initiated by administrators.

- **What Type of Backup is required?**

While drafting the backup policies and procedures, network defender should also determine the type of backup required. The type of backup depends on an organization's needs. The three basic types of backup include:

- **Full Backups:** This includes a backup of all data. It is the simplest form of backup, but a highly time-consuming process.
- **Incremental Backups:** Here, the backup is created only when the data are changed since the last full backup. It is a less time-consuming process.
- **Differential Backups:** It backs up all selected files that are new and changed since the last full backup.

- **Where to Back Up Data:**

The backup policy should mention the location of the backed-up data and where they will be stored. Administrators can store the data on a physical external device, cloud, or both.

It is important to test and evaluate all backup policies.



## Confidential Data Policy



- Confidential data policy defines **guidelines** for identifying an organization's confidential data and procedures to handle them

### Design Considerations:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>Treatment of confidential data including data storage, access, transmission, sharing, disposal, handling, and disclosure</li><li>Use of confidential data</li></ul> | <ul style="list-style-type: none"><li>Security controls for confidential data</li><li>Emergency access to the data</li></ul> |
|---|--|

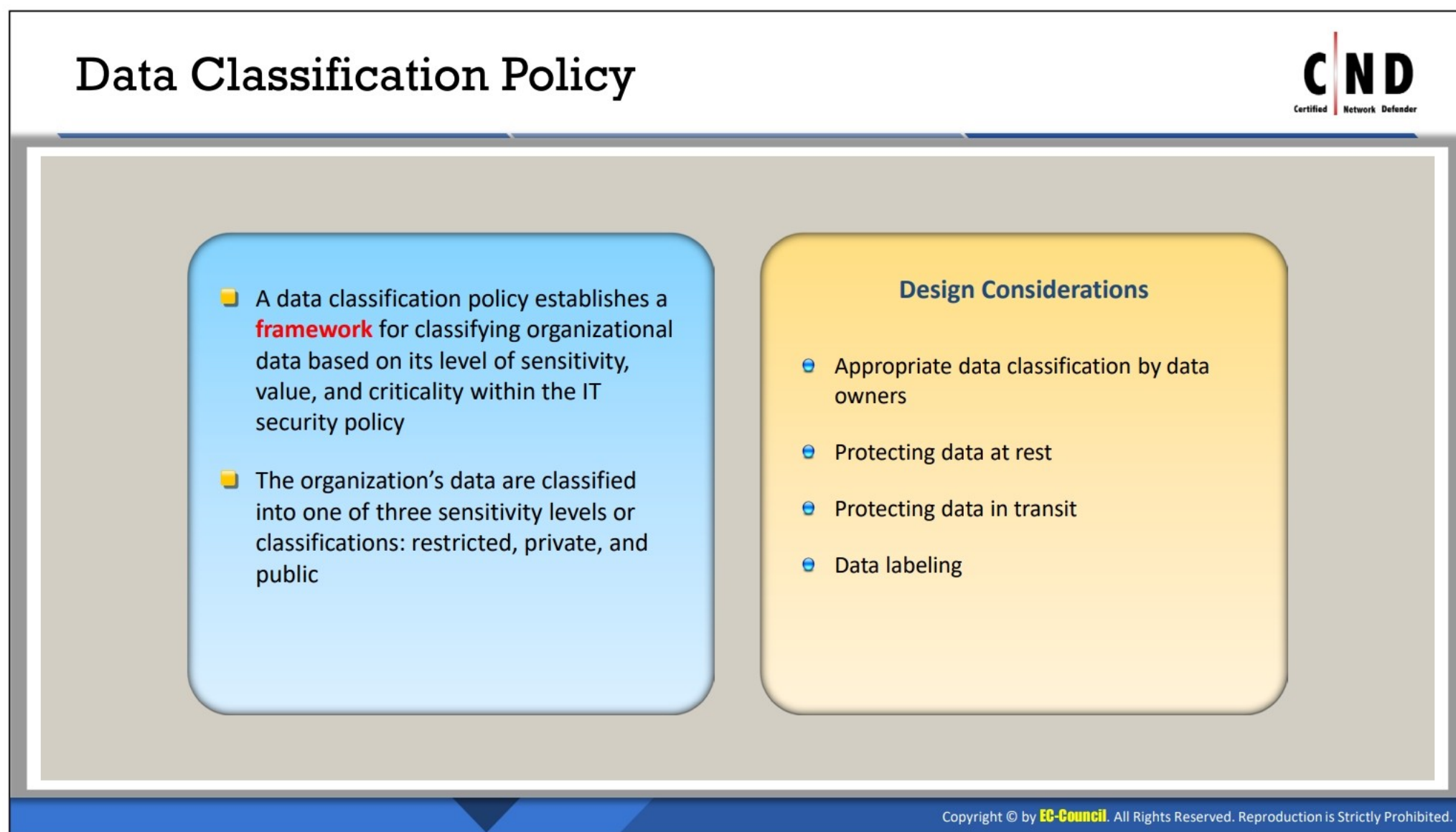
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Confidential Data Policy

A confidential data policy is a set of information that requires high levels of protection. It may consist of salary details, product details, and organization structure details, among other information. It is the responsibility of network defenders to ensure confidential data are secured from non-authorized access.

Drafting of a confidential data policy will help an organization protect information that is important to the existence of the business. The presence of a confidential data policy ensures users maintain the integrity and confidentiality of the business, which will further help overall business growth.





## Data Classification Policy


The data classification policy document aims to classify sensitive data and secure it as per its class. The implementation of a data classification policy helps an organization maintain and secure its data and resources. The classification of data and prioritizing its risk level depends on an organization. It can classify its data according to the user-requirement, security requirement, or managerial requirement. The prioritization of the risk level can be restricted, confidential, or public. The data classification policy should also include a list of users with information access rights.

Points to consider when developing a data classification policy:

- Employees should avoid distribution of any restricted or confidential data internally and externally.
- Authorized employees dealing with confidential data should send such data only in an encrypted format through email.
- Administrators should have a secure backup of the data and monitor the backups regularly. The backups should have strong user credentials.
- After receiving the confidential data, an employee should scan the device or the file to avoid any malicious activity.
- If the authorized employee finds confidential data that is public, they should immediately delete the data (if possible).
- The document should mention the action taken against employees if they do not adhere to the policy.
- An organization should perform regular audits to ensure authorized employees are following the required measures.



## Internet Usage Policy



Internet usage policy governs the way the organization's **Internet connection** is used by every device on the network

### Design Considerations

- Internet usage limit for official as well as personal use
- Time frame for personal use
- Method adoption for web usage monitoring
- Levels of privacy for employees
- Restricted content

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Internet Usage Policy


An Internet usage policy informs employees about the rules to be followed while accessing the corporate Internet network. The implementation of such policies helps an organization maintain a secure network. Using an Internet policy keeps the systems secure and helps the user understand the types of risks a network can encounter. The policy should make employees aware that browsing prohibited sites or downloading files from unreliable sources can attract disciplinary action.

A small negligence from an employee or administrator end can lead to a major vulnerability in the network. The Internet usage policy must be accepted by all employees and it must be signed by them to acknowledge their understanding of the policy. Network defenders should (in consultation with top management) ensure the following:

1. **Limited Usage:** Employees should be aware that corporate Internet is used for official use only. Employees should refrain from using the Internet for their personal use such as for downloading movies.
2. **Setting a Timeframe for Personal Use:** If an organization plans to allow employees to use the Internet for personal purposes, it can set a timeframe for the use.
3. **Method for Monitoring Web Use:** Network defenders should set monitoring standards to keep track of user activities on the Internet. These monitoring standards should follow the policies drafted in the document.
4. **Discuss and Decide What Content Should Never be Allowed:** Network defender should discuss with top management and decide on a list of sites that should be denied or can be added to a list of non-trusted sites.




## Server Policy




- Server policy establishes a **standard** for the base configuration of an organization's server
- An effective server policy restricts unauthorized access to an organization's data and technology


### Design Considerations



**Location** and **protection** consideration for servers



**Configuration** of servers



**Monitoring** of servers

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Server Policy

A server policy is an internal organizational policy that defines the handling of server issues. It includes the details of installation, configuration, and services required for the server. The policy document authorizes only its target audience—network/system administrators—to have access to read it. The policy states administrators have the rights to perform deletions or modifications in a server. Following the policy, if any changes are made, network defenders are required to inform management or the users that will be affected by the changes.

The policy should cover the points that can help administrators rebuild the network or servers during a time of a disaster or calamity. With many troubleshooters available, the document reduces the troubleshooting time of the administrators.

For every server on a secure network, there are lists of items that must be documented and reviewed regularly to keep a private network secure. The server list of information must be updated as new servers are added to the network and updated regularly:

- Server name
- Server location
- Server function or purpose
- System hardware components, including the make and model of each part in the system
- List of all software running on the server, including the OS, programs, and services
- Configuration information about the server including:
  - Event log settings
  - Comprehensive list of services that are running



- Configuration of any security lockdown tool or setting
- Account settings

The responsibilities in enforcing general server policies include:

1. **User Restriction:** Servers are the foundation of a functioning organization; administrators should not allow server access privileges to anyone in an organization except those who have been given permission by them.
2. **Configuration Compliance:** At times, administrators may have to make changes to the configuration settings of a server. Such exceptions should be permissible. The changes should be monitored.
3. **Server Registration:** Server registration should follow the corporate enterprise management system.
4. **Updating the Corporate Enterprise Management System:** It is the responsibility of the administrator to update the corporate enterprise management system regularly; this keeps the network and machines running smoothly.
5. **Parallelism in Modifications:** Administrators should ensure that the configuration changes made on the server comply with the change management procedure.



## Wireless Network Policy



■ A wireless network policy states the **rule and regulations** for accessing an organization's wireless network resources

### Design Consideration

- Defining an **access point** for a WLAN
- **Placement** of an access point
- Technologies used for **wireless connectivity**
- Procedure **for integration** of a new system into the wireless environment
- Procedure for **monitoring** the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Network Policy

The wireless network policy is designed to protect organizational resources against intrusion from a wireless network. It applies to all wireless devices in use by an organization or those that connect through a wireless device to any organization network.

A network defender's responsibilities in enforcing wireless policies are:

1. **Access Point:** Administrator should provide a clear description of new established access points in the network. All access points must be registered and approved. They should be connected to an organizational network.
2. **Configuration:** Administrators should configure the service set identifier on all wireless devices in order to ensure they do not reveal any information about an organization.
3. **Permissible Devices:** The policy document should mention the type of devices that can be used to connect to the corporate wireless network. Only those devices that are approved by management should be connected to the network.
4. **Permissible Technologies:** Administrators should define what technologies can be accessed through the wireless network.



## User Access Control Policy



■ **User access control policy** gives an organization the ability to control, restrict, monitor, and protect corporate resource availability, integrity, and confidentiality

### Design Considerations

- 1** Who can access (people, process, or machines)?
- 2** What system resources can be accessed?
- 3** What files can be read?
- 4** What programs can be executed?
- 5** How to share data with other entities?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## User Access Control Policy

The access control policy provides a way to control the interaction between users, systems, and resources. An access control policy helps an organization control, constrain, and defend the resource availability of an organization.

The access control policy should define:

- Who can access (people, process, and machines)?
- What system resources can be accessed?
- What files can be read?
- What programs can be executed?
- How to share data with other entities?

The policy should address the typical access control practices such as:

- Undefined user or unknown account logins should be prohibited.
- Powerful accounts such as an administrator account must be monitored continuously.
- Lock access to accounts after crossing a limited number of unsuccessful login attempts.
- Remove unused accounts.
- Administer strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unrequired system features and unused ports.
- Restrict global access rules.



## Switch Security Policy



Switch security policy describes a required **minimal security** configuration for the switches in the network

### Design Considerations

- 1 Is the switch data **monitored** regularly?
- 2 Are **unnecessary** services and applications blocked?
- 3 Are all stored **passwords** and **sensitive data** encrypted ?
- 4 Is the switch located in a **restricted** area?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Switch Security Policy

The switch security policy should be based on the following aspects:

1. **Monitor Regularly:** The data in the switch should be monitored regularly for smooth network function.
2. **Services and Applications:** It is not necessary to block all services and applications of the switch device. Block the items that are not required and those that are known to be vulnerable.
3. **Encryption:** Administrators should encrypt all stored data and passwords.
4. **Restricted Area:** Physical storage of the switch should be in a restricted area.
5. **Configuring a L3 switch:** If an organization is using an L3 switch, it should be configured identical to the router policy.

A network administrator's switch policy responsibilities include:

1. **Enable Password:** You should always maintain the "enable password" option. This helps keep the switch in a secure encrypted form.
2. **Timeout Periods:** Setting session timeout periods on the switch will not keep the switch busy, until the time a packet does not reach its destination.
3. **Privileges:** Privileges should be enabled on all levels of the switch.
4. **SSH:** Administrators should avoid using Telnet as a communication channel. SSH has proven to be more secure than Telnet. Use SSH with a strong password.



5. **Port Security:** Port security limits the MAC-based access. Enhancing the security of the switch. Limit MAC-based access by implementing port security.
6. **Disable Ports:** Ports that are not used by the switch should be disabled. Administrators can assign these ports to an unused virtual LAN (VLAN) number.
7. **Configure Trunk ports:** Trunk ports carry traffic for all VLANs. A VLAN number that is not in use should handle the configuration of trunk ports.
8. **VLAN Restrictions:** Use a static VLAN and limit the number of VLANs that can be transported over the trunk.
9. **AAA Framework:** The Authentication, Authorization, and Accounting framework includes the access of computer resources, implementation of policies, and information about services. AAA provides local and remote access to the switch.
10. **Switch Logs:** Set the switch to log data, and then transfer it to a secure log host
11. **Disable the Following if Not in Use:**
  - Cisco discovery protocol
  - Dynamic trunking
  - Scripting environments like Tcl shell
12. **Encryption:** Enable Password-encryption and network time protocol (NTP) configuration following the corporate standard.
13. **ACL:** ACL's to be configured following an organization hierarchy and requirements.
14. **Disable VTP:** If you are unable to disable VLAN trunking protocol (VTP), then set VTP to management domain, password, and pruning. After performing the above steps set VTP to transparent mode.



## Intrusion Detection and Prevention (IDS/IPS) Policy



- The IDS and IPS policy facilitates **detection** and **prevention** of intrusion into an organization's network

### Design Considerations:

- **Deployment** of a standard IDS system
- **Monitor** log files of an IDS continuously
- Regularly **update** the intruder's definition in the IDS logic for all evolving threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Intrusion Detection and Prevention (IDS/IPS) Policy

The policy of an IDS/IPS should facilitate the detection and prevention of intrusions in an organization's network.

The IDS and IPS policy design should include the following components:

1. **Deployment of Standard IDS System:** For a successful working IPS, administrators should deploy a standard IDS system across the network. The successful deployment of an IDS ensures threats will be detected and prevented using the IPS standards.
2. **Monitor Log Files of an IDS Continuously:** For monitoring the activity on a network continuously, administrators should actively audit and monitor the IDS.
3. **Regular Update:** It is important for administrators to perform regular updates for the intruder's definitions in IDS logic as per evolving threats.
4. **Need of IPS:** It is advisable to deploy an IPS for large organizations. Deployment and implementation of an IPS ensures threats are detected using the same software as an IDS and prevents the networking using these prevention tools.



## Encryption Policy



- The encryption policy defines an **acceptable use and management** of encryption methods, techniques, and tools throughout an enterprise
- The policy is **applicable to all enterprise network resources**, users (staff or stakeholders, among others), internal network (LAN, Wi-Fi) and remote (WAN) connections
- **Design considerations:** It should define encryption standards that need to be used in an enterprise wired/wireless data communication, servers, desktops, laptops, smart phones, removable storage devices, USB memory sticks, VPN, and Wi-Fi.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Encryption Policy

The encryption policy sets universal standards for organizations to facilitate data protection. It involves establishing business and technical strategies for accomplishing data security. The encryption policy determines the need for data encryption and the process of encrypting it.

The encryption policy is applicable to large and small organizations. It is applicable, but not limited, to employees, partners, vendors, and stakeholders. It is necessary to understand every aspect of the policy to implement it further across an organization. The encryption policy defines the standards that can be deployed and implemented in electronic devices such as servers, laptops, smart phones, and removable devices.

Encryption policies should be designed based on the following points:

1. **Encryption Algorithm:** Once the encryption policy is approved by management, administrators should research the encryption algorithm that can be implemented in the infrastructure.
2. **Changes in Hash Functions:** Change the hash functions of the selected algorithm, if required.
3. **Key Type:** As per an organization's requirement, administrators can use a symmetric or asymmetric key for encrypting the data.
4. **Verified Certificates:** Before installing any certificate on the server, administrators should verify the authenticity of the certificates and its provider.
5. **Secure Sockets Layer and Transport Layer Security Certificates:** Ensure the servers are using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates, and that both of these have a trusted certificate.



## Router Policy



Router policy describes a required **minimal security** configuration for all routers in the network

### Design Considerations:

- User authentication
- Access rules
- Placement
- Password management
- Services required/disallowed/blocked

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Router Policy

An organization should establish router policies for the smooth functioning of the IT infrastructure.

The router policies should be designed based on the following points:

- No Local User Account:** Routers must use the Terminal Access Controller Access Control System (TACACS) user authentication. Administrators should not create local user accounts on the router.
- Encryption:** The security of the router can be set using the “enable secret password” on the router in a secure encrypted form.
- Corporate Management System:** All routers should be included in the corporate enterprise management system with a designated point of contact.
- Do Not Touch:** Administrators should place warnings such as “Do not touch” on the routers to avoid any mishandling by employees.
- Maintain Standards:** Routers should comply with the standards outlined in the Router IOS Template.
- Non-usage of SNMP:** Administrators should use standardized corporate simple network management protocol (SNMP) strings. They should avoid using public and private SNMP community strings.
- Login Information:** Administrators should ensure every router saves system logging information to a local RAM buffer. The information should also be stored on “syslog” server.



8. **Configuration of VTY:** Virtual terminal (VTY) should be configured to accept connections for the required set of protocols only.
9. **Administrators should Consider Blocking the Following Services:**
  - Incoming packets with an invalid source address
  - Incoming packets with spoofed source addresses (i.e., company names)
  - Transmission control protocol and user datagram protocol small services
  - Source routing
  - Web services running on the router
  - IP directed broadcasts
  - Cisco discovery protocol on all third-party interfaces



## Policy Implementation Checklist



After the **security policy** has been created, the most difficult part of the process is deploying it throughout the **organization**

- 1 Make sure the security policy is **approved** by senior management
- 2 Make sure the security policy is officially **adopted** as a company policy
- 3 **Review** each policy and decide how it can be enforced within an organization
- 4 Ensure that **appropriate** tools and techniques are in place to conform to the policy
- 5 **Develop** a policy change plan for both the network and the policy itself
- 6 **Coordinate** with other departments to develop procedures based on the policies
- 7 **Provide** basic information security awareness training to employees

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Policy Implementation Checklist

Implementation of the security policy occurs after the policy is built, revised, and updated. A proper model and outline of the policies must be created. Suggestions from stakeholders must be included to directly correlate it with the interests of an organization. After its completion, the final version must be made available to all staff members for familiarization. It must be readily available at any time needed. It must be placed on the internal network and intranet. Proper training of the policies must be given to employees for their prompt understanding, and suggestions must always be taken into consideration. For effective implementation, job rotation should ensure different employees handle the data, so they may identify any limitations in the security policy. Company data have a critical nature. They must not be sent to everyone and must not be made public; hence, proper care is expected when handling or storing data. There must be a proper security awareness program as well as cooperation and coordination among employees. Once the security policy is designed and developed, the next step in the process is deployment.

#### Guidelines for Successfully Implementing the Policy:

- Ensure the security policy is backed by an organization's senior management team and is officially adopted as company policy.
- Peruse each policy and determine how it will be applied within an organization.
- Ensure the correct tools are available to conform to the policy.
- Create a plan to make any necessary changes to either the network or the policy.
- Work with the necessary departments within your company (e.g., legal, IT, and human resources) to establish procedures to support your policies.



- Provide basic information security awareness training to everyone through a basic Security Awareness Program.
- Make the security policy available to all employees with access to the information assets the policy governs.
- The Information Security Officer or IT Security Program Manager are responsible for implementing and managing the security policy.
- Ensure an organization is well equipped with the technology and tools needed to manage the security policy properly.
- Ensure visitors are provided the AUP (Acceptable User Policy) in the event they are allowed to use the company's network.





#### LO#04: Conduct security awareness training

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### LO#04: Conduct Security Awareness Training

Employee and user training plays an important part in the governance of the overall security of an organization. An untrained employee or user can pose a considerable risk to an organization. Hence, it is important to make them aware about security policies, and conduct other awareness training programs to maintain organization security. This section explains the importance of conducting security awareness trainings and keys aspects to be covered in different types of training.



## Employee Awareness and Training



- Employees are one of the **primary asset** of organization and can be part of an organization's attack surface
- An organization need to provide formal security awareness training for its employees when they join and periodically thereafter, so employees
  - Know how to defend themselves and the organization against threats
  - Follow security policies and procedures for working with IT
  - Know whom to contact if they discover a security threat
  - Can identify the nature of the data based on data classification
  - Protect physical and informational assets of that organization
- Moreover, organization should provide security awareness training to employees to **meet regulatory requirements**, if they want to comply with certain regulatory framework

### ■ Different methods to train employees are:

- Classroom style training
- Online training
- Round table discussions
- Security awareness website
- Providing hints
- Making short films
- Conducting seminars

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Employee Awareness and Training

Employees are one of the primary assets of an organization and can be part of an organization's attack surface. The actions of an employee—such as negligence, errors, susceptibility to social engineering, or clicking spam links—can lead to an attack. An employee awareness training initiated during orientation and periodically thereafter can enhance protection. The training is typically related to the knowledge and attitudes of employees tasked with the security of physical and informational assets.

- Expertise to defend themselves and an organization against threats;
- Follow security policies and procedures for working with information technology;
- Know whom to contact if they discover a security threat;
- Should be able to identify the nature of data based on data classification;
- Protect the physical and informational assets of an organization when the employees come into contact with them—for example, contacting with secrets, privacy concerns, and classified information;
- Know how to handle critical information such as review of employee nondisclosure agreements;
- Know the proper methods for protecting critical information on systems with password policy and the use of two-factor authentication;
- Know the consequences of failing to secure information, which may result in employment loss; and



- An organization should provide security awareness training to employees to meet regulatory requirements if they want to comply with a certain regulatory framework.

The different methods to train employees include:

- Classroom style training
- Online training
- Round table discussions
- Security awareness website
- Providing hints
- Making short films
- Conducting seminars
- Simulation employee training
- Hands-on training
- Lectures
- Coaching/mentoring
- Case studies
- Management specific activities
- Group discussions and activities



## Employee Awareness and Training: Security Policy



- Security policy training teaches employees how to **perform** their duties and to comply with the security policy
- Organizations should train new employees before granting them access to the network or provide limited access until the completion of their **training**

### Advantages:

- Effective **implementation** of a security policy
- Policies are followed and not just **enforced**
- Creates **awareness** on compliance issues
- Helps an organization **enhance** its network security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Employee Awareness and Training: Security Policy

Security policy training and procedures are required to ensure security and effective network management.

- The security policy training program helps employees appropriately recognize and respond to security threats in real time. The training teaches employees understand the importance of data on their devices or systems. Employees adapt themselves to secure computing habits.
- The security policy training makes employees aware of new updates on probable vulnerabilities that can occur if they do not follow the policies.
- Security policy training and awareness helps minimize security breaches in an organization. Early identification of a breach decreases the cost to an organization.
- Security policy awareness among users helps notify them about new security policies through published policy documentation and descriptive security documentation for users, for example.
- Employees following the security policy reduce their possibility of being subject to potential fines or legal actions.
- An effective training program will help employees monitor their computing behavior and inform their security concerns to management. The training will enhance the overall compliance with the company's security policies and procedures.



## Employee Awareness and Training: Physical Security



- Proper training should be given to **educate employees** on physical security
- Training increases the knowledge and awareness about physical security
- Training should educate employees about how to:
  - Minimize breaches
  - Identify the elements that are more prone to hardware theft
  - Assess the risks handling sensitive data
  - Ensure physical security at the workplace

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Employee Awareness and Training: Physical Security

Well-trained and skilled personnel can minimize the risk of a physical security threat to a great extent. An organization should provide proper physical security awareness training to all its employees. The training or awareness program should

- Provide methods to reduce attacks;
- Examine all devices and the chances of a data attack;
- Teach the risks of carrying sensitive information;
- Teach the importance of having security personnel;
- Inform employees about whom should report to about suspicious activities;
- Teach what to do when employees leave systems and workplaces unattended; and
- Teach the disposal procedures for disposing critical paper documents and storage media.



## Employee Awareness and Training: Social Engineering



- Train employee on possible social engineering techniques and how to **combat** these techniques

| Areas of Risk | Attack Techniques              | Train employee/Help Desk on:   |
|---------------|--------------------------------|--|
| Phone         | Impersonation                  | <ul style="list-style-type: none"><li>Not providing any confidential information, if this has occurred</li></ul>   |
| Dumpsters     | Dumpster Diving                | <ul style="list-style-type: none"><li>Not throwing sensitive documents in the trash</li><li>Shredding document before putting into the trash</li><li>Erasing magnetic data before putting into the trash</li></ul> |
| Email         | Phishing, malicious attachment | <ul style="list-style-type: none"><li>Differentiating between legitimate email and a targeted phishing email</li><li>Not downloading malicious attachment</li></ul>  |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Employee Awareness and Training: Social Engineering


A simple social engineering awareness training can be const-effective. It is useful in reminding employees about an organization's policies, which can ultimate help employees recognize and prevent social engineering attacks. Employees must be trained on possible social engineering techniques and how to combat social engineering techniques.

Some of the social engineering techniques the employees should be aware of include:

- Physical social engineering (tail-gaiting, piggy-backing);
- Changing passwords (attacker poses as an authority and asks to change the username and password);
- Name-drop (using the higher authority's name to gain access to something);
- Relaxing conversation (trying to build up a rapport with the employee); and
- New hire (attacker poses as a new employee to take a tour around the office).



## Employee Training and Awareness: Data Classification



Organization should train employees on how to tell if information is confidential


| Areas of Risk | Attack Techniques              | Train employee/Help Desk on  |
|---------------|--------------------------------|--|
| Office        | Stealing sensitive information | How to classify and mark document-based classification levels and keep sensitive document in secured place |

**Typical Information classification levels:**

- Top Secret (TS)
- Secret
- Confidential
- Restricted
- Official
- Unclassified
- Clearance
- Compartmented information

Security labels are used to mark the **security level requirements** for the information assets and controls access to it

Organizations use security labels to manage access clearance to their information assets



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

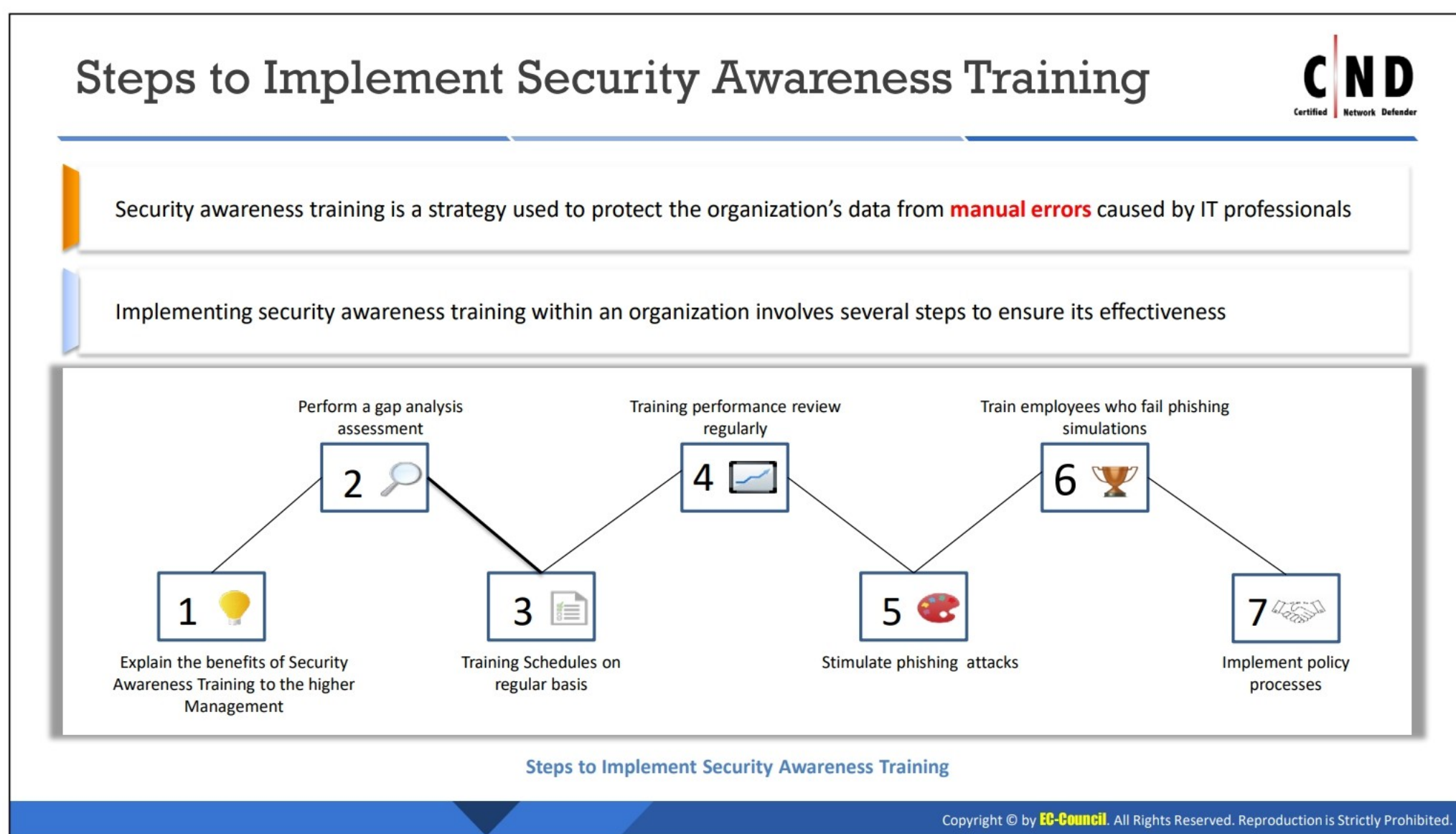
## Employee Training and Awareness: Data Classification

Security labels are used to restrict access to information in high and low security areas as a part of mandatory access control decisions. This enables easy understanding for users with and without permission to access and easy clearance of a large group of users. It defines the sensitivity of the data or the object and authorizations required for accessing the object or data. It provides a list of users who can access the document or the device and enables the user to understand the documents that they can access.

Security labels are categorized into different types based on who can access the data or object.

- **Unclassified:** No access permissions are required in order to access unclassified documents. Any person at any level may access these documents.
- **Restricted:** Only a few people can access the data or object. Sensitive data may be restricted for use in an organization because of its technical, business, and personal issues.
- **Confidential:** Confidential data or objects exposed may lead to financial or legal issues in an organization. Documents may be highly confidential or only confidential. Revealing these data—whether confidential or highly confidential—will lead to loss of critical information.
- **Secret:** Users authorized to access secret files may access secret, confidential, restricted, and unclassified data. Users cannot access documents or objects labeled as top secret, as it requires a higher clearance level.
- **Top Secret:** Users accessing top secret documents may access top secret, secret, confidential, restricted, and unclassified data.





## Steps to Implement Security Awareness Training

Security awareness training is a strategy followed by organizations to prevent data breaches and attacks resulting from employee errors. Using this strategy, organizations protect their critical data against infiltrators.

The following steps are involved in implementing security awareness training to strengthen the security of the organization are as follows:

- **Get Buy-in from the top down:** Explain why security awareness training is important and its benefits. Ensure the explanation should be well-tailored and well-pitched blended with the organization's goals and values.

The top-down approach helps quickly acquire the necessary materials and resources for training. It will allow an increase in the number of employees to adopt training.

- **Perform a gap analysis assessment:** Assess the organization's security awareness vulnerabilities and potential human risks. To do this, set up a gap analysis assessment as follows:
  - Identify the places where cyber-attacks frequently occur, and analyze why employees are susceptible to phishing emails.
  - Establish an ideal future state, outlining the potential savings if no staff falls victim to cyber-attacks.
  - Analyze the current state to identify the causes contributing to data breaches and assess if workers are adequately trained.



- Assess how many employees have fallen victim to cyber threats by comparing the current state of the organization and the its desired state.
  - Create a plan to bridge the gaps and identify the ways to fix them.
- **Schedule regular and consistent training:** Educate the organization's staff frequently to protect the organization's data, as cyber-attacks continue to increase. The need for ongoing security awareness training becomes increasingly important.
- **Review training performance regularly:** Review employees' performance regularly during and after training to assess their progress and identify areas of improvement. Provide employees with short tests to evaluate their performance, determine their next steps, and assess the key metrics that shall help measure the impact of the training to educate the employees through real-time training and overcome any exiting gaps.
- **Deploy periodic phishing simulations:** Measure employees' improvement through periodic phishing simulations, which help employees understand the mechanics of cyber security threats.
- **Educate employees who fail phishing simulations:** Address employees who repeatedly fail phishing simulations. Use frequent phishing exercises to help them identify phishing attempts. Identify additional resources needed for their education, such as changing their response processes, reinforcing rewards for reporting phishing attempts, and including gamification and specific stories about the consequences of falling for phishing.
- **Implement policy processes:** Provide employees with clear policy documentation during their training using existing templates, such as email and password policies, to save money and time. Edit these templates as needed to fit organizational needs.





### LO#05: Discuss other administrative security measures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## LO#05: Discuss Other Administrative Security Measures

This section explains the administrative security measures such as maintaining staff hiring and leaving process as well as employee monitoring, which together play an important role in an organization's security.



## Staff Hiring and Leaving Process



■ Consider and implement personnel security measures, starting from the selection and hiring of staff or contractors to **relieving** them of their duties

- Provide orientation sessions explaining the company background, along with their roles and responsibilities, and security policies
- Insert clauses in the contract to enforce personnel security for contractors and audit their compliance
- Remove access rights and collect all company assets from employees and contractors when they leave the organization
- Hire employees after a thorough identity verification and background check
- Contractors should be hired with the same due diligence as in-house employees are

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Staff Hiring and Leaving Process

Consider and implement the following personnel security measures, starting from the selection and hiring of staff or contractors to relieving them of their duties.

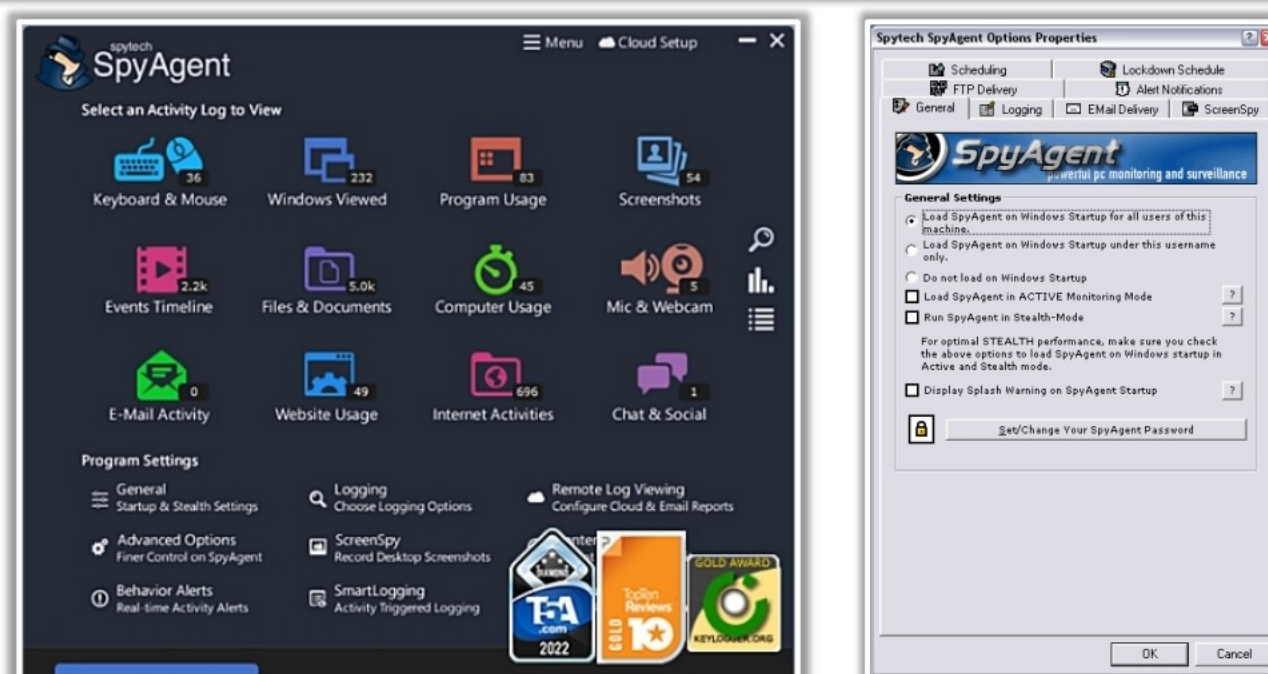
- Provide orientation sessions explaining the company background, along with the staff or contractors' roles and responsibilities, and security policies.
- Insert clauses in the contract to enforce personnel security for contractors and audit their compliance.
- Remove access rights and collect all company assets (e.g., keys, access cards, systems, mobile phones) from employees and contractors when they leave an organization.
- Remove critical organization data from the employee's personal device before he or she leaves.
- Change network and workstation passwords.
- Deactivate an organization's email accounts and remote access accounts.
- Conduct a debriefing session to detect any unnoticed electronic form of encrypting files/work in progress.
- Hire employees after thorough identity verification and background check.
- Contractors should be hired with the same due diligence as in-house employees are.
- Remove biometric or badge access codes.



## Employee Monitoring



- The organization should conduct **indiscriminate monitoring of employees' activities** to detect any act related to the policy violation
- Use employee monitoring tool such as **Spytech SpyAgent** to monitor employee behavior



Source: <https://www.spytech-web.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Employee Monitoring

An organization should conduct indiscriminate monitoring of employee's activities to detect any activity that may violate policy. Employee monitoring is helpful to measure and enhance productivity and secure corporate resources. This can be done by tracking attendance and collecting proof of the hours that employees have worked. This way, unacceptable behavior may be prevented or curtail before it impacts a business. Use employee monitoring tools such as Spytech SpyAgent to monitor employee behavior.

### Spytech SpyAgent

Source: [www.spytech-web.com](http://www.spytech-web.com)

Spytech SpyAgent is a spy software that allows monitoring and recording of all user activity on a computer. It provides the following activity monitoring and surveillance features:

- Keystroke logging
- Screenshot capturing
- Website activity
- Application usage monitor
- Emails sent and received monitoring
- Events timeline logging
- Internet social network activity and chat conversations
- Webmail and website content
- Computer usage logging



- Sound-triggered microphone audio recording
- Webcam capture recording
- Files uploaded and downloaded, files/documents accessed, files system usage, and files/documents printed
- Window and mouse activity
- Clipboard logging
- Activity logging
- Real-time remote desktop viewing and control
- Specific program logging
- Spyanywhere cloud access to settings and real-time log viewing
- Email log delivery
- FTP log delivery





## LO#06: Discuss asset management


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### LO#06: Discuss Asset Management

Network defenders must be aware of their organization's IT asset management (ITAM), which involves tracking an asset from its discovery to its eventual disposal. This section explains what ITAM is, its key components, types, and complete lifecycle. Additionally, this section covers tools useful for ITAM and best practices for best asset management.



## IT Asset Management



IT asset management(ITAM) is the process of **maintaining the logs** of all assets of an organization's IT infrastructure

The assets can be hardware, software, licenses, or information of an organization

It involves **developing and maintaining** policies, standards, processes, and measurements to manage IT assets in accordance with risk, control, governance, compliance, costs and performance objectives that are set by an organization

### Advantages of ITAM

- Thorough **tracking** of hardware and software assets
- Ensuring compliance with license agreements
- Assessing software installation
- Integrating procurement and IT management
- Removing rogue devices
- Enhancing employee productivity

### Components of ITAM

- Financial data** comprises estimating the cost of purchasing and **operating assets**, their value generation, and their possible resale price
- Physical data** comprises the **information** about the location of an asset and the current usage of it
- Contractual data** comprises the clauses that exist in the **contract** between a company/vendor/purchaser

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## IT Asset Management

IT Asset Management (ITAM) involves tracking an asset throughout its lifecycle, from initial discovery to final disposal. This process helps make strategic decisions regarding IT assets using relevant contractual, financial, and inventory data. Such assets could be hardware, software, licenses, or even the proprietary information of an organization. ITAM is instrumental in the development and maintenance of policies, standards, processes, and metrics that manage IT assets in accordance with risk, control, governance, compliance, cost, and performance objectives set by an organization.

Utilizing ITAM, security teams can efficiently identify and remove rogue devices, and prevent unauthorized installations. The system aids in detecting missing assets and discovering those that are vulnerable. IT administrators can leverage asset inventory data to ensure all IT assets are properly accounted for and configured with the appropriate tools to keep software applications up to date. The security administrators, through ITAM, gain comprehensive visibility into IT devices, ensuring each device is securely configured and updated with the latest security updates.

### Advantages of ITAM

The advantages of ITAM include:

- **Thorough tracking of assets:** ITAM enables meticulous tracking of computing assets, complete with details including the date of purchase, product number, and technical specifications like CPU type, memory, processor speed, IP address, and available disk space. By providing specifications of both software and hardware, it enables transparency in IT capabilities.



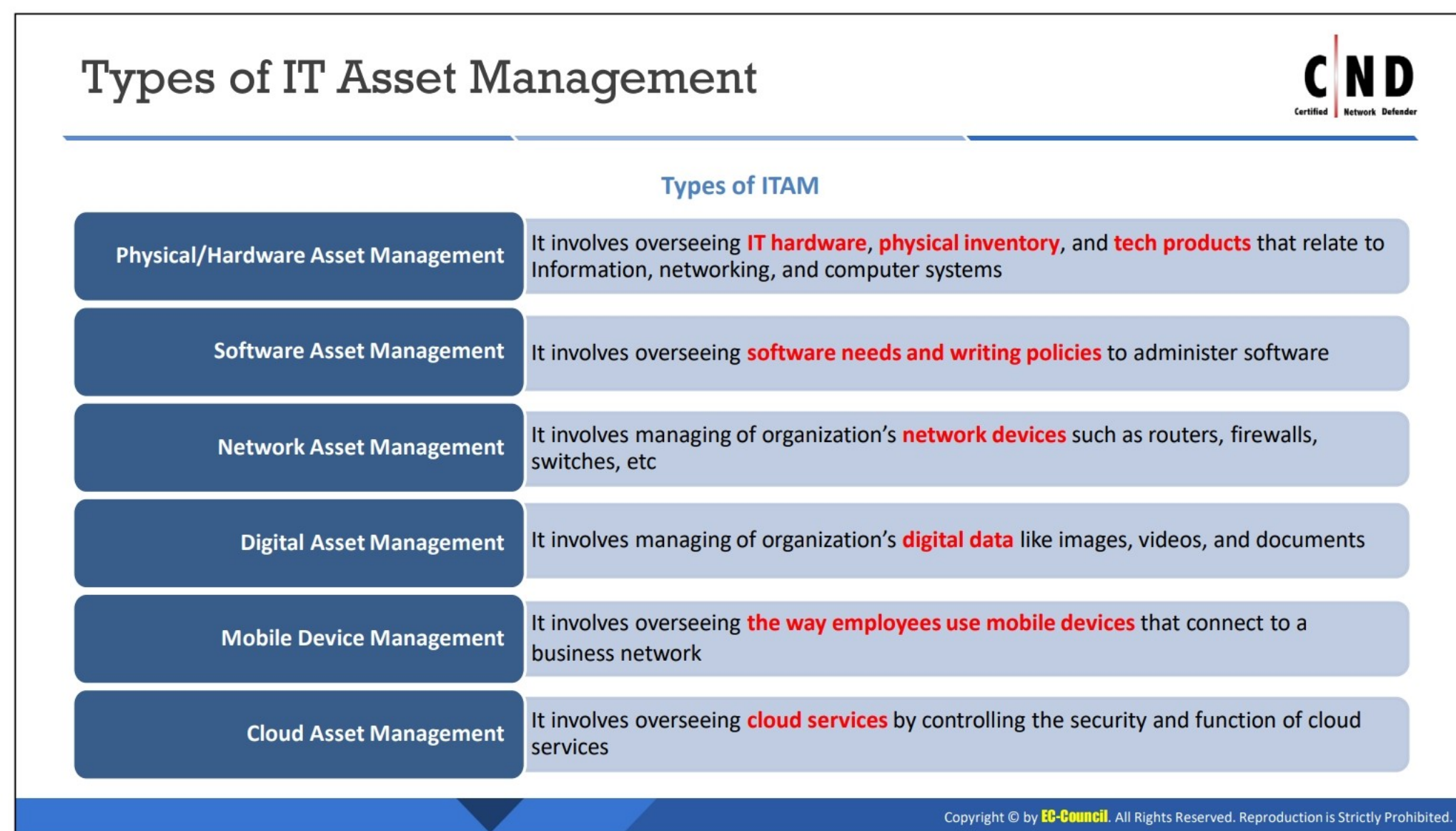
- **Ensures compliance with license agreements:** ITAM automatically detects software installed on every machine linked to the network. This automated detection can be cross-referenced with service level agreements, ensuring compliance with licensing agreements and avoiding risk of penalties.
- **Assesses software installation:** ITAM assesses installations and analyzes usage data, helping organizations identify and remove unneeded software licenses that incur extra expenditures. Monitor the number of devices on which a specific application is set up, along with the real usage metrics of that application. A purchased license holds no value if the user never uses the application—presenting a scope for the organization to reduce expenses.
- **Integrates procurement and IT management:** ITAM offers a comprehensive perspective on how the organization fulfills its hardware and software requirements by merging procurement and IT administration into a unified dashboard. This holistic approach enables for precise evaluations of existing software while projecting future necessities within a single interface. This seamless integration facilitates efficient strategic planning and careful budget distribution. For hardware, the system provides valuable insights into procurement that can guide budget allocation for refreshing and analyzing financial data with IT inventory. Plan new purchases based on inventory reaching the end of its lifespan, and data on IT inventory utilization.

### Components of ITAM

The key components of ITAM include:

- **Financial data:** This comprises estimating the costs associated with purchasing, and operating assets, their value generation, and their possible resale price. This data set comprises details such as purchase date, depreciation, quantity, and purchase price.
- **Physical data:** This comprises information about the location and current usage status of an asset. It identifies the assets that are currently in use, as well as those out of commission due to damage or malfunction.
- **Contractual data:** This component comprises the clauses stipulated in contracts between the company/vendor/purchaser. These clauses generally comprise service levels, maintenance, license types, device quantities, pricing, and contract durations. Accurate contractual data is essential for understanding the rights and responsibilities associated with the IT assets of the organization.





## Types of IT Asset Management

The various types of ITAM are as follows:

- **Physical asset management:** This type involves supervising IT hardware, physical inventory, and technology products related to information, networking, and computing systems. It helps organizations decide on the kind of devices an organization requires. The strategy for physical ITAM revolves around evaluating the technical specifications pertinent to a project or operational needs. Management of physical devices often encompasses locating appropriate storage, verifying device compatibility with existing software, and initiating equipment orders to support scalability. Examples of physical assets include monitors, hard drives, and scanners.
- **Software asset management:** This involves managing an organization's software needs and developing policies for software administration. The aim is to ensure all software is appropriately licensed. This includes careful review of third-party software license agreements to ensure that software is installed on the permitted number of devices and is frequently updated. Software assets can range from internal business applications to client-focused software products and third-party programs.
- **Network asset management:** This type pertains to the management of the organization's network infrastructure. Responsibilities include network inventory management, configuration management, and performance monitoring of network assets such as firewalls, wireless access points, routers, and switches.
- **Digital asset management:** This involves managing the organization's data and information assets. Digital assets refer to any data input into a database, and this type of



asset management refers to organizing that data efficiently. Examples include photos, videos, spreadsheets, financial details, and customer information.

- **Mobile device management:** This type of asset involves overseeing the way employees use mobile devices that connect to a business network. It refers to implementing policies that dictate usage to ensure data safety and security. Standards for the types of apps that can be downloaded on devices are also set. Elements of mobile assets include password-protecting organizational apps, limiting access to an organization's data through mobile devices, and downloading administrative software on company-owned phones.
- **Cloud asset management:** Numerous organizations now opt for cloud storage for their data, moving away from internal databases. Managing cloud assets involves guaranteeing the uninterrupted availability of online-hosted data and services for employees. It entails scrutinizing the key roles that cloud services play within the organization and overseeing their security and performance. Examples of cloud-based assets include online servers, metadata histories, web storage, and cloud security and compliance measures.



## ITAM Process: Asset Identification and Categorization



- Asset identification and categorization constitutes the **fundamental first step in ITAM**
- It provides a clear understanding of the IT resources possessed by the organization such as where they are located and how they are being used

### Asset Identification

- It includes discovering and documenting all physical (e.g., computers, servers, networking equipment) and digital (e.g., software licenses, digital certificates, data) IT assets present in an organization

### Asset Categorization

- The identified assets are categorized (grouped based on various criteria) to optimize tracking of the assets
- The grouping criteria may vary from organization to organization based on their requirements and goals
- Commonly assets are categorized based on:
  - Type of asset
  - Usage
  - Location
  - Owner/Department
  - Lifecycle Stage
  - Vendor/Manufacturer
  - Criticality
  - License Type

| NAME                    | TYPE           | DOMAIN    | IP ADDRESS  | MAC ADDRESS       | MANUFACTURER                  | MODEL      |
|-------------------------|----------------|-----------|-------------|-------------------|-------------------------------|------------|
| CONHG4501.conhsoc.local | Linux          | -         | 10.40.0.13  | 98:30:30:30:30:30 | Dell Inc.                     | OptiPlex 9 |
| CONHG4502.conhsoc.local | Linux          | -         | 10.40.0.14  | 98:30:30:30:30:30 | Dell Inc.                     | OptiPlex 9 |
| CONHG4503.conhsoc.local | Linux          | -         | 10.40.0.15  | 98:30:30:30:30:30 | Dell Inc.                     | OptiPlex 9 |
| CONHG4504               | Router         | -         | 10.40.0.16  | 98:30:30:30:30:30 | Netgear Inc.                  | JS64 v4    |
| CONHG4505.conhsoc.local | NAS            | -         | 10.40.0.17  | 98:30:30:30:30:30 | Network Appliance Corporation | NetScout   |
| CONHG4506               | Windows Server | WOPH4506P | 10.40.0.1   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4507               | Windows        | CONH4507  | 10.40.0.2   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4508               | Windows        | CONH4508  | 10.40.0.3   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4509               | Windows        | CONH4509  | 10.40.0.4   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4510               | Windows        | CONH4510  | 10.40.0.5   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4511               | Windows        | CONH4511  | 10.40.0.6   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4512               | Windows        | CONH4512  | 10.40.0.7   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4513               | Windows        | CONH4513  | 10.40.0.8   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4514               | Windows        | CONH4514  | 10.40.0.9   | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4515               | Windows        | CONH4515  | 10.40.0.10  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4516               | Windows        | CONH4516  | 10.40.0.11  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4517               | Windows        | CONH4517  | 10.40.0.12  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4518               | Windows        | CONH4518  | 10.40.0.13  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4519               | Windows        | CONH4519  | 10.40.0.14  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4520               | Windows        | CONH4520  | 10.40.0.15  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4521               | Windows        | CONH4521  | 10.40.0.16  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4522               | Windows        | CONH4522  | 10.40.0.17  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4523               | Windows        | CONH4523  | 10.40.0.18  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4524               | Windows        | CONH4524  | 10.40.0.19  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4525               | Windows        | CONH4525  | 10.40.0.20  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4526               | Windows        | CONH4526  | 10.40.0.21  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4527               | Windows        | CONH4527  | 10.40.0.22  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4528               | Windows        | CONH4528  | 10.40.0.23  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4529               | Windows        | CONH4529  | 10.40.0.24  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4530               | Windows        | CONH4530  | 10.40.0.25  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4531               | Windows        | CONH4531  | 10.40.0.26  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4532               | Windows        | CONH4532  | 10.40.0.27  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4533               | Windows        | CONH4533  | 10.40.0.28  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4534               | Windows        | CONH4534  | 10.40.0.29  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4535               | Windows        | CONH4535  | 10.40.0.30  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4536               | Windows        | CONH4536  | 10.40.0.31  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4537               | Windows        | CONH4537  | 10.40.0.32  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4538               | Windows        | CONH4538  | 10.40.0.33  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4539               | Windows        | CONH4539  | 10.40.0.34  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4540               | Windows        | CONH4540  | 10.40.0.35  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4541               | Windows        | CONH4541  | 10.40.0.36  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4542               | Windows        | CONH4542  | 10.40.0.37  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4543               | Windows        | CONH4543  | 10.40.0.38  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4544               | Windows        | CONH4544  | 10.40.0.39  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4545               | Windows        | CONH4545  | 10.40.0.40  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4546               | Windows        | CONH4546  | 10.40.0.41  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4547               | Windows        | CONH4547  | 10.40.0.42  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4548               | Windows        | CONH4548  | 10.40.0.43  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4549               | Windows        | CONH4549  | 10.40.0.44  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4550               | Windows        | CONH4550  | 10.40.0.45  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4551               | Windows        | CONH4551  | 10.40.0.46  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4552               | Windows        | CONH4552  | 10.40.0.47  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4553               | Windows        | CONH4553  | 10.40.0.48  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4554               | Windows        | CONH4554  | 10.40.0.49  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4555               | Windows        | CONH4555  | 10.40.0.50  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4556               | Windows        | CONH4556  | 10.40.0.51  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4557               | Windows        | CONH4557  | 10.40.0.52  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4558               | Windows        | CONH4558  | 10.40.0.53  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4559               | Windows        | CONH4559  | 10.40.0.54  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4560               | Windows        | CONH4560  | 10.40.0.55  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4561               | Windows        | CONH4561  | 10.40.0.56  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4562               | Windows        | CONH4562  | 10.40.0.57  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4563               | Windows        | CONH4563  | 10.40.0.58  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4564               | Windows        | CONH4564  | 10.40.0.59  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4565               | Windows        | CONH4565  | 10.40.0.60  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4566               | Windows        | CONH4566  | 10.40.0.61  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4567               | Windows        | CONH4567  | 10.40.0.62  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4568               | Windows        | CONH4568  | 10.40.0.63  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4569               | Windows        | CONH4569  | 10.40.0.64  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4570               | Windows        | CONH4570  | 10.40.0.65  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4571               | Windows        | CONH4571  | 10.40.0.66  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4572               | Windows        | CONH4572  | 10.40.0.67  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4573               | Windows        | CONH4573  | 10.40.0.68  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4574               | Windows        | CONH4574  | 10.40.0.69  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4575               | Windows        | CONH4575  | 10.40.0.70  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4576               | Windows        | CONH4576  | 10.40.0.71  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4577               | Windows        | CONH4577  | 10.40.0.72  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4578               | Windows        | CONH4578  | 10.40.0.73  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4579               | Windows        | CONH4579  | 10.40.0.74  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4580               | Windows        | CONH4580  | 10.40.0.75  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4581               | Windows        | CONH4581  | 10.40.0.76  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4582               | Windows        | CONH4582  | 10.40.0.77  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4583               | Windows        | CONH4583  | 10.40.0.78  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4584               | Windows        | CONH4584  | 10.40.0.79  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4585               | Windows        | CONH4585  | 10.40.0.80  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4586               | Windows        | CONH4586  | 10.40.0.81  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4587               | Windows        | CONH4587  | 10.40.0.82  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4588               | Windows        | CONH4588  | 10.40.0.83  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4589               | Windows        | CONH4589  | 10.40.0.84  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4590               | Windows        | CONH4590  | 10.40.0.85  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4591               | Windows        | CONH4591  | 10.40.0.86  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4592               | Windows        | CONH4592  | 10.40.0.87  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4593               | Windows        | CONH4593  | 10.40.0.88  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4594               | Windows        | CONH4594  | 10.40.0.89  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4595               | Windows        | CONH4595  | 10.40.0.90  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4596               | Windows        | CONH4596  | 10.40.0.91  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4597               | Windows        | CONH4597  | 10.40.0.92  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4598               | Windows        | CONH4598  | 10.40.0.93  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4599               | Windows        | CONH4599  | 10.40.0.94  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4600               | Windows        | CONH4600  | 10.40.0.95  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4601               | Windows        | CONH4601  | 10.40.0.96  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4602               | Windows        | CONH4602  | 10.40.0.97  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4603               | Windows        | CONH4603  | 10.40.0.98  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4604               | Windows        | CONH4604  | 10.40.0.99  | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |
| CONHG4605               | Windows        | CONH4605  | 10.40.0.100 | 00:10:30:30:30:30 | VMware, Inc.                  | VMware ES  |

LANSWEEPER: Asset Identification

Source: [www.lansweeper.com](http://www.lansweeper.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ITAM Process: Asset Identification and Categorization

The first step in ITAM process is asset identification and categorization, which provides a clear understanding of the IT resources possessed by the organization. This includes their location and how they are used.

### Asset Identification

This phase includes discovering and documenting all physical assets like computers, servers, and networking equipment, as well as digital assets such as software licenses, digital certificates, and data. An accurate asset inventory is created at this stage, containing thorough data about each device. This inventory helps in asset maintenance, identifies and remediates firmware vulnerabilities, and ensures all systems are always secured and up to date. Configuring asset discovery according to organizational needs is also an integral part of this stage.

### Asset Categorization

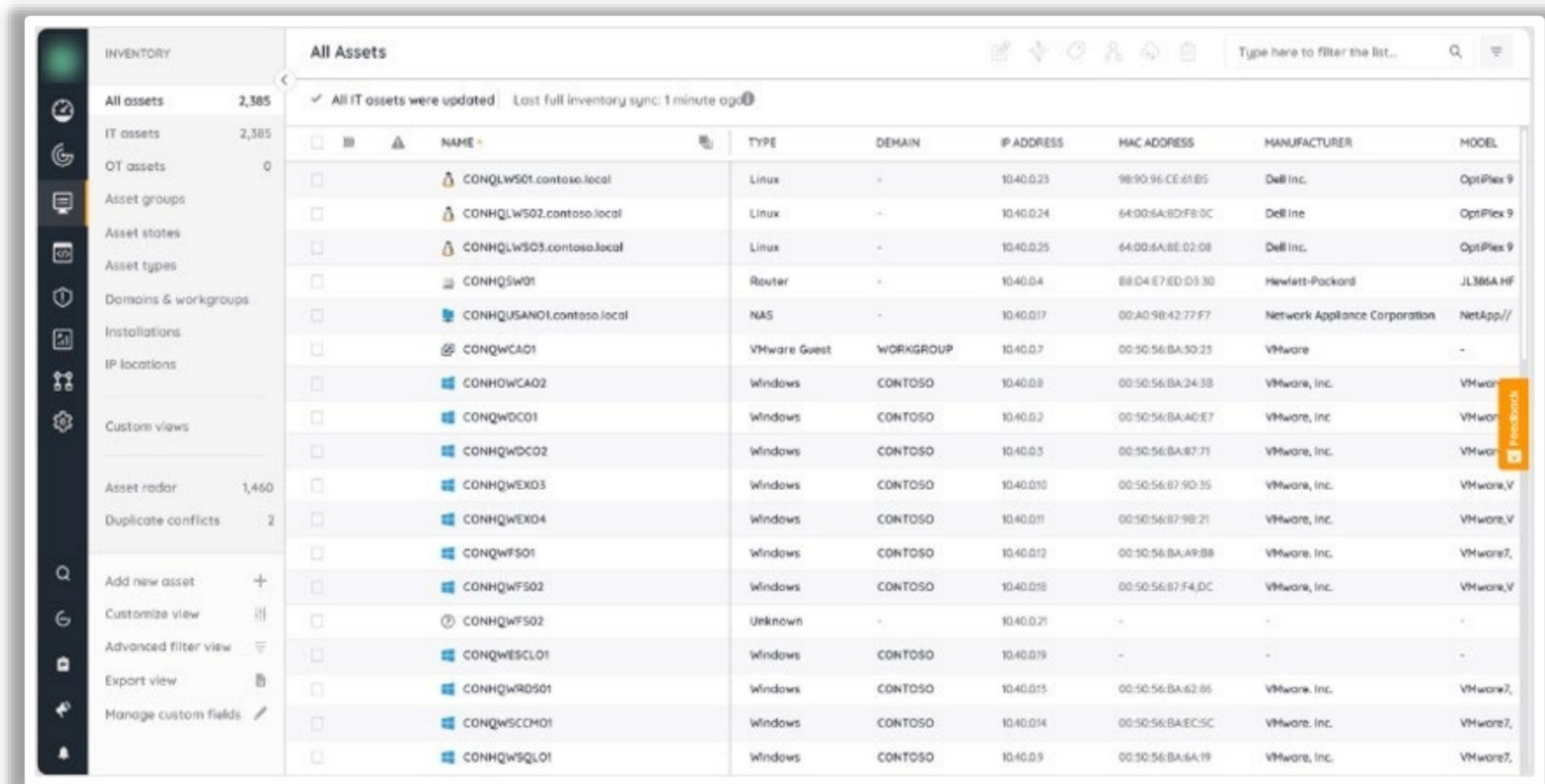
Once assets are identified, they are categorized based on various criteria to streamline asset tracking. The assets can be automatically sorted into predefined types, but dynamic asset groups can also be created. Alternatively, assets can be sorted according to their IP addresses. The method of grouping may differ from one organization to another, influenced by their specific requirements and goals.

Common criteria for categorizing assets include:

- Type of Asset
- Usage
- Location



- Owner/Department
- Lifecycle Stage
- Vendor/Manufacturer
- Criticality
- License Type



The screenshot displays the Lansweeper 'All Assets' page. On the left is a sidebar with navigation options: INVENTORY, All assets (2,385), IT assets (2,385), OT assets (0), Asset groups, Asset states, Asset types, Domains & workgroups, Installations, IP locations, Custom views, Asset radar (1,460), and Duplicate conflicts (2). The main area shows a table of assets with columns: NAME, TYPE, DOMAIN, IP ADDRESS, MAC ADDRESS, MANUFACTURER, and MODEL. The table lists various assets including Linux servers, a Router, a NAS, and multiple Windows VMs. A status bar at the top indicates 'All IT assets were updated' and 'Last full inventory sync: 1 minute ago'.

| NAME                      | TYPE         | DOMAIN    | IP ADDRESS | MAC ADDRESS       | MANUFACTURER                  | MODEL      |
|---------------------------|--------------|-----------|------------|-------------------|-------------------------------|------------|
| CONQLWS01.contoso.local   | Linux        | -         | 10.40.0.23 | 98:90:96:CE:61:B5 | Dell Inc.                     | OptiPlex 9 |
| CONHQLWS02.contoso.local  | Linux        | -         | 10.40.0.24 | 64:00:5A:8D:F8:0C | Dell Inc.                     | OptiPlex 9 |
| CONHQLWS03.contoso.local  | Linux        | -         | 10.40.0.25 | 64:00:5A:8E:02:08 | Dell Inc.                     | OptiPlex 9 |
| CONHQSW01                 | Router       | -         | 10.40.0.4  | 88:D4:E7:ED:D3:30 | Hewlett-Packard               | JL386A HF  |
| CONHQUSAN01.contoso.local | NAS          | -         | 10.40.0.17 | 00:A0:9B:42:77:F7 | Network Appliance Corporation | NetApp//   |
| CONHQWCA01                | VMware Guest | WORKGROUP | 10.40.0.7  | 00:50:56:BA:50:23 | VMware                        | -          |
| CONHQWCA02                | Windows      | CONTOSO   | 10.40.0.8  | 00:50:56:BA:24:3B | VMware, Inc.                  | VMware7,   |
| CONHQWDC01                | Windows      | CONTOSO   | 10.40.0.2  | 00:50:56:BA:AD:E7 | VMware, Inc.                  | VMware7,   |
| CONHQWDC02                | Windows      | CONTOSO   | 10.40.0.3  | 00:50:56:BA:87:71 | VMware, Inc.                  | VMware7,   |
| CONHQWEX03                | Windows      | CONTOSO   | 10.40.0.10 | 00:50:56:87:90:35 | VMware, Inc.                  | VMware7,   |
| CONHQWEX04                | Windows      | CONTOSO   | 10.40.0.11 | 00:50:56:87:9B:21 | VMware, Inc.                  | VMware7,   |
| CONHQWFS01                | Windows      | CONTOSO   | 10.40.0.12 | 00:50:56:BA:A9:B8 | VMware, Inc.                  | VMware7,   |
| CONHQWFS02                | Windows      | CONTOSO   | 10.40.0.18 | 00:50:56:87:F4:DC | VMware, Inc.                  | VMware7,   |
| CONHQWFS02                | Unknown      | -         | 10.40.0.21 | -                 | -                             | -          |
| CONHQWESCL01              | Windows      | CONTOSO   | 10.40.0.19 | -                 | -                             | -          |
| CONHQWRDS01               | Windows      | CONTOSO   | 10.40.0.15 | 00:50:56:BA:62:86 | VMware, Inc.                  | VMware7,   |
| CONHQWSCCH01              | Windows      | CONTOSO   | 10.40.0.14 | 00:50:56:BA:EC:5C | VMware, Inc.                  | VMware7,   |
| CONHQWSQL01               | Windows      | CONTOSO   | 10.40.0.9  | 00:50:56:BA:6A:19 | VMware, Inc.                  | VMware7,   |

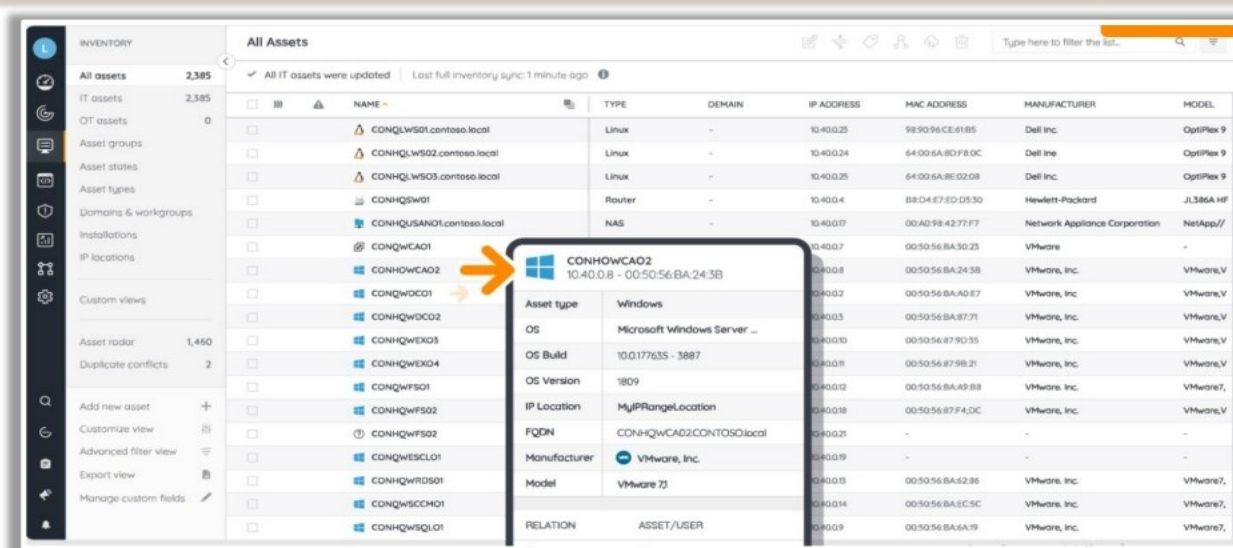
Figure 2.1: Lansweeper Asset Discovery



## ITAM Process: Asset Tracking



- Asset tracking involves **continuous monitoring** of IT assets with the help of an ITAM tool
- Accurate details of each asset such as asset name, serial number, purchase date, warranty status, license details, service-level agreements (SLAs) along user assignments, and condition of the physical assets are required to track assets



LANSWEEPER: Asset Tracking

Source: [www.lansweeper.com](http://www.lansweeper.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ITAM Process: Asset Tracking

Asset tracking enables real-time notification capabilities for various changes, including new software installations, hardware removals, software licensing status, and much more. This feature allows users to keep tabs on a myriad of factors with just a few clicks. By setting up policies and scheduling scans, users can gain insights into the types of files present within their network. Accurate details of each asset such as asset name, serial number, purchase date, warranty status, license details, service-level agreements (SLAs) along user assignments, and condition of the physical assets are required to track assets

Users can also establish rules for scanning specific types of files—such as audio, video, or documents—and determine the amount of disk space they occupy. Additionally, an ITAM tool can alert users when unnecessary files are deleted on computers with limited disk space, enabling better storage management.

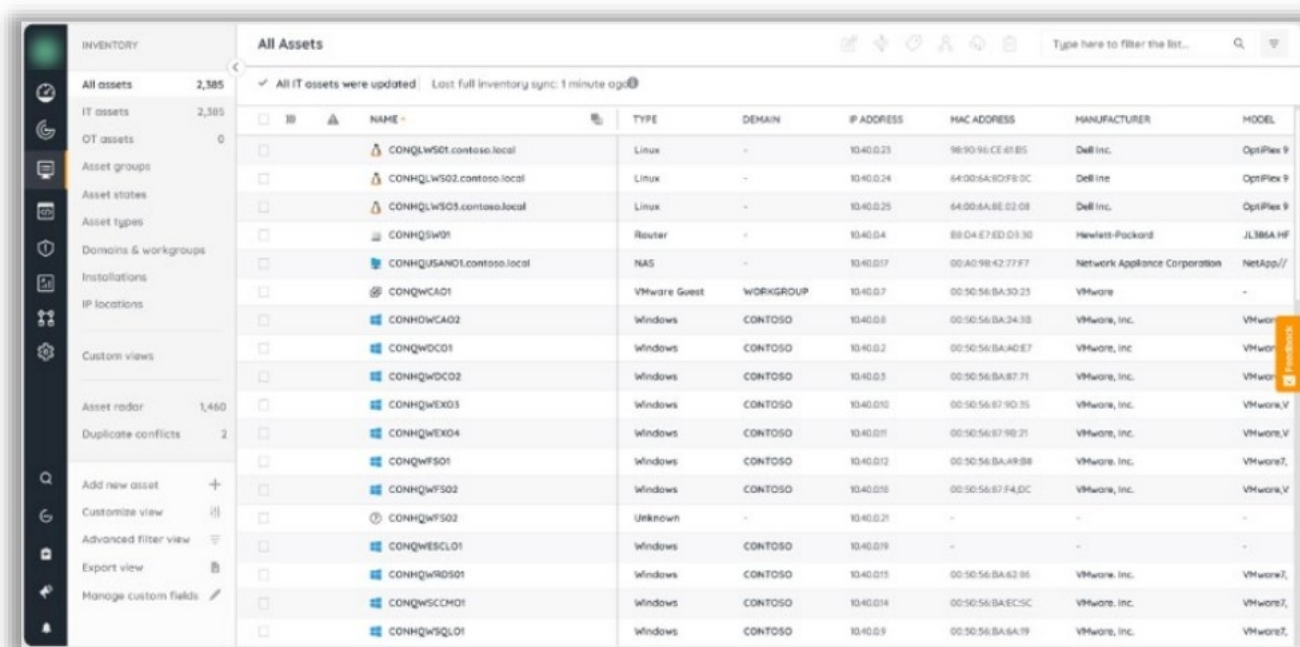


Figure 2.2: Asset Discovery in Lansweeper



## ITAM Process: Asset Maintenance



- Maintenance involves proper maintenance of the IT assets protects organizations' IT assets from unexpected downtime and security breaches
- The maintenance activities performed on IT assets are logged into the ITAM system for tracking the asset's performance
- Regular inspections** and audits, **scheduled maintenance**, and developing a clear plan for asset lifecycle management, from procurement to retirement, are key practices for proper asset maintenance

| ASSET NAME  | INSTALL ONE OF THESE UPDATES | ASSET DOMAIN | STATE  | WORKSTATION/SERVER | USER NAME | USER DOMAIN | IP ADDRESS | IP LOC... |
|-------------|------------------------------|--------------|--------|--------------------|-----------|-------------|------------|-----------|
| CONESWFS01  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.66 |           |
| CONESWWS01  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.71 |           |
| CONHOWCA02  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.8  |           |
| CONHQWDC01  | KB5022286                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.2  |           |
| CONHOWDC02  | KB5022286                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.3  |           |
| CONHOWEX03  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.10 |           |
| CONHQWEX04  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.11 |           |
| CONHOWZFS01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.12 |           |
| CONHOWFS02  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.18 |           |
| CONHOWRDS01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.13 |           |
| CONHOWSCH01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.14 |           |
| CONHOWSOL01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.9  |           |
| CONHOWWS01  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.41 |           |
| CONHOWWS02  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.20 |           |

LANSWEEPER: Report

Source: [www.Lansweeper.com](http://www.Lansweeper.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ITAM Process: Asset Maintenance

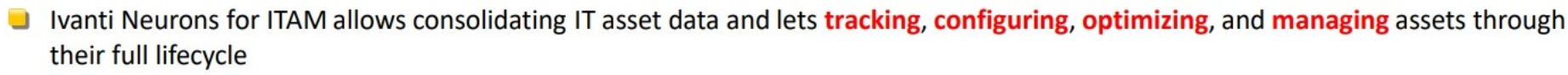
Regular maintenance is essential for maintaining hardware assets operating at their best and extending their lifespan. This includes both proactive measures, such as scheduled updates, and preventive strategies, such as reactive maintenance to tackle unexpected issues or malfunctions. Effective upkeep safeguards an organization's IT assets against unexpected downtime and security breaches. All maintenance activities conducted on these assets are meticulously logged into the ITAM system, which aids in tracking asset performance.

| ASSET NAME  | INSTALL ONE OF THESE UPDATES | ASSET DOMAIN | STATE  | WORKSTATION/SERVER | USER NAME | USER DOMAIN | IP ADDRESS | IP LOC... |
|-------------|------------------------------|--------------|--------|--------------------|-----------|-------------|------------|-----------|
| CONESWFS01  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.66 |           |
| CONESWWS01  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.71 |           |
| CONHOWCA02  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.8  |           |
| CONHQWDC01  | KB5022286                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.2  |           |
| CONHOWDC02  | KB5022286                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.3  |           |
| CONHOWEX03  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.10 |           |
| CONHQWEX04  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.11 |           |
| CONHOWZFS01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.12 |           |
| CONHOWFS02  | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.18 |           |
| CONHOWRDS01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.13 |           |
| CONHOWSCH01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.14 |           |
| CONHOWSOL01 | KB5022286                    | CONTOSO      | Active | Server             | -         | -           | 10.40.0.9  |           |
| CONHOWWS01  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.41 |           |
| CONHOWWS02  | KB5022282                    | CONTOSO      | Active | Workstation        | -         | -           | 10.40.0.20 |           |

Figure 2.3: Maintenance Records in Lansweeper



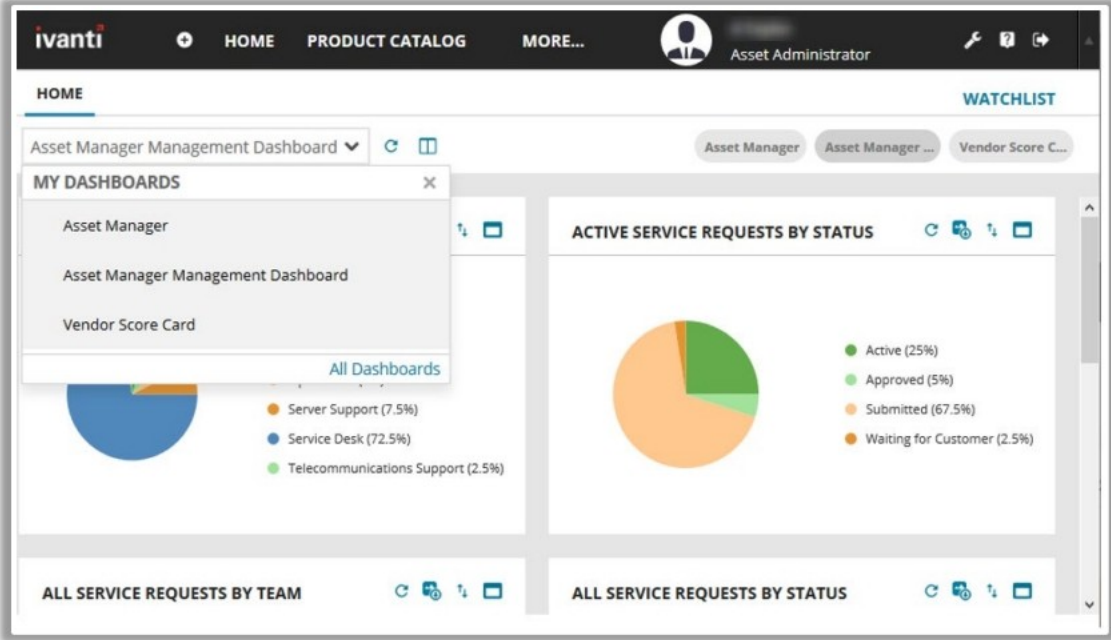
## IT Asset Management Tool: Ivanti Neurons



Ivanti Neurons for ITAM allows consolidating IT asset data and lets **tracking, configuring, optimizing, and managing** assets through their full lifecycle

### Features

- It tracks asset availability and performance
- It manages assets anytime and anywhere
- It stores vendor information to ensure managing strategic vendors effectively
- It provides insight into assets to gain control of the assets



The screenshot shows the Ivanti Neurons Dashboard. It features a top navigation bar with 'HOME', 'PRODUCT CATALOG', and 'MORE...'. Below this, there's a 'HOME' section with a dropdown menu for 'Asset Manager Management Dashboard'. A 'MY DASHBOARDS' panel lists 'Asset Manager', 'Asset Manager Management Dashboard', and 'Vendor Score Card'. A pie chart shows 'ACTIVE SERVICE REQUESTS BY STATUS' with categories: Active (25%), Approved (5%), Submitted (67.5%), and Waiting for Customer (2.5%). Another pie chart shows 'ALL SERVICE REQUESTS BY TEAM' with categories: Server Support (7.5%), Service Desk (72.5%), and Telecommunications Support (2.5%).

Ivanti Neurons Dashboard

Source: [www.ivanti.com](http://www.ivanti.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ITAM Tools: Ivanti Neurons

Source: [www.ivanti.com](http://www.ivanti.com)

Ivanti Neurons for ITAM offers a centralized platform for consolidating IT asset data. It allows for tracking, configuring, optimizing, and strategic management of assets throughout their entire lifecycle. The platform's flexible design allows users to create and adhere to customized workflows, providing a complete overview of hardware, server, client, virtual, cloud, and software assets from acquisition to decommissioning.

### Key Features

The tool boasts a wide array of features, such as:

- Tracking asset availability and performance
- Management of assets while on-the-go
- Cost and contract transparency
- Enhanced user interaction through a product catalog
- Quick asset updates via barcode scanning
- Vendor relationship management
- Seamless integration with a variety of services
- Effective strategies for improved service delivery



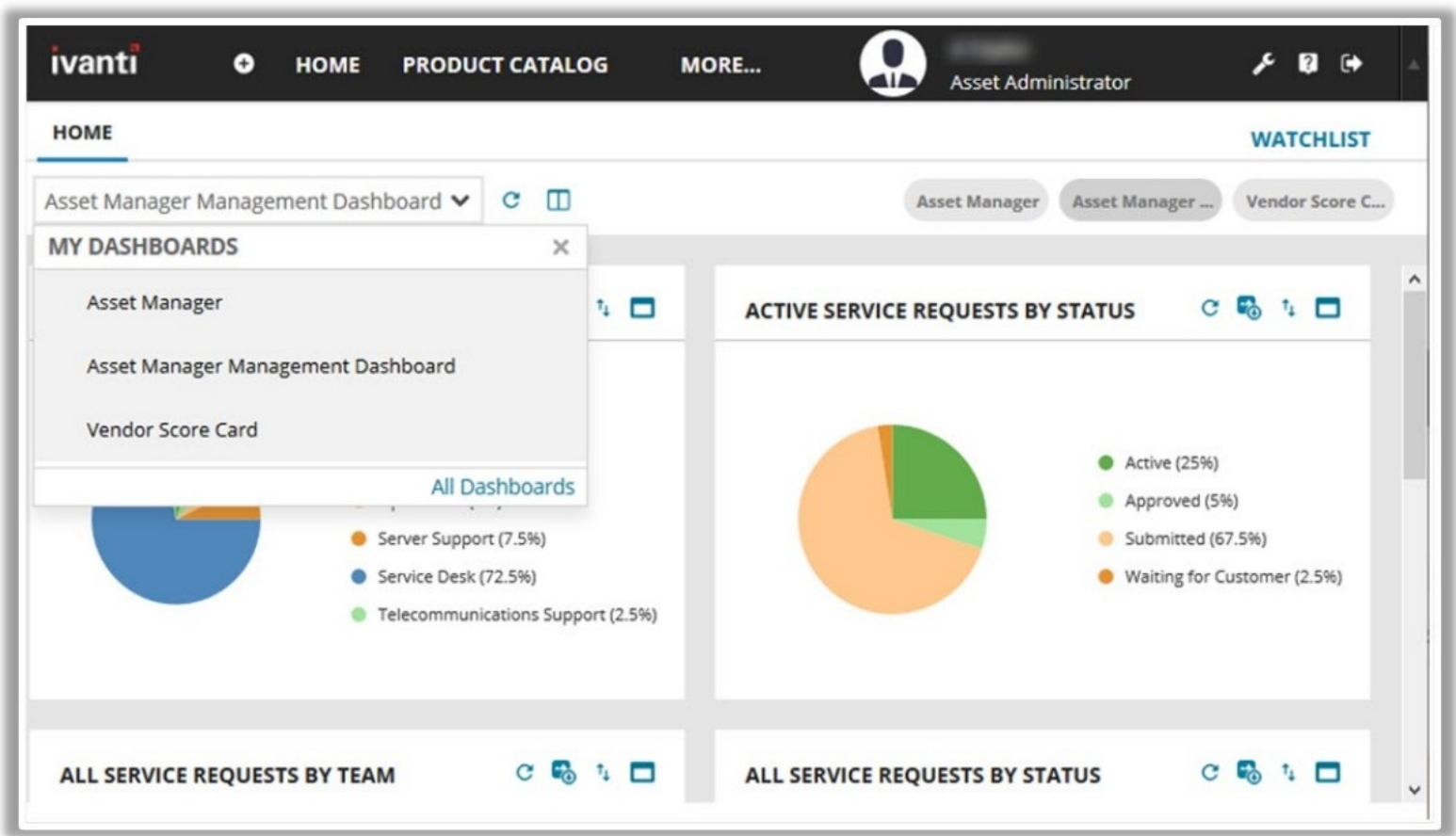


Figure 2.4: Ivanti Neurons for ITAM



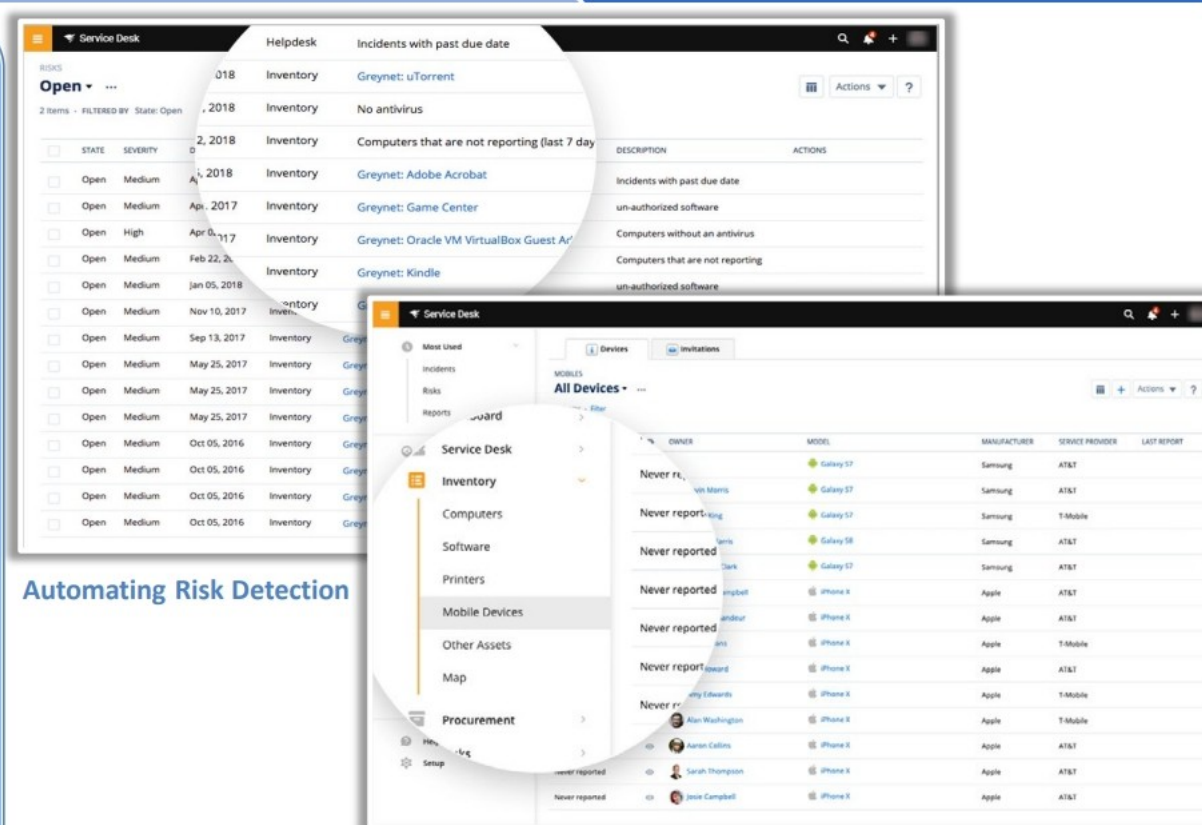
## IT Asset Management Tool: SolarWinds Service Desk



- SolarWinds Service Desk manages full IT **asset inventory** with comprehensive ITAM software. It **automates** IT asset management and manages license compliance from the cloud

### Key Features

- Provides consolidating assets with a unified IT asset management dashboard
- Automates risk detection by using asset management tools
- Leverages IT asset management to align assets with incidents
- Automates discovering current assets for better IT asset management
- Allows creating a centralized overview of asset configurations



### Automating Risk Detection

### IT Asset Management Dashboard

Source: [www.solarwinds.com](http://www.solarwinds.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ITAM Tool: SolarWinds Service Desk

Source: [www.solarwinds.com](http://www.solarwinds.com)

SolarWinds service desk manages full IT asset inventory through its comprehensive ITAM software. It keeps software licenses up to date by visualizing the full asset lifecycle, identifying areas to reduce overall costs. The platform automates ITAM and manages license compliance from the cloud.

### Key Features

Its features include the following:

- Consolidating assets via a unified ITAM dashboard.

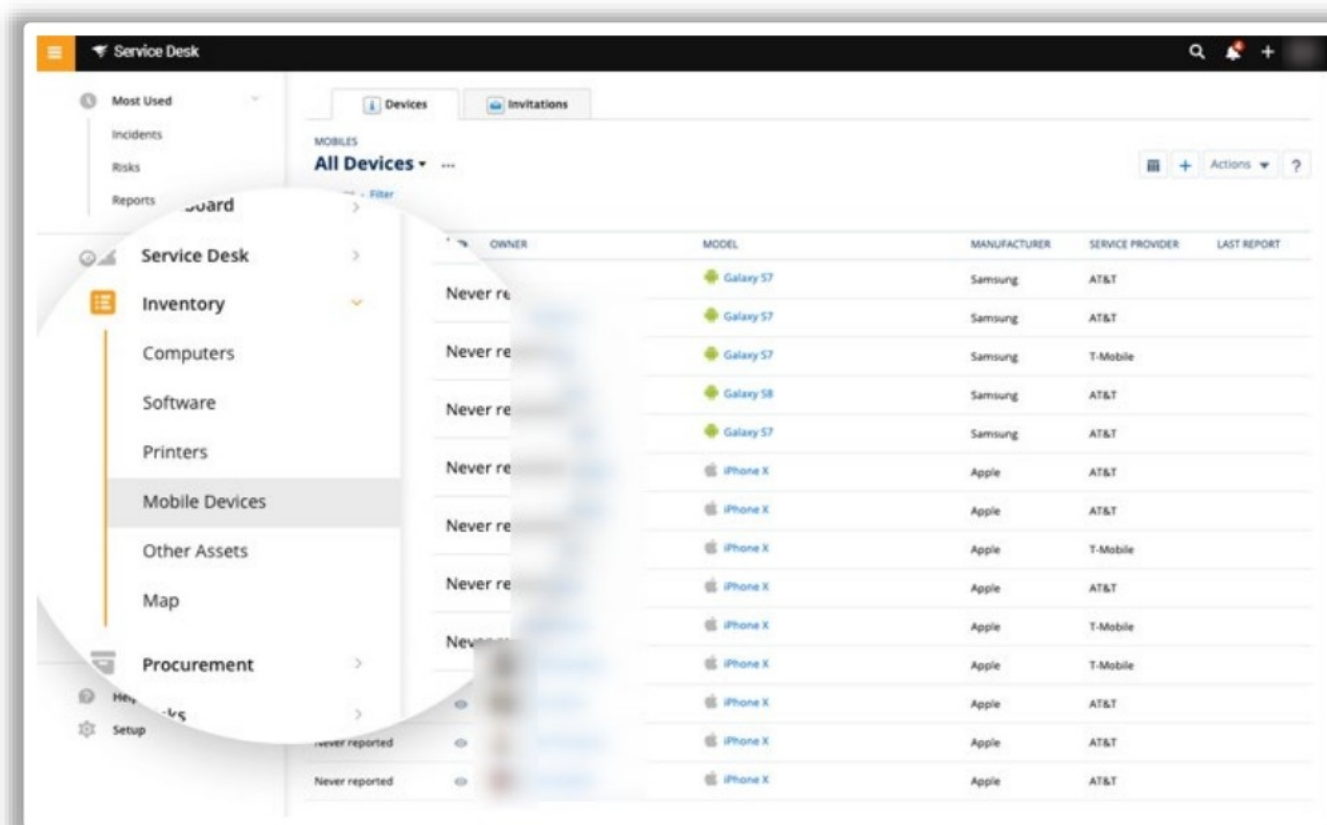


Figure 2.5: IT Asset Management Dashboard



- Automating risk detection with asset management tools

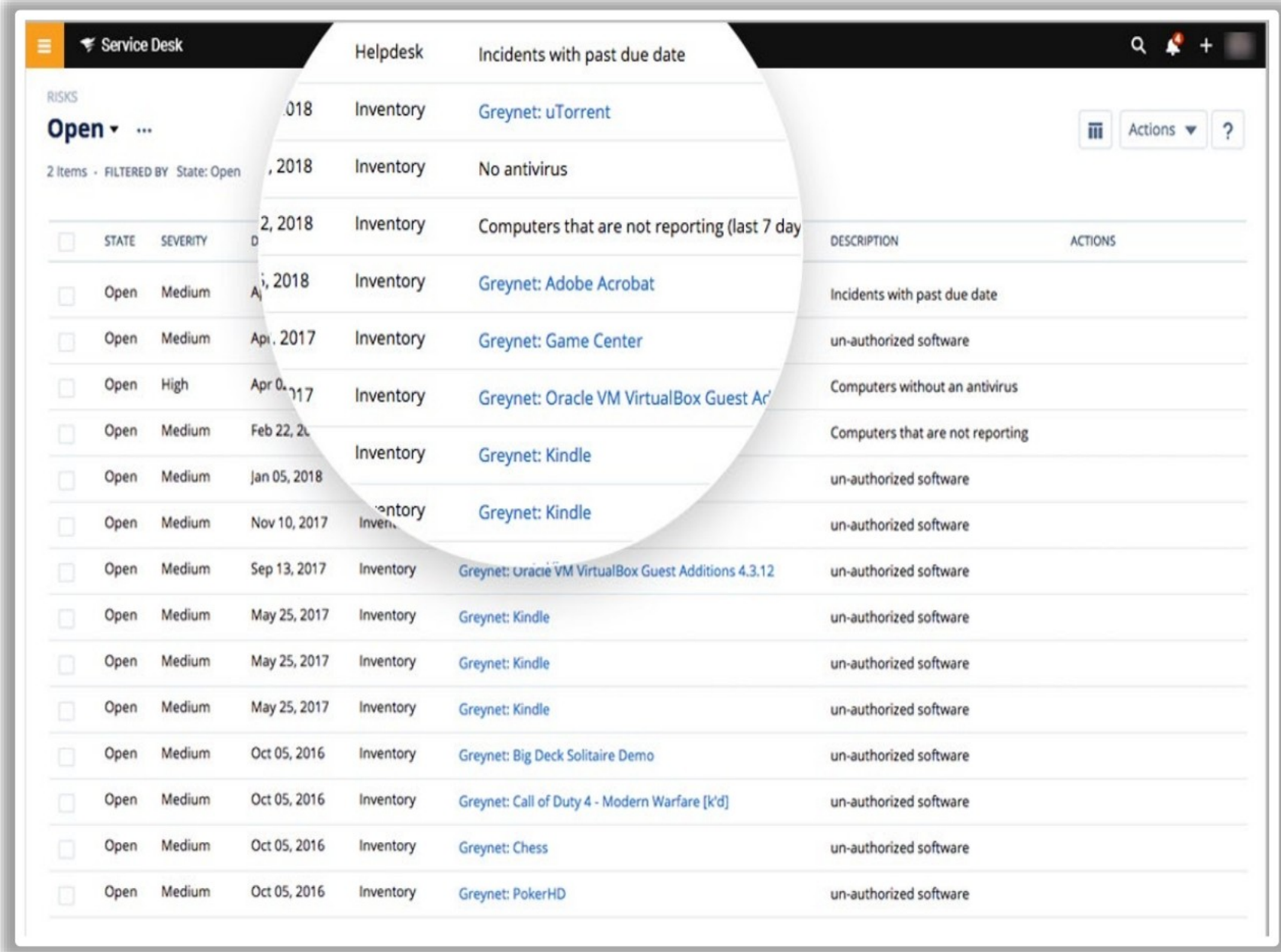


Figure 2.6: Automating Risk Detection

- Aligning assets with incidents through ITAM.

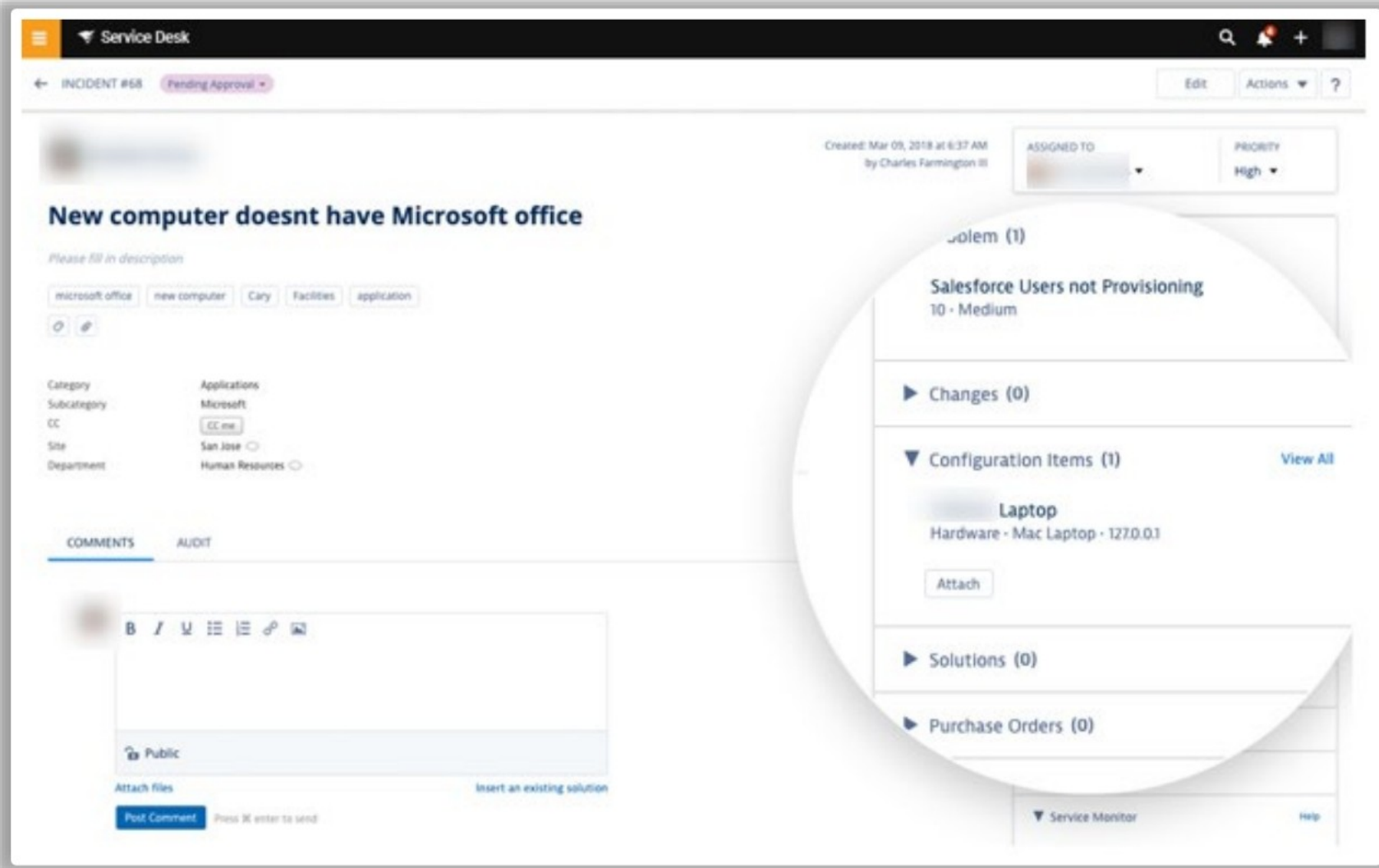
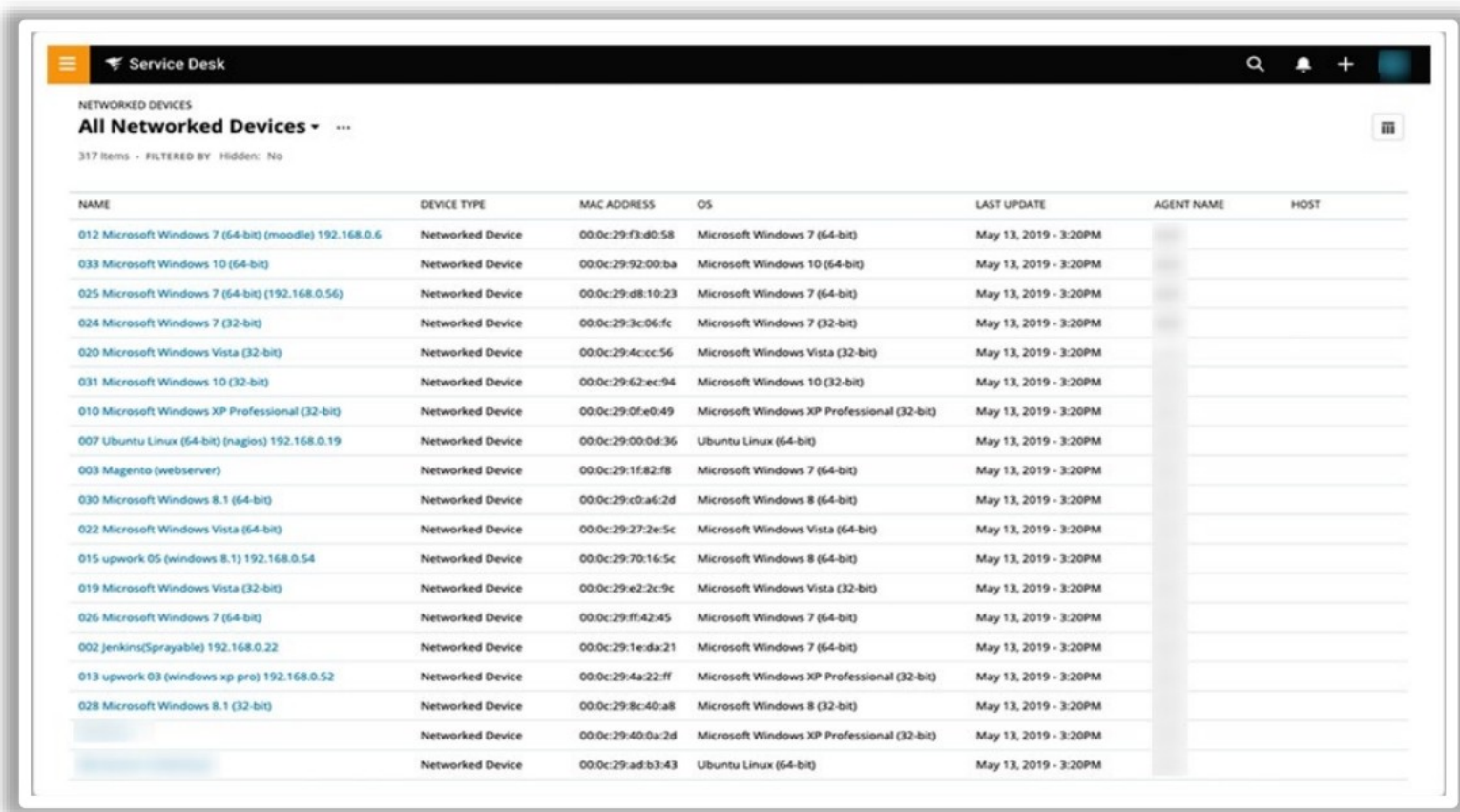


Figure 2.7: Aligning Assets with Incidents



- Automating the discovery of current assets for better ITAM.

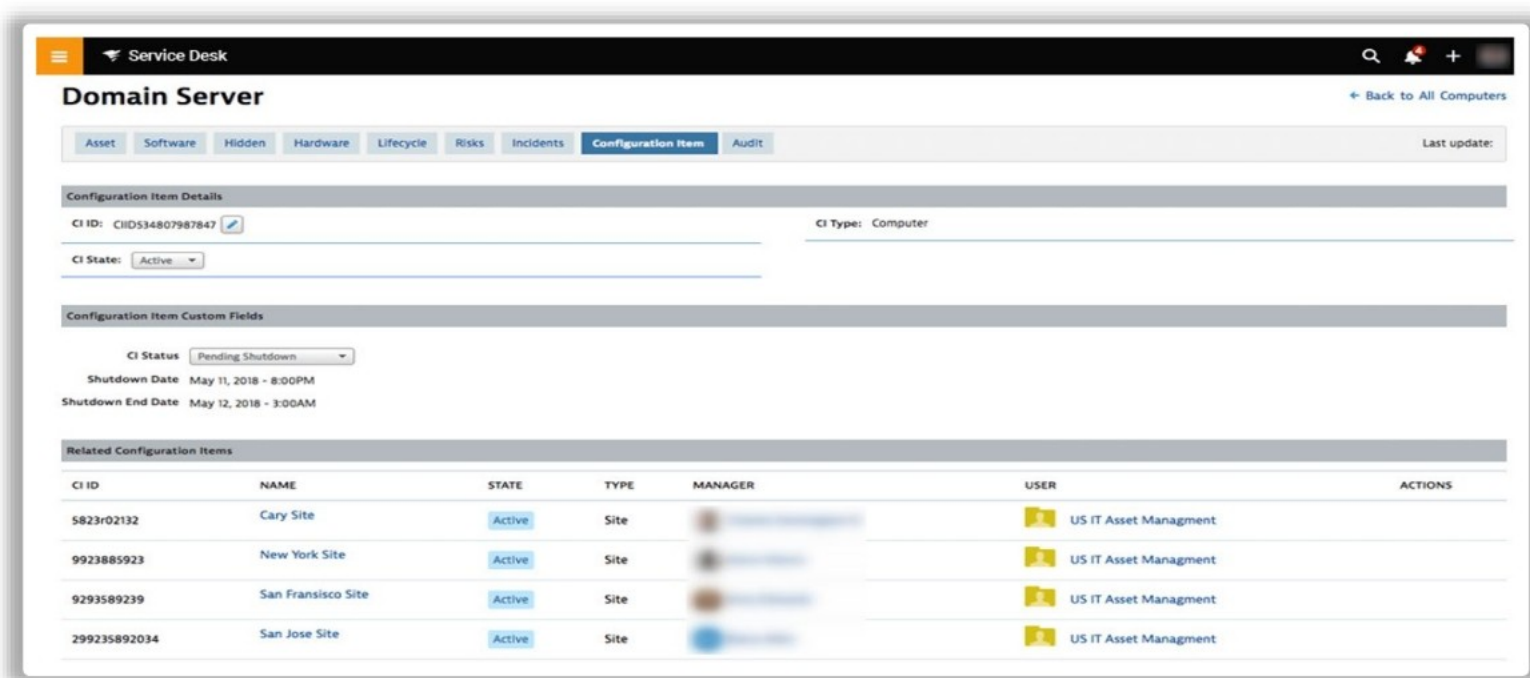


The screenshot shows the 'Service Desk' interface with a table titled 'All Networked Devices'. The table has 7 columns: NAME, DEVICE TYPE, MAC ADDRESS, OS, LAST UPDATE, AGENT NAME, and HOST. It lists various devices including Microsoft Windows 7, 10, and XP, Ubuntu Linux, and Magento (webserver).

| NAME  | DEVICE TYPE      | MAC ADDRESS       | OS   | LAST UPDATE           | AGENT NAME | HOST |
|---|------------------|-------------------|--|-----------------------|------------|------|
| 012 Microsoft Windows 7 (64-bit) (moodle) 192.168.0.6 | Networked Device | 00:0c:29:f3:d0:58 | Microsoft Windows 7 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 033 Microsoft Windows 10 (64-bit)                     | Networked Device | 00:0c:29:92:00:ba | Microsoft Windows 10 (64-bit)              | May 13, 2019 - 3:20PM |            |      |
| 025 Microsoft Windows 7 (64-bit) (192.168.0.56)       | Networked Device | 00:0c:29:d8:10:23 | Microsoft Windows 7 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 024 Microsoft Windows 7 (32-bit)                      | Networked Device | 00:0c:29:3c:06:fc | Microsoft Windows 7 (32-bit)               | May 13, 2019 - 3:20PM |            |      |
| 020 Microsoft Windows Vista (32-bit)                  | Networked Device | 00:0c:29:4ccc:56  | Microsoft Windows Vista (32-bit)           | May 13, 2019 - 3:20PM |            |      |
| 031 Microsoft Windows 10 (32-bit)                     | Networked Device | 00:0c:29:62:ec:94 | Microsoft Windows 10 (32-bit)              | May 13, 2019 - 3:20PM |            |      |
| 010 Microsoft Windows XP Professional (32-bit)        | Networked Device | 00:0c:29:0f:e0:49 | Microsoft Windows XP Professional (32-bit) | May 13, 2019 - 3:20PM |            |      |
| 007 Ubuntu Linux (64-bit) (nagios) 192.168.0.19       | Networked Device | 00:0c:29:00:0d:36 | Ubuntu Linux (64-bit)                      | May 13, 2019 - 3:20PM |            |      |
| 003 Magento (webserver)                               | Networked Device | 00:0c:29:1f:82:f8 | Microsoft Windows 7 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 030 Microsoft Windows 8.1 (64-bit)                    | Networked Device | 00:0c:29:c0:a6:2d | Microsoft Windows 8 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 022 Microsoft Windows Vista (64-bit)                  | Networked Device | 00:0c:29:27:2e:5c | Microsoft Windows Vista (64-bit)           | May 13, 2019 - 3:20PM |            |      |
| 015 upwork 05 (windows 8.1) 192.168.0.54              | Networked Device | 00:0c:29:70:16:5c | Microsoft Windows 8 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 019 Microsoft Windows Vista (32-bit)                  | Networked Device | 00:0c:29:e2:2c:9c | Microsoft Windows Vista (32-bit)           | May 13, 2019 - 3:20PM |            |      |
| 026 Microsoft Windows 7 (64-bit)                      | Networked Device | 00:0c:29:ff:42:d5 | Microsoft Windows 7 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 002 Jenkins(Sprayable) 192.168.0.22                   | Networked Device | 00:0c:29:1e:da:21 | Microsoft Windows 7 (64-bit)               | May 13, 2019 - 3:20PM |            |      |
| 013 upwork 03 (windows xp pro) 192.168.0.52           | Networked Device | 00:0c:29:4a:22:ff | Microsoft Windows XP Professional (32-bit) | May 13, 2019 - 3:20PM |            |      |
| 028 Microsoft Windows 8.1 (32-bit)                    | Networked Device | 00:0c:29:8c:40:a8 | Microsoft Windows 8 (32-bit)               | May 13, 2019 - 3:20PM |            |      |
|   | Networked Device | 00:0c:29:40:0a:2d | Microsoft Windows XP Professional (32-bit) | May 13, 2019 - 3:20PM |            |      |
|   | Networked Device | 00:0c:29:ad:b3:43 | Ubuntu Linux (64-bit)                      | May 13, 2019 - 3:20PM |            |      |

Figure 2.8: Discovering Current Assets

- Offering a centralized overview of asset configurations.



The screenshot shows the 'Service Desk' interface with a 'Domain Server' configuration page. It includes tabs for Asset, Software, Hidden, Hardware, Lifecycle, Risks, Incidents, Configuration Item, and Audit. The 'Configuration Item' tab is selected, showing details for CI ID: CID534807987847, CI Type: Computer, and CI State: Active. Below this, there are 'Configuration Item Custom Fields' including CI Status (Pending Shutdown), Shutdown Date (May 11, 2018 - 8:00PM), and Shutdown End Date (May 12, 2018 - 3:00AM). At the bottom, there is a table of 'Related Configuration Items'.

| CI ID        | NAME               | STATE  | TYPE | MANAGER | USER                  | ACTIONS |
|--------------|--------------------|--------|------|---------|-----------------------|---------|
| 5823r02132   | Cary Site          | Active | Site |         | US IT Asset Managment |         |
| 9923885923   | New York Site      | Active | Site |         | US IT Asset Managment |         |
| 9293589239   | San Francisco Site | Active | Site |         | US IT Asset Managment |         |
| 299235892034 | San Jose Site      | Active | Site |         | US IT Asset Managment |         |

Figure 2.9: Centralized Overview of Asset Configurations



## Other Asset Management Tools



|  |   |
|--|---|
|  <b>ServiceNow</b><br><a href="https://www.servicenow.com">www.servicenow.com</a>                   |  <b>Lansweeper</b><br><a href="https://www.lansweeper.com/">https://www.lansweeper.com/</a>                      |
|  <b>IBM Maximo</b><br><a href="https://www.ibm.com/products/maximo">www.ibm.com/products/maximo</a> |  <b>AssetSonar</b><br><a href="https://www.assetsonar.com/">https://www.assetsonar.com/</a>                      |
|  <b>SyAMsoftware</b><br><a href="https://syamsoftware.in">syamsoftware.in</a>                      |  <b>ManageEngine AssetExplorer</b><br><a href="https://www.manageengine.com/">https://www.manageengine.com/</a> |

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Other Asset Management Tools

The other asset management tools are as follows.

### ServiceNow

**Source:** <https://www.servicenow.com/>

ServiceNow automates the end-to-end lifecycle for software licenses, hardware assets, and the cloud on one platform. It optimizes technology asset investments across software, hardware, and cloud. It helps in gaining visibility and automated workflows at every stage of the asset lifecycle. It aligns assets to business strategy. It mitigates risk with a single, real-time view across unlicensed software deployments, re-harvesting options, and automated steps to remediate a compliance issue.

### IBM Maximo

**Source:** <https://www.ibm.com/>

IBM Maximo is a fully integrated enterprise asset management (EAM) platform that uses advanced analytics tools and IoT data to improve operational availability, extend asset lifecycles, and optimize performance. It efficiently plans, schedules, dispatches, and tracks work using Maximo Scheduler. It enables field technicians to real-time access asset data on smart mobile devices, at the right place and time to get their work done. Maximo also manages the configuration of high-value, complex, and regulated asset lifecycles of each component.

### SyAMsoftware

**Source:** <https://syamsoftware.in>



SyAM's software simplifies the management of all devices across the network by bringing their configuration data to a centralized asset database using an Asset Management Dashboard to quickly access key data. It provides key asset information such as system hardware configuration, operating system configuration, applications, App Name Version, and asset data including location, function, last used, and user access time/date.

### **Lansweeper**

**Source:** <https://www.lansweeper.com/>

Lansweeper discovers all IT and IoT assets on the network without the need to install any software on the system. It eliminates blind spots by providing exhaustive visibility into every device, user, and software within the entire technology state. It also manages the asset lifecycle and documents critical information related to business criticality, network management, and IT service management. It consolidates all asset details in a centralized system of record and leverages vulnerability information from the NIST catalog, connected to the assets, to derive valuable vulnerability insights. Additionally, it has diagramming capabilities that enhance the experience of discovering and understanding the state of inventory.

### **AssetSonar**

**Source:** <https://www.assetsonar.com/>

AssetSonar maintains, tracks, and manages a single source of truth for the IT asset landscape. It tracks custody, location, and maintenance of IT assets across their hardware lifecycle, from acquisition to disposal. It also maintains a consolidated view of installed and cloud software licenses through automated Agent-based scans and integrations with Google Workspace and Okta User Directories. It assigns software license entitlements for employees and runs software reconciliation to monitor both assigned and unassigned software installations across employee devices.

### **ManageEngine AssetExplorer**

**Source:** <https://www.manageengine.com/>

ManageEngine AssetExplorer is a web-based ITAM software that assists in monitoring and managing assets in the network throughout their entire lifecycle, from the planning phase to the disposal phase. It effectively manages both software and hardware assets, ensuring software license compliance, and tracking purchase orders and contracts. AssetExplorer is very easy to install and operate seamlessly right out of the box.





## Asset Management Best Practices

The best practices for asset management are as follows.

- **Establish policies and procedures:** An ITAM policy supplies a set of guiding standards, methods, goals, and intentions for effective management of an ITAM. Policy terms vary according to the company's needs. Effective policies are designed based on the below-listed components:
  - **Asset Standards:** To recognize specific IT assets to be used.
  - **BYOD guidelines:** To create methods for supporting "Bring Your Own Devices".
  - **Security guidelines:** To propose guidelines that provide security for physical and logical hardware and software assets.
  - **Software licensing guidelines:** To track laws and regulations, asset licensing, and ensuring compliance with all related agreements.
  - **Configuration standards:** To find how standardized software and hardware, assets are to be configured.
  - **Technical support and maintenance practices:** To describe the processes for service dispatch, preventive maintenance, technical support, problem escalation, and asset-related pairings.
  - **Configuration management guidelines:** To maintain consistent, updated configuration, and prompt changes as needed, it is important to define associated practices for asset configuration management and change control.



- **Asset move, add, and change practices:** To monitor requests for and actions involving transfers, modifications, and physical additions concerning allocating both software and hardware.
  - **Asset disposal guidelines:** To determine the procedures to be used when hardware and software assets are no longer needed and are to be disposed of as applicable.
- **Conduct regular internal audits:** By conducting regular audits, ensure that IT is under control. The benefits of regular internal auditing are as follows.
  - In IT infrastructure, it reduces existing discrepancies
  - It serves as an early warning system
  - It helps in avoiding penalties and fines
- **Use automated tools:** Employ these tools for the automatic detection of hardware, software, and network assets. These insights help businesses make smart decisions and optimize their ROI.
- **Establish a centralized asset repository:** A centralized asset repository accounts for all the hardware and software inventory in ITAM. It serves various IT infrastructure library functions such as incident management, service level management, configuration management, and problem management. This repository comprises discovery of all hardware and software components, capturing essential details including the type of asset, specification, etc.
- **Implement asset lifecycle management:** Asset lifecycle management is a continuing process of ensuring that the assets are tracked and used to their full capacity. It helps in increasing the organization's productivity by helping in making decisions on the IT needs and services. When an asset expires, it helps in purchasing decisions by examining several resources and lifecycle stages of an asset. It helps in viewing history and maintenance data that include downtime and costs.
- **Optimize asset usage:** Optimize asset usage by quantifying the total value of unused hardware and software applications. ITAM optimizes the usage of IT assets of the organization to minimize waste. This optimization reduces the extra maintenance costs and improves efficiency.
- **Ensure compliance:** Compliance ensures that the organization follows the rules made by authorities and the government. It aids businesses in ensuring that IT assets adhere to rules and requirements. It also helps in licensing agreements of software, thereby avoiding costly penalties for non-compliance.
- **Monitor security risks:** Monitoring provides an overview of all the assets, thereby reducing data risks. Ensuring the safety of the organization's data by tracking assets that might be vulnerable to hacking or theft.
- **Document and track changes:** Track and document IT assets activities such as hours of use, location, changes made to the asset, and modifications. Continuously monitor and



document these changes in the database, With immediate notification if any significant changes are noticed.

- **Continuous improvement:** For continuous improvement, use different scanning techniques to keep refreshing the asset database. Schedule automatic scans to track changes to the asset database. These changes comprise the deletions and modifications made to the asset database. For continual improvements, activities such as new purchases, newly leased equipment, and assets scanned from a newly acquired facility need to be added to the asset database.





### LO#07: Learn how to stay up to date on security trends and threats

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## **LO#07: Learn How to Stay Up to Date on Security Trends and Threats**

The current cyber security landscape is rapidly evolving. Staying on top of all the cyber security information, having knowledge of the latest security trends and staying aware of changing threat information is evident. This section explains the importance of staying up to date and the different ways to stay up to date on security trends and threats.



## Staying Up to Date on Security Trends and Threats



- To strengthen the cyber security posture of the organization, it is necessary to stay **up-to-date** on security trends and threats

### Methods to Stay Up-to-Date on Security Trends

- Follow cyber security news sources
- Participate in cyber security conferences and webinars
- Join cyber security communities and groups
- Follow-up with cyber security reports and research
- Actively participate in security Competitions
- Build a network with security professionals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Staying Up to Date on Security Trends and threats

The world of security is dynamic and ever-changing, requiring continuous learning and adaptability. An organization needs to stay up to date to ensure that its security measures are effective in protecting against the most recent cyber threats, physical attacks, and other risks. To strengthen the cybersecurity posture of the organization, consider the following methods to stay up to date on security trends and threats:

- Follow cybersecurity news sources
- Participate in cybersecurity conferences and webinars
- Join cybersecurity communities and groups
- Keep up with cybersecurity reports and research
- Actively participate in security competitions
- Build a network with security professionals



## Follow Cyber Security News Sources





- Get the latest updates on cyber security trends by **regularly visiting** reputed websites and blogs focusing on latest updates on security breaches, vulnerabilities, and emerging threats
- Some popular cyber security news sources are as follows:



Cyber Security News Sources

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Follow Cyber Security News Sources

Get the latest updates on cybersecurity trends by regularly visiting reputable websites and blogs that focus on the latest updates on security breaches, vulnerabilities, and emerging threats.

A few popular cybersecurity news sources are as follows:

- **www.itsecurityguru.org**

The IT Security Guru is a cybersecurity news source that offers a daily news digest featuring all the top IT security stories you need to know. The aim is to make IT security news interesting and digestible through Cyber Bites and Insight sections, which feature the most interesting and creative voices in the security world. It also features interviews with leading IT security experts and provides video content, delivering top trending IT security news stories every morning.

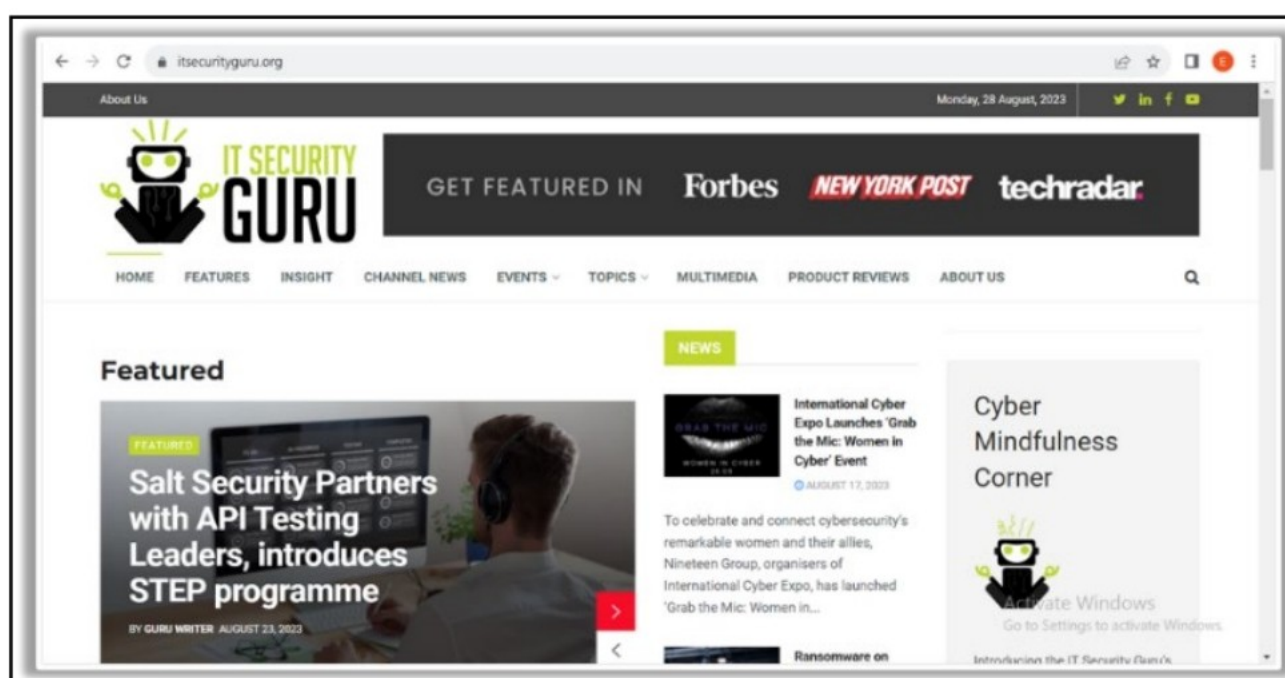


Figure 2.10: Cybersecurity News Source - IT Security Guru



- **www.darkreading.com**

Dark Reading is a cybersecurity news site dedicated to connecting the cybersecurity community. It comprises thought leaders, Chief Information Security Officers (CISOs), and technology experts, as well as thousands of other professionals. The site enables enterprise security staff and decision-makers to learn about emerging cyber threats, vulnerabilities, and technology trends, and offers potential defenses against the latest attacks and key technologies and best practices that could help protect their most valuable information in the future.

Dark Reading has 14 different sections that delve deep into enterprise security issues, covering topics like analytics, attacks & breaches, application security, cloud security, endpoints, information, and communication systems, ICS/OT, IoT, operations, perimeters, physical security, remote workforce, risk, threat intelligence, and vulnerabilities and threats.



Figure 2.11: Cyber Security News Source - Dark Reading

- **www.danielmiessler.com**

Miessler is a highly-regarded cybersecurity specialist, consultant, and author who maintains a personal blog focused on cybersecurity.

- **www.thehackernews.com**

This site is the most popular and up to date source for breaking cybersecurity news, offering valuable insights into emerging threats and solutions.

- **www.infosecurity-magazine.com**

The site provides a wide range of free educational content, including a well-established webinar channel, white paper syndication programs, and industry-leading virtual conferences on cybersecurity topics.

- **www.csoonline.com**

Serving enterprise security decision-makers and users, this site delivers critical information needed to stay ahead of evolving threats and defend against criminal



cyberattacks. With content spanning from risk management to network defense to fraud and data loss prevention, CSO offers unparalleled depth and insight to support key decisions and investments for IT security professionals.

- **[www.lastwatchdog.com](http://www.lastwatchdog.com)**

The Last Watchdog operates in the computer network and security industry and is widely considered one of the top cybersecurity websites.

- **[www.schneier.com](http://www.schneier.com)**

Bruce Schneier, dubbed a “security guru”, runs a blog on computer security at [www.schneier.com](http://www.schneier.com).

- **[www.krebsonsecurity.com](http://www.krebsonsecurity.com)**

Krebs writes a daily blog focusing on cybercrime and computer security.

- **[www.nakedsecurity.sophos.com](http://www.nakedsecurity.sophos.com)**

Naked Security is a newsroom dedicated to providing the latest news, opinions, tips, and analysis on computer security and the internet.



## Participate in Cyber Security Conferences and Webinars



Participate in physical and virtual conferences to learn from experts about the latest **emerging threats**

### Popular Cyber Security Conferences

|  |   |  |  |   |   |
|--|---|--|--|---|---|
| <b>Black Hat USA</b><br>It takes place annually in Las Vegas and focuses on <b>hacking and security vulnerability</b> research. It features keynote speeches from industry leaders, hands-on training, high-quality presentations, engaging discussions, and workshops | <b>ENISA Cybersecurity Standardisation Conference</b><br>It is held in Brussels, Belgium, and focuses on EU <b>cybersecurity policies</b> and initiatives | <b>IOT Solutions World Congress</b><br>It is an annual conference that focuses on the <b>IoT and security</b> . It is held in Barcelona, Spain | <b>Cloud Expo Asia</b><br>It is an annual conference that focuses on the impact of <b>cloud computing</b> on businesses and society. It is held in Singapore. It covers keynote speeches, panel discussions, and workshops led by experts in the field | <b>DEF CON 31</b><br>It takes place in Las Vegas and <b>focuses on hacking</b> . It features talks and events, such as social engineering contests and lockpicking competitions | <b>RSAConference</b><br>It takes place annually in San Francisco and covers topics, including <b>risk management, compliance, cloud security, and mobile security</b> |
|--|---|--|--|---|---|

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Participate in Cyber Security Conferences and Webinars

Participating in conferences and webinars is an excellent way to stay informed about the latest emerging threats. Attending events organized by academics, communities, or businesses allows for networking with other professionals in the field and learning from the latest case studies, innovations, and research in cybersecurity. Webinars offer live or recorded presentations, discussions, demonstrations, and question-and-answer sessions on a variety of security topics, issues, and solutions.

### Examples of Popular Cyber Security Conferences

- **Black Hat USA:** Held annually in Las Vegas, this conference zeroes in on hacking and security vulnerability research. It offers keynote speeches from industry leaders, hands-on training sessions, high-quality presentations, and interactive workshops and discussions. Participants gain insights into the latest trends, techniques, and technologies in hacking and security.
- **ENISA Cybersecurity Standardization Conference:** Located in Brussels, Belgium, this conference is centered on EU cybersecurity policies and initiatives. It serves as a platform for professionals to discuss and share ideas on the latest developments in cybersecurity. Attendees include industry experts, researchers, and government officials.
- **IoT Solutions World Congress:** This annual conference in Barcelona, Spain, focuses on IoT and security. It covers a wide range of topics related to connected devices, systems, and their security, providing attendees with up-to-date trends and developments in the field.
- **Cloud Expo Asia:** Hosted in Singapore, this annual event explores the impact of cloud computing on businesses and society. Participants can expect keynote speeches, panel



discussions, and workshops led by field experts, covering the latest trends in cloud computing.

- **DEF CON 31:** Also taking place in Las Vegas, DEF CON is the world's oldest and largest cybersecurity conference. Known for its vibrant atmosphere, it features a variety of events such as social engineering contests and lockpicking competitions, in addition to talks that keep participants abreast of the latest trends in hacking.
- **RSA Conference:** Held annually in San Francisco, this conference covers a broad spectrum of topics including risk management, compliance, cloud security, and mobile security.
- **Secure World:** Targeting security professionals, this conference offers industry panels, breakout sessions, and networking opportunities with vendors and local security association chapters.
- **CyberSecurity Festival:** Hosted in Surrey, UK, the event delves into topics like the emerging cyber threat landscape, cyber insurance, diversity in the cyber sector, humanitarian sector cybersecurity, automation, and zero trust.
- **Gartner Security & Risk Management Summit:** Taking place in National Harbor, Maryland, US, this conference addresses a myriad of security areas, providing technological insights for professionals in software and data safety, cybersecurity operations, information security, and cyber and IT risk management.
- **Blue Team Con:** Held in Chicago, USA, this conference gathers executives, salespeople, IT experts, and students to discuss current cybersecurity issues.
- **Infosec World:** Located in Lake Buena Vista, Florida, this conference covers diverse topics such as DevSecOps, data protection, cloud security, incident response, governance, regulation, and compliance.
- **(ISC)<sup>2</sup> Security Congress:** This three-day event provides up to 18 CPE (Continuing Professional Education) credits, a variety of educational sessions, and career advancement opportunities. Topics covered include cloud, network, and software security.



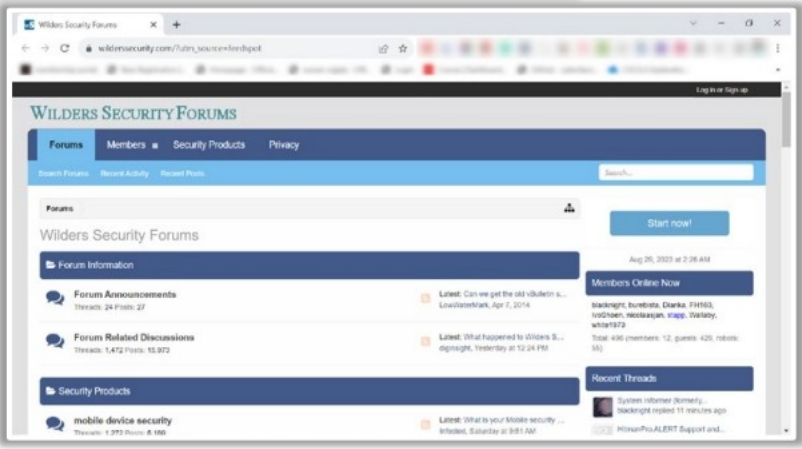
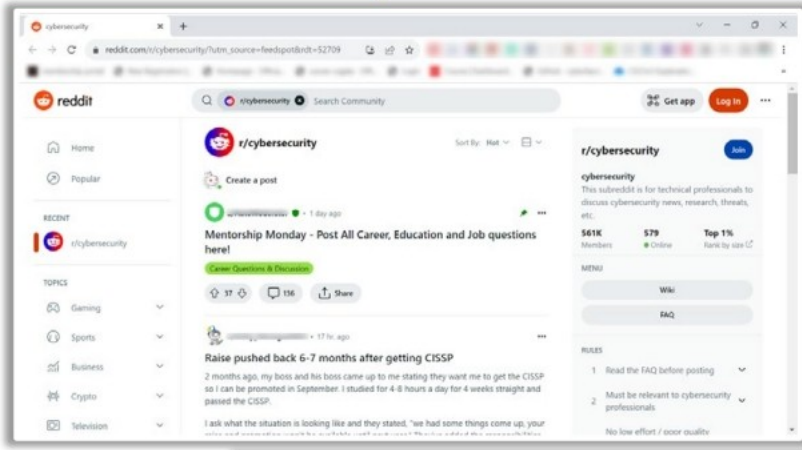
## Join Cyber Security Communities and Groups

The online forums and communities dedicated to cyber security are platforms to discuss and understand the **latest security trends**

Join these **communities** and **groups** to get opportunities to learn and share knowledge with other security professionals

A few of **popular** cyber security forums are:

- Reddit » Cyber security (OR) r/cybersecurity
- Reddit » Netsec (OR) r/netsec
- Reddit » Netsecstudents (OR) r/netsecstudents
- Bleeping Computer Forums
- Antionline Forums
- Spiceworks Community » Security Forum
- Hacklido
- ESET Security Forum » Malware Finding and Cleaning
- Wilders Security Forums
- MalwareTips Forum



reddit Cyber Security Forum

WILDERS SECURITY FORUMS Cyber Security Forum

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Join Cyber Security Communities and Groups

Online forums and communities focused on cybersecurity serve as platforms to discuss and understand the latest security trends. These spaces offer opportunities to learn from and share knowledge with other security professionals.

### Popular Cyber Security Forums

- **Wilders Security Forums:** It is an online chat room for people who want to know more about virtual safety and privacy. In the forum, you can find threads on Antivirus, Anti-malware, Encryption, Privacy, Mobile Security, Firewalls, Spyware, and many other topics. It also serves as a networking space. Users run polls, post updates and industry updates, and share their knowledge with thousands of security professionals. In addition, the forum is a vast content library. You can use the search bar to find almost every topic related to security and privacy. Members share both text and images. Users can join the forum for free and set up an account within minutes. Posting is only possible if a user has an account. However, users can view the forum without an account.



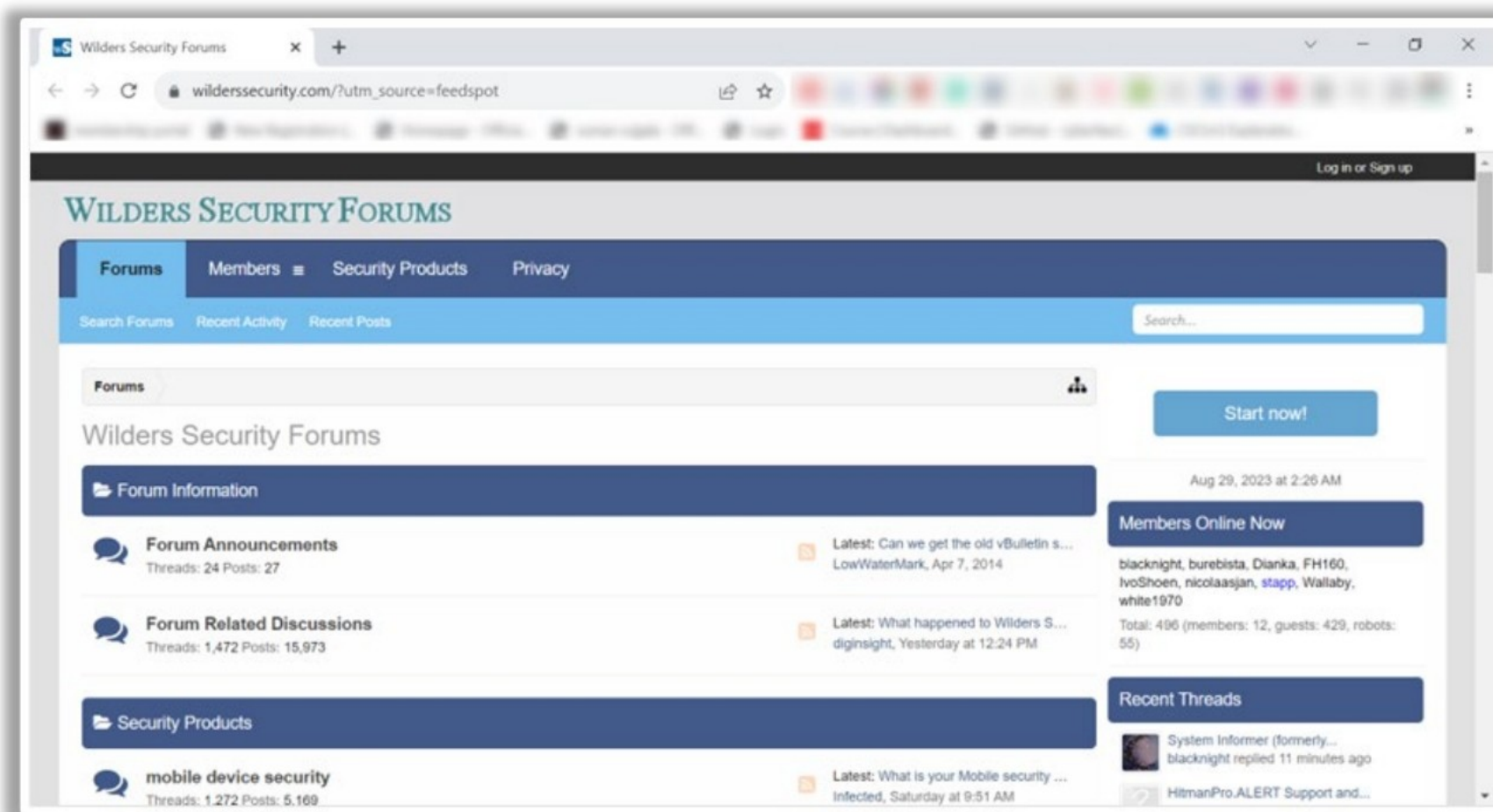


Figure 2.12: Cyber Security Community - Wilders Security Forums

- **Reddit » Cyber security (OR) r/cybersecurity:** Targeted at technical community members, this Reddit subsection discusses various cybersecurity topics and provides training on security certifications/courses such as Certified Network Security Specialist, AWS Cloud Certified, Fortinet Security Appliance, and Hack.me, IBM Security Learning Academy, and many more.

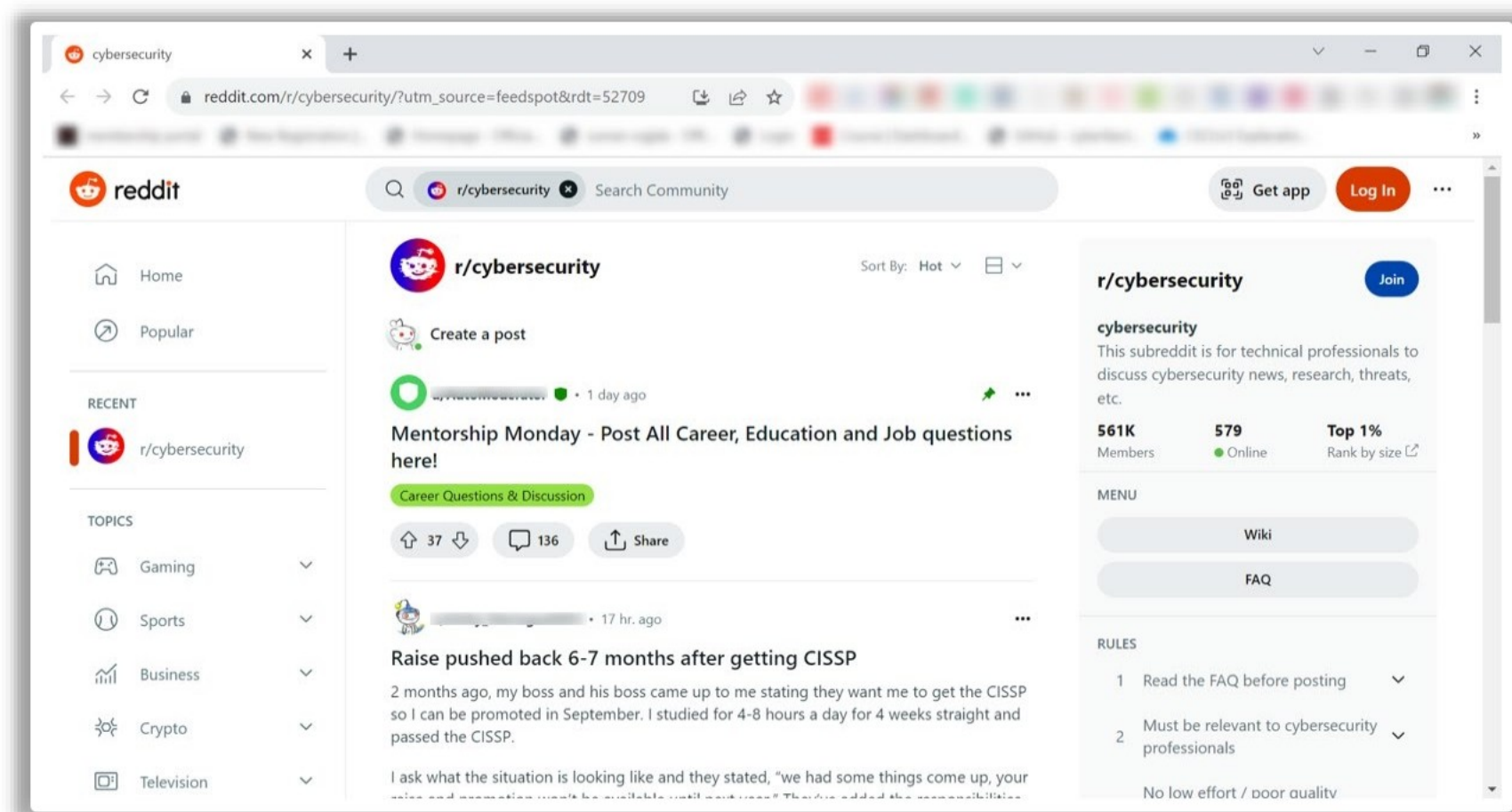


Figure 2.13: Wilders Security Forums - r/cybersecurity

- **Reddit » Netsec (OR) r/netsec:** This community-driven platform focuses on aggregating and disseminating content related to technical information security, catering to professionals, learners, and researchers worldwide.
- **Reddit » Netsecstudents (OR) r/netsecstudents:** This subreddit is a resource hub for network security topics, aimed at helping students share resources and ask questions.



- **Bleeping Computer Forums:** A community for people of all ages to learn, support each other, and solve problems.
- **Antionline Forums:** Here, discussions revolve around internet safety, with topics ranging from firewalls to wireless security.
- **Spiceworks Community » Security Forum:** These forums facilitate the exchange of information on IT security topics like Antivirus, Firewalls, and web content filtering.
- **Hacklido:** An open-source blogging platform for developers to connect with the global cybersecurity community.
- **ESET Security Forum » Malware Finding and Cleaning:** Run by ESET, a global security software company that helps protect computers from all kinds of cyber threats. They make security software for both home users and businesses all over the world.
- **MalwareTips Forums:** This community-based platform aims to provide the latest information and tools to combat malware and other cyber threats.

Share your own cybersecurity knowledge and insights through blog posts, articles, or presentations. This may benefit the members in the community in understanding the threats they face. Your knowledge sharing does not have to be only about cyber threats. For example, you may share security checklist that can help them for deploying a tool in their network, share best practices to secure their working environment, share different approaches and strategies of a cybersecurity concept, etc. All these may help their organizations to implement stronger defenses against modern cyber threats.

Leverage collaboration tools to join security-related channels and engage in real-time discussions. For example:

- **Slack:** This tool facilitates seamless collaboration with colleagues, much like in-person interactions, by bringing relevant people and information together.
- **Discord:** This app supports voice, video, and text chats, which allows to connect with communities and friends.



## Follow-up with Cyber Security Reports and Research

Study the periodically released reports from **reputed** security vendors and organizations

These reports help understand and analyze the latest **security trends** and provide insights into the **threat landscape**

Government cybersecurity agencies and Computer Emergency Response Teams (CERTs) such as US-CERT (United States), CERT-EU (European Union), and CERT-In (India) publish alerts, advisories, and reports about **current threats**



Example Cyber Security Reports and Research

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Follow-up with Cyber Security Reports and Research

Regularly consult reports from reputable security vendors and organizations to stay updated on the latest security trends. Government agencies and computer emergency response teams (CERTs) like US-CERT, CERT-EU, and CERT-In frequently publish alerts and advisories on current threats.

Cert-In performs various roles in cybersecurity, including:

- Issuing forecasts and alerts for cybersecurity incidents.
- Providing emergency measures for handling cyber security incidents.
- Publishing advisories, guidelines, and whitepapers on cybersecurity best practices.

### Examples of Cyber Security Reports and Research

- **Cybercrime Magazine:** It formulates its own ground-up research. It synthesizes, vets, and researches from the most likely resources such as analysts, associations, industry experts, vendors, and media publishers to give readers a bird 's-eye view of cybercrime and cybersecurity industry.



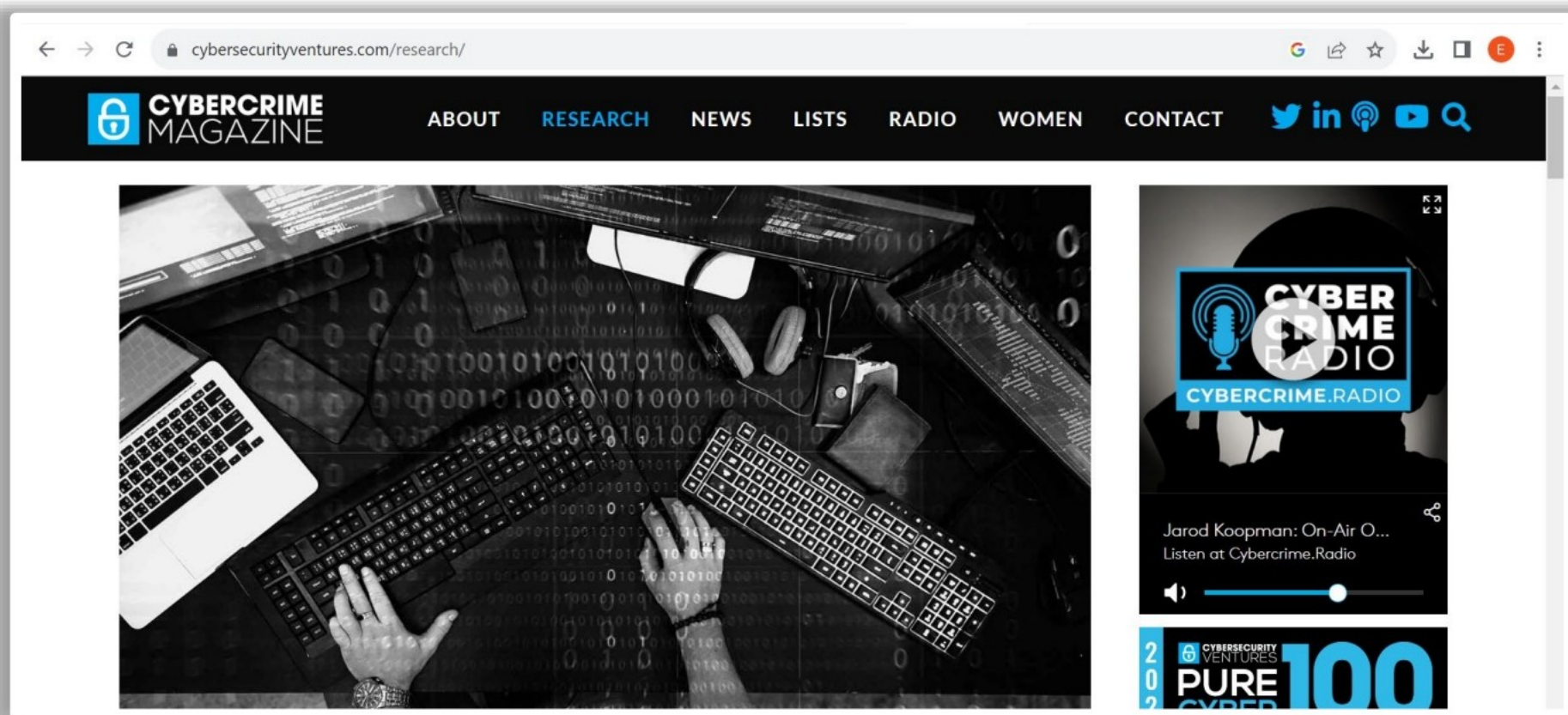


Figure 2.14: Cyber Security Reports and Research provided by Cybercrime Magazine

- **CrowdStrike Global Threat Report:** A highly-regarded annual intelligence brief, this report delves into the tactics of today's adversaries and what it takes to outmaneuver them. The report highlights trends, events across the cyber threat landscape, and notable themes.



Figure 2.15: Cyber Security Reports and Research provided by CrowdStrike



- **BlackBerry Global Threat Intelligence Report:** Serving as a key resource for cybersecurity professionals globally, this report helps to stay informed of the latest cybersecurity threats and challenges specific to different industries.

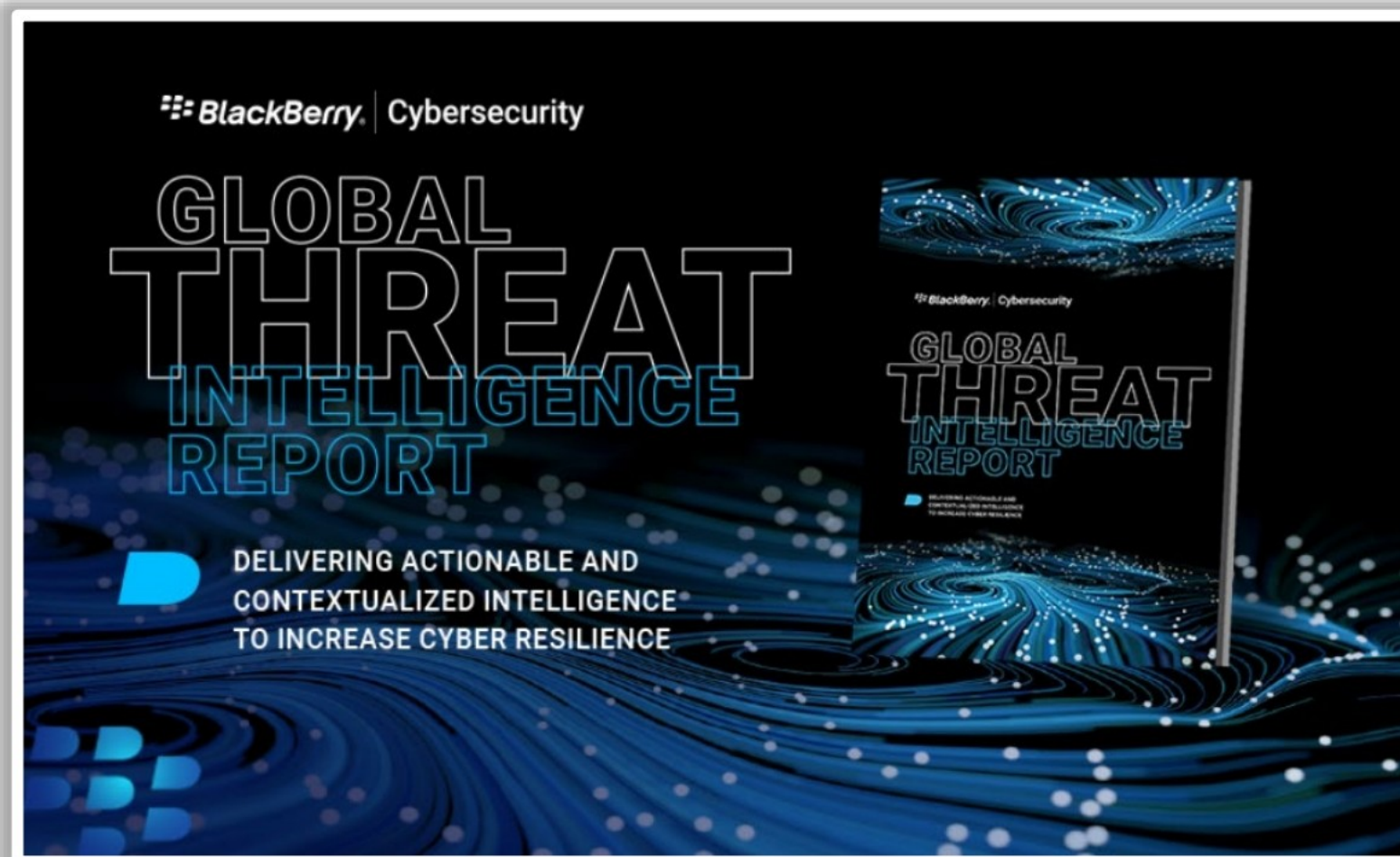


Figure 2.16: Cyber Security Reports and Research provided by BlackBerry

- **Trend Micro:** This cybersecurity threat report focuses on major security concerns that are currently surfacing and prevailing, discusses how cybercriminals, specifically ransomware actors, are taking their cue from legitimate organizations when it comes to diversifying their portfolios and rebranding their image. It also lists the top vulnerabilities that malicious actors have abused.



Figure 2.17: Cyber Security Reports and Research provided by Trend Micro



## Actively Participate in Security Competitions



Participating in **cybersecurity competitions**, such as the National Cyber League (NCL) Games, gives opportunities to prepare and validate your skills understand your competency to face in **real-world** cybersecurity challenges

Source: <https://nationalcyberleague.org/>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


### Actively Participate in Security Competitions

Participating in security competitions is a proactive approach to enhance understanding of the ever-evolving landscape of cyber security. This provides a practical avenue for cyber enthusiasts and professionals to stay up to date on the latest security threats. These competitions often simulate real-world scenarios, challenging participants to apply their skills to solve intricate problems and addressing vulnerabilities.

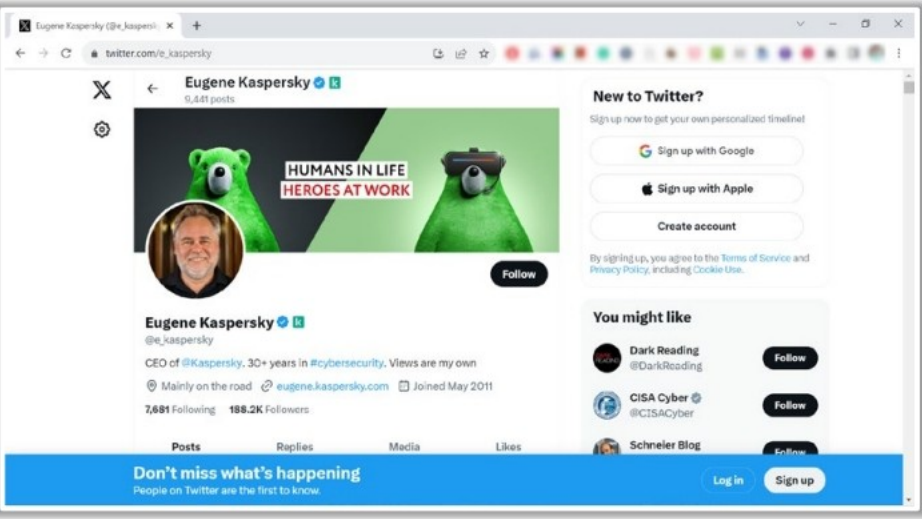
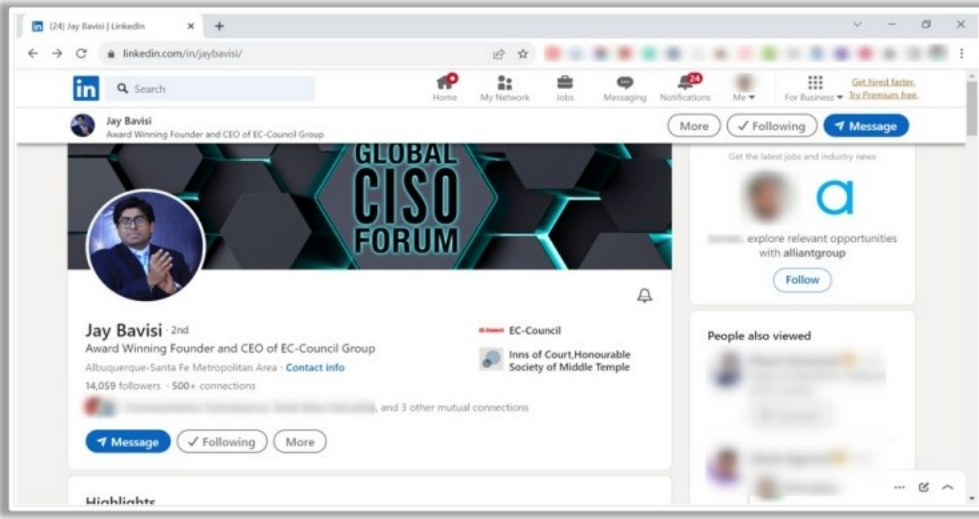
The collaborative aspect of these competitions adapts the participants to a sense of community and this shared pursuit of knowledge creates a platform for networking and knowledge exchange, allowing participants to learn from each other's experience, strategies, and their way of approach. This collective learning experience contributes significantly to overarching goal of staying ahead of security developments.



## Build a Network with Security Professionals



- Build a network with cyber security professionals to gain real-time knowledge about **vulnerabilities** and **emerging threats**
- Follow cybersecurity experts, researchers, and organizations on **social media platforms** such as Twitter, LinkedIn, and Reddit



A Few of Popular Security Professionals

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Build a Network with Security Professionals

Networking is pivotal for gaining real-time knowledge of vulnerabilities and emerging threats. Follow industry experts and organizations on platforms like Twitter, LinkedIn, and Reddit.

In a swiftly evolving field like cybersecurity, a professional network can be invaluable for staying up to date.

When engaging with security professionals, maintain a respectful and considerate demeanor. Building trust is essential for cultivating long-lasting professional relationships.



## Module Summary



- Security policies outline constraints using rules and regulations concerning every aspect of an organization's network security
- The security policy is an integral part of the Information Security Management Program for organizations
- Policy statements must be written in a very clear and formal style
- Information system security policy defines guidelines to safeguard an organization's information systems from malicious use
- A BYOD policy provides a set of guidelines to maximize business benefits and minimize risks while using an employee's personal device on an organization's network
- Security Policy Training and Awareness is required for effective implementation of security policies
- Stay up-to-date on security trends and threats to strengthen the cyber security posture of the organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Summary

In this module, you have successfully learned the various aspects in administrative security such as regulatory framework compliance, designing and developing security policies, training and awareness, staff hiring and leaving process, and employee monitoring.



This page is intentionally left blank.