

Security Principles for CCSM

Information Security Concepts and Governance



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



CCSM Certification Examination

Domains	Weights
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR), & Incident Response	10%
3. Access Control Concepts	22%
4. Network Security	24%
5. Security Operations	18%



What is security?



What Is Security?

Positive Viewpoint

Safety

Confidence

Trust

Not Positive Perspective

The security guard at the front door

Something that gets in the way of doing my job

Restrictions and passwords

“Not my job”



Security Principles for the CCSM Certification

Agenda:

**Information Security Concepts
and Governance**

Risk Management

Security Controls

(ISC)² Code of Ethics



Information Security Concepts and Governance



Governance



Accountability

Oversight

Leadership

- Communication and support for policy and procedures (making the theory 'real')



Information Assurance



Assurance is achieved through good practices

- Including security

Data and Information are two of the most valuable assets of most organizations

- Data must be protected throughout the data lifecycle
 - In all forms
 - At all times
 - In all places



Purpose of Information Assurance/Security

Comply with Laws and Regulations

Privacy – PII, PHI

GDPR

Health care

HIPAA

Financial

GLBA, SOx

Support business goals



Elements of Security



People



Technology



**Physical/
Environmental**

The 'right' people doing the 'right' things in the 'right' way



Key Points Review



Security supports business needs

- Provides assurance to management

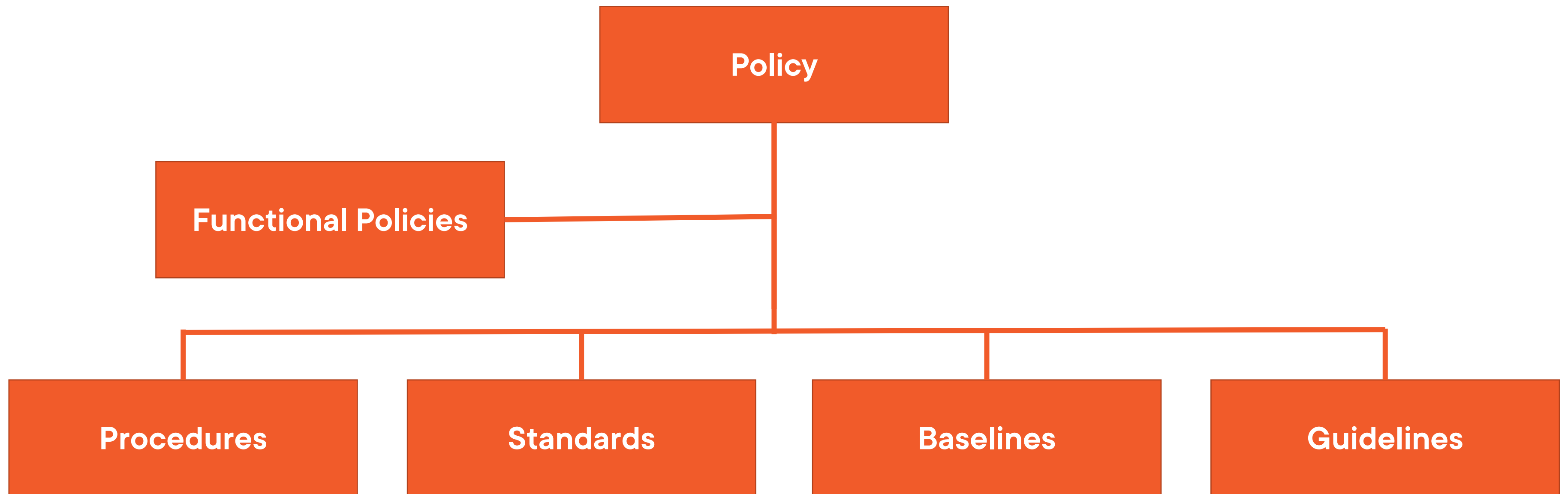
**Security consists of People, Technology,
and Physical/ Environmental**



Policy, Procedures, Standards, Baselines, and Guidelines



Policy Hierarchy



Policies



Provide direction

- Mandates what is and is not allowed

Signed by management

Example – acceptable use policy

Procedures

Mandate how something must be done

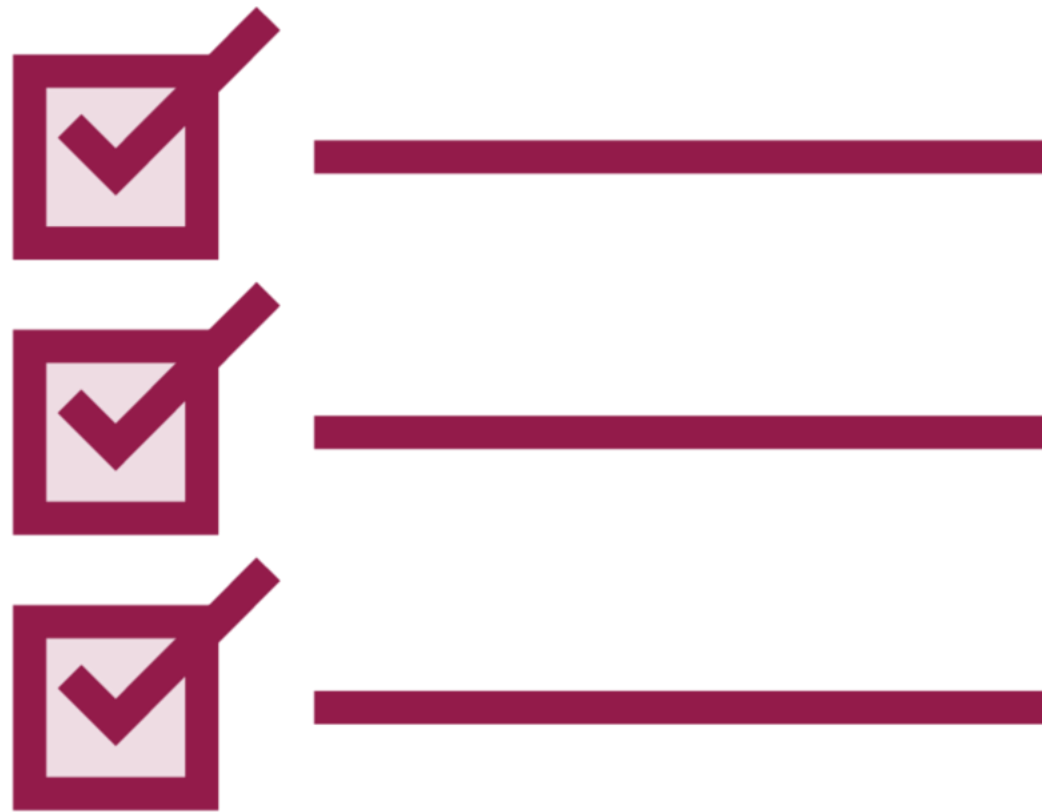
Provisioning new user access

Step-by-step actions

Enforce the intent of policy



Standards



Mandate required solutions

- Equipment purchases
- Compliance with good practices
 - ISO/IEC 27001 compliance





Baselines

Mandate minimum acceptable levels of action

- Equipment configuration
- Minimum password length





Guidelines

Recommendations not mandatory

- How to select a good password



Key Points Review



A policy is of no value if it is not supported by instructions of what to do and how to do it

The security policy demonstrates management's commitment to the information security program



The Information Security Triad



CIA



Confidentiality



Integrity



Availability

Used to define a complex term like 'security' in a meaningful way



Confidentiality



Protecting information from improper disclosure

- Privacy
 - Employee and customer data
- Secrecy
 - Trade secrets
 - Research
 - Marketing plans



Integrity

Preserving accuracy of data and data processing

Protection from improper modification

- Unauthorized users
- Users performing unauthorized functions



Authorized Entities



Ensuring that only authorized entities can access or modify data

- Authentication
 - Examined in Domain Three: Access Controls
 - Multi-factor Authentication (MFA)
 - Do not trust a single authentication technique

Availability

Ensuring that systems and data are accessible when required

Protection from destruction

Backups

Loss of access

DDoS attacks

Cut cables/equipment failure

Redundancy



Non-repudiation



Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.

NIST SP800-53 r5



Summary



This module set out the foundation for an information security program and the definitions for some key terminology

Security does not ‘just happen’, it must be managed with a strategy and actions to realize the strategy

