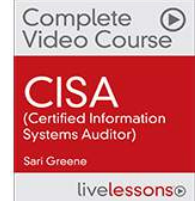


A large, light gray play button icon is positioned on the left side of the slide. It consists of a white right-pointing triangle centered within a series of concentric circles, all rendered in a light gray color.

Welcome

CISSP Crash Course - Part 1
January 17, 2018

Sari Greene - Intro



e: sari@sarigreen.com

t: [@sari_greene](https://twitter.com/sari_greene)

w: www.sarigreen.com

Polling Question – Who are you?

- I've just begun studying for the CISSP exam.
- I am in the mist of studying for the CISSP exam.
- I am almost ready to take the CISSP exam.
- I am already a CISSP.

CISSP Crash Course Objectives

If you have just begun studying:

- Immersion into the eight (ISC)² common body of knowledge (CBK) security domains.

If you are in the mist of studying:

- Assess your strengths and weaknesses and perhaps modify your study plan.

If you are almost ready to take your exam:

- Reinforce your knowledge and fill in some gaps.

If you are already a CISSP:

- Enhance your skillset.

Day 1 Crash Course Agenda

Segment 1: Domain 1 Security & Risk Management (85 minutes)

- Short break

Segment 2: Domain 2 Asset Security (30 minutes)

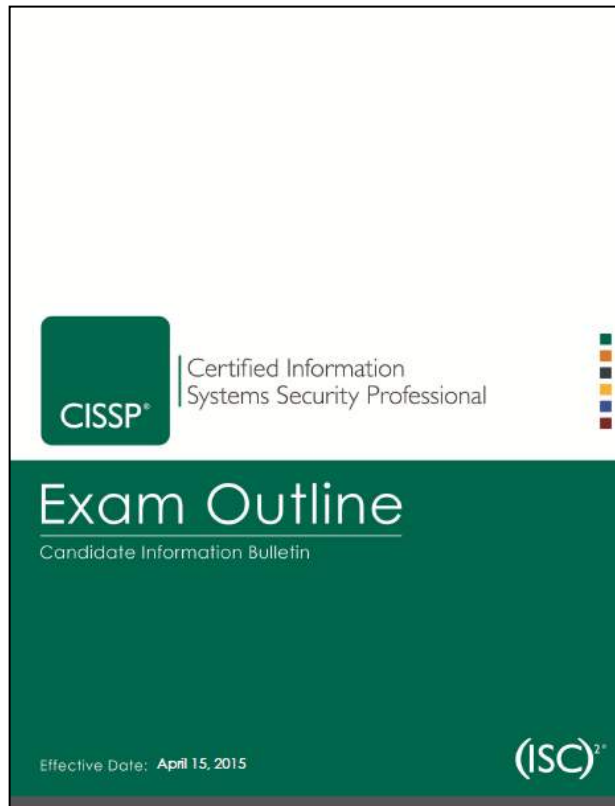
- Short break

Segment 3: Domain 3 Security Engineering (85 minutes)

- Short break

Segment 4: Test Taking Strategies (10 minutes)

Candidate Information Bulletin



This is a crash course and not a comprehensive course. We will touch on each of the objectives.

- My Complete CISSP 24hr. Video Course dives deep into every topic.
- My CISSP Exam Prep 7 hr. Video Course dives extra deep into challenging and/or unfamiliar topics.

Note: Revised exam scheduled to be released in April 2018. Current content is applicable.

New Test Format

Effective Dec. 18, 2017 (ISC)² introduced Computerized Adaptive Testing (CAT).

- This more precise evaluation reduces the maximum exam administration time from 6 hours to 3 hours, and it reduces the items necessary to accurately assess a candidate's ability from 250 items on a linear, fixed-form exam to as little as 100 items (to a maximum of 150) on the CISSP CAT exam.
- You cannot review a question.
- 25 unscored questions will be included.
- The exam content outline and passing standard for both versions of the examination are exactly the same. You still need to score 700 out of 1000 points. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format.

<https://www.isc2.org/Certifications/CISSP/CISSP-CAT>

A large, light gray play button icon is positioned on the left side of the slide. It consists of a white right-pointing triangle centered within a series of concentric circles, all rendered in a light gray color.

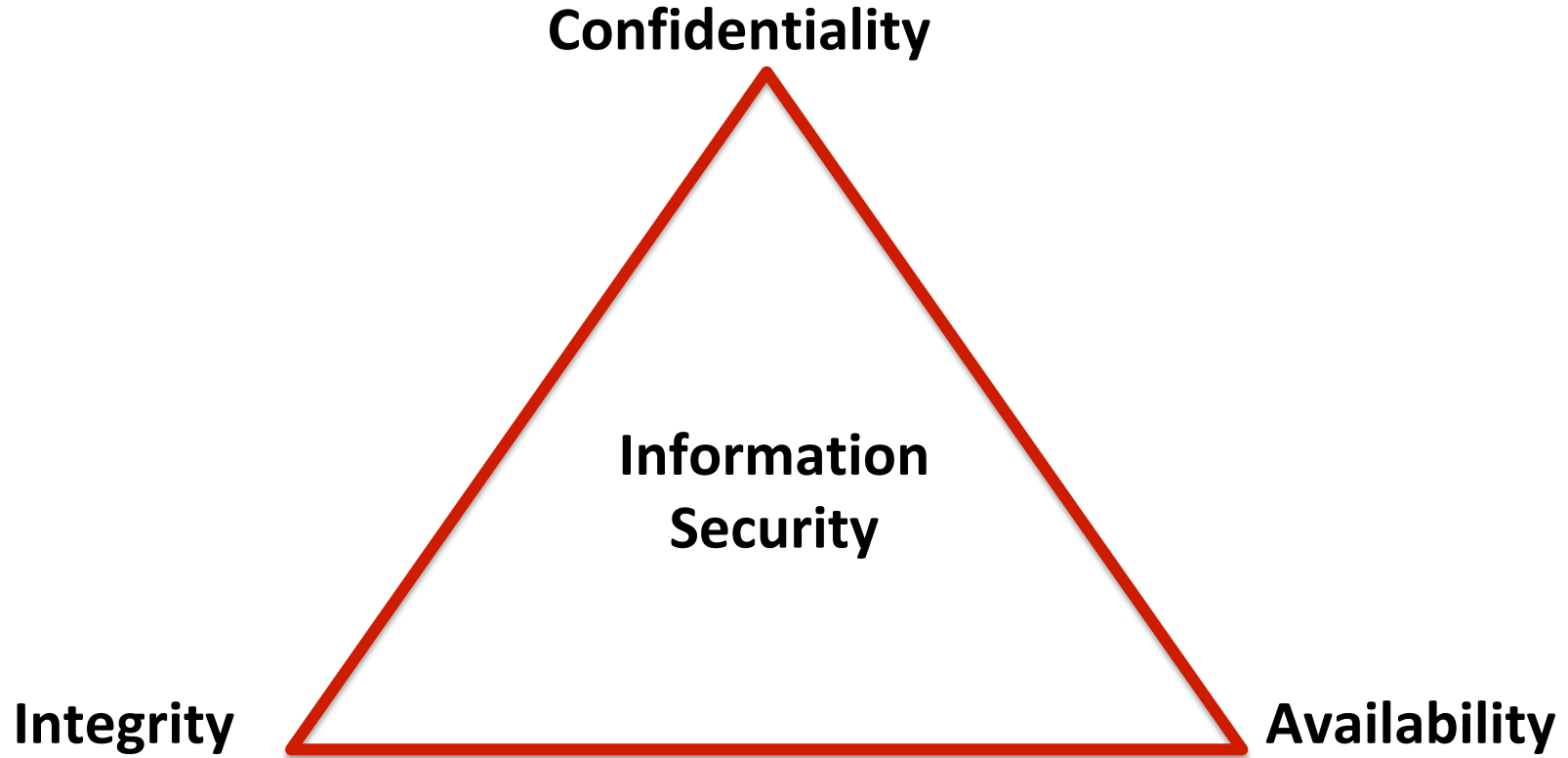
DAY 1 - Segment #1

Domain 1: Security and Risk Management

Domain 1 Security & Risk Management

A. Understanding and applying the concepts of confidentiality, integrity and availability	G. Understanding business continuity requirements
B. Applying security governance principles	H. Contribute to personnel security policies
C. Compliance requirements	I. Understand and apply risk management concepts
D. Legal and regulatory issues in a global context	J. Understand and apply threat modeling
E. Understanding professional ethics	K. Integrate security risk considerations into acquisition strategy and practice
F. Developing and implementing policies, standards, procedures	L. Establish and manage information security education, training and awareness

CIA Triad



CIA Principles

- *Confidentiality* is the principle that only authorized people, processes, or systems have access to information and that information must be protected from unauthorized disclosure.
- *Integrity* is the principle that data and systems should be protected from intentional, unauthorized, or accidental changes.
 - *Data integrity* implies information is known to be good, and that the information can be trusted as being complete, consistent, and accurate.
 - *System integrity* implies that a system will work as it is intended to.
- *Availability* is the principle that information and systems are operating and accessible when needed.

5 Supporting A's

Accountability	Accountability is the process of tracing actions to the source. In other word, who did what.
Authentication	Authentication is the positive identification of a person or system who is seeking access to information or to a system.
Authorization	Authorization is granting users and systems a predetermined level of access to resources.
Accounting	Accounting is the logging of access and uses of information resources.
Assurance	Assurance is the processes we use to develop confidence that our security measures are working as intended.

Strategic Alignment

It's time to bury the myth that security is an IT issue!

- Every information security decision must be informed by organizational goals and be in alignment with strategic objectives.
- When strategically aligned, security functions as a business enabler that adds value.

Governance and Leadership

As applied to information security, governance is the responsibility of leadership to:

- Determine and articulate the organization's desired state of security.
- Provide the strategic direction, resources, funding, and support to ensure that the desired state of security is achieved and sustained.

Due Care and Due Diligence

Due care is the standard of care that a prudent person would have exercised under the same or similar conditions.

- Actions taken by an organization to protect its stakeholders, investors, employees, and customers from harm.

Due diligence is defined as continued effort and activity.

- Act of investigating and understanding the threats and risks a company faces.

Downstream liability means your business is indirectly responsible for damages another business suffers.

- Downstream liability can apply when you owe a duty of care or service to another party including taking corrective action.

Compliance

Organizations are responsible for complying with all local, state, federal and union laws and regulations.

- Consideration should be given to local customs, traditions and practices (cultural, tribal and religious).

Think global, obey local. Jurisdiction is related to location of data and systems (processing, transmission, storage).

- Privacy and security regulations (or lack of)
- Access of local governments to stored or transmitted data
- Attitudes toward “foreigners”
- Law enforcement jurisdiction

Legislative & Regulatory Compliance

Regulation	Focus
GLBA (U.S.)	Security and privacy of financial records
HIPAA (U.S.)	Security and privacy of medical records
FERPA (U.S.)	Security and privacy of student educational records
COPPA (U.S.)	Security and privacy related to the online collection and use of data for minors under 13
State	Data protection requirements including encryption (x states) End of life destruction/disposal requirements (31 states and Puerto Rico) Data breach notification requirements (48 states, District of Columbia, Guam, Puerto Rico and the Virgin Islands)
Data Protection Directive / GDPR (EU)	Data protection for all individuals within the European Union. GDPR (General Data Protection Regulations – effective May 2018 also addresses the export of personal data outside of the EU.
Cookie Law (E.U)	Web cookies inform and consent requirements

Intellectual Property Law

Element	Protection
Patents	<i>Patents</i> are designed to protect an invention. The invention must be novel, not obvious, and has to provide some utility. A patentable invention must be something that can be produced.
Trademarks	A <i>trademark</i> is intended to protect recognizable names, icons, shape, color, sound, or any combination used to represent a brand, product, service, or company.
Copyrights	A <i>copyright</i> covers the expression of an idea rather than the idea itself (which is protected by a patent).
Trade secrets	<i>Trade secrets</i> refer to proprietary business and technical information, processes, designs, or practices that are confidential and critical to a business. Trade secrets don't require any registration and remain the only legal control for IP to remain undisclosed.

Privacy is the right of an individual to control the use of his personal information.

- Personal information (*PI*, *PII*, *NPPI*) may include discrete information such as a Social Security number, financial account number, password and PIN, driver's license number, passport number, medical record, educational records, and biometric data.
- Personal information can also include, but is not limited to, shopping habits, search engine queries, browsing history, email, pictures, location, and GPS travel.

Data Breach

An *security incident* is an event or action that endangers the confidentiality, integrity, or availability of information or information systems.

A *data breach* is when data is exfiltrated or extracted or there is a loss of control. A data breach may trigger reporting and notification requirements.

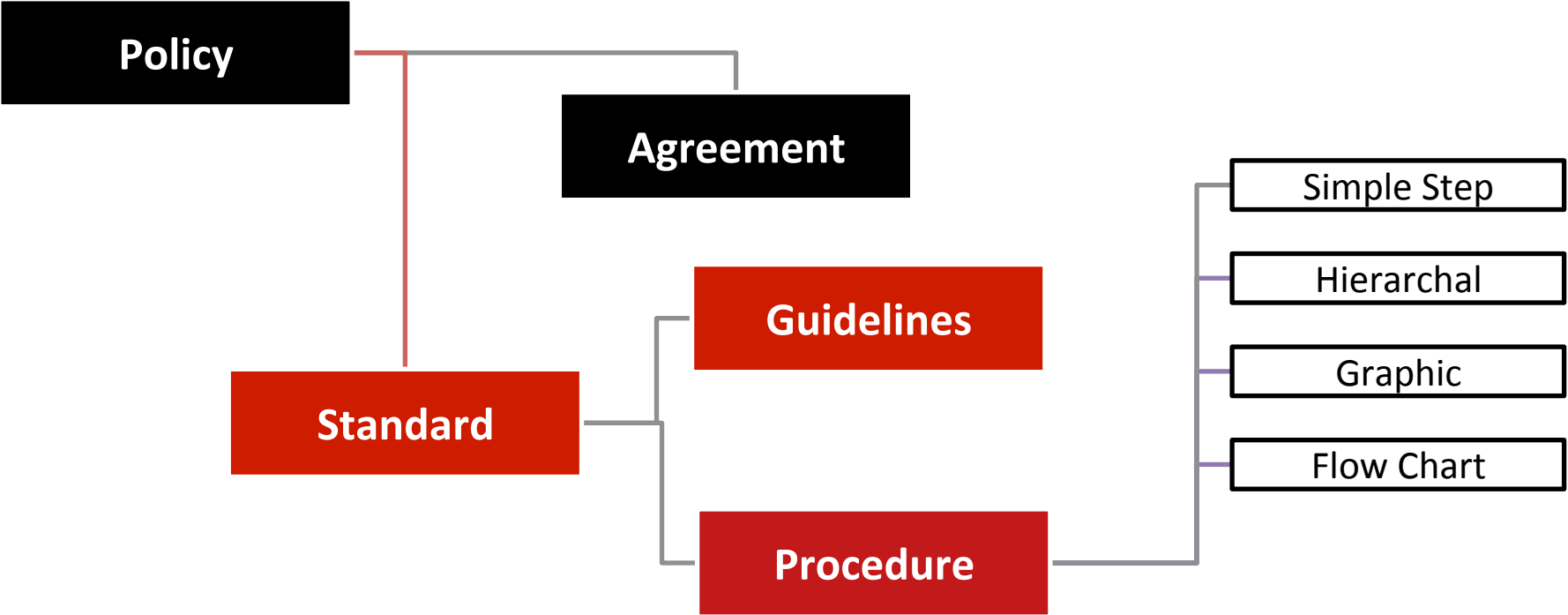
Professional Ethics

Organizational code of ethics (code of conduct).

Exercise (ISC)² Code of Professional Ethics.

- “Protect society, the common good, necessary public trust and confidence and the infrastructure. Act honorable, honestly, justly, responsibly, and legally. Provide diligent and competent service to principles. Advance and protect the profession.”

Governance Communication



Information Security Policies

The objective of a policy is to communicate management's expectations and requirements with the objective of providing direction.

- Information security policies codify the high-level requirements for protecting information and information assets and ensuring confidentiality, integrity, and availability.
- Every component of an information security program should have a corresponding policy and standards.
- Written information security policies may be a regulatory or contractual compliance requirement.

Standards, Baselines and Guidelines

Standards serve as specifications for the implementation of policy and dictate mandatory requirements.

Baselines are the aggregate of standards for a specific category or grouping such as a platform, device type, ownership, or location.

Guidelines help people understand and conform to a standard. Guidelines are customized to the intended audience and are not mandatory.

Procedures

Procedures are instructions for how a policy, standard, baseline, or guideline is carried out in a given situation. Procedures focus on discrete actions or steps, with a specific starting and ending point.

Four commonly used formats:

- Simple step
- Hierarchy
- Graphic
- Flowchart

Business Continuity

In its simplest form, business continuity is the capability of a business to operate in adverse conditions.

The objective of business continuity planning is to prepare for the continued operation of essential functions and services during disruption of normal operating conditions.

To support this objective:

- Essential services and processes are identified.
- Threat scenarios are evaluated.
- Response, recovery, and contingency plans are developed.
- Strategies, plans, and procedures are tested.

Business Impact Analysis

The objective of a *Business Impact Analysis (BIA)* is to identify essential services, systems, and infrastructure.

- *Essential* means that the absence of or disruption of services would result in significant, irrecoverable, or irreparable harm to the organization, employees, business partners, constituents, community, or country.

A Business Impact Analysis (BIA) is used by management to:

- make investment decisions.
- prioritize resources.
- guide the development of incident response, disaster recovery, and business contingency (continuity) plans.

Fundamental BIA Questions

The BIA process should answer the following questions.

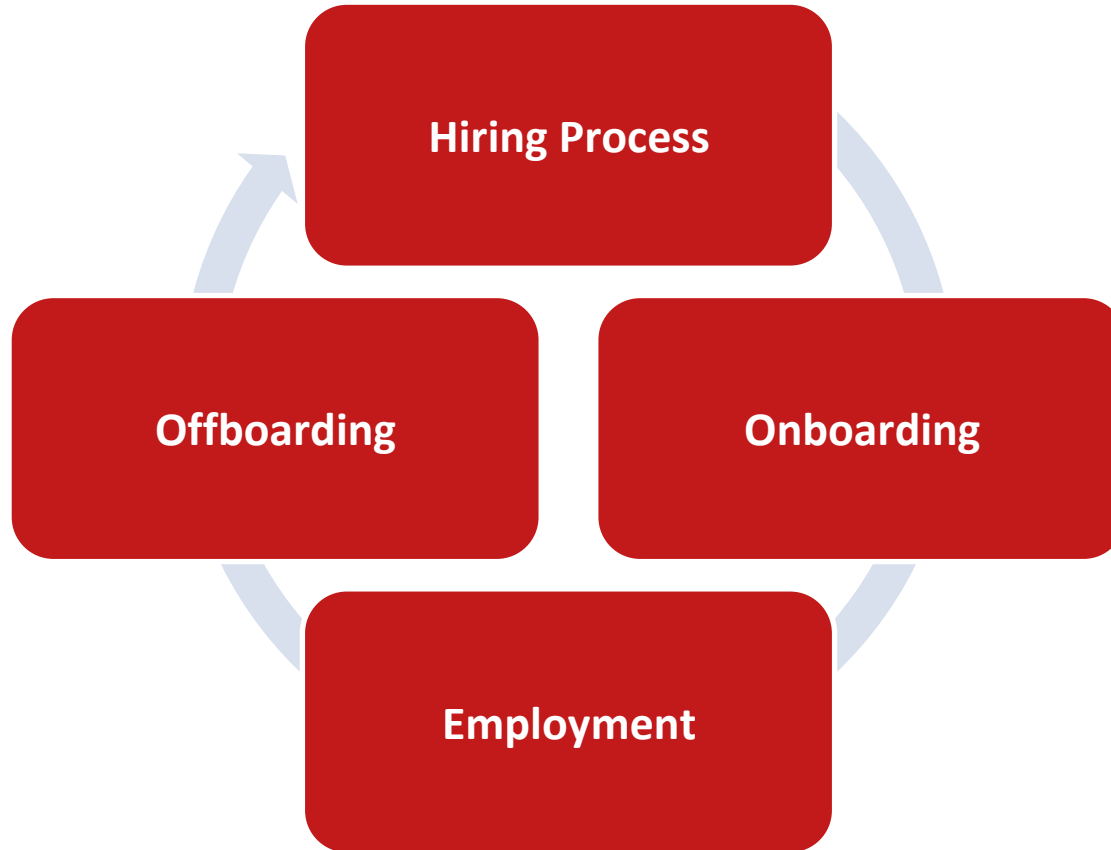
- What is the organization's essential business process?
- What is the impact of a disruption (e.g. life, property, safety, finance, reputation)
- What are the related resources and dependencies (including single point of failure)?
- What are the process, system, and data recovery requirements?

The outcome of BIA is a prioritized matrix of services, systems, and infrastructure.

Business Impact Metrics

Abbr.	Metric	Definition
MTD MTO	Maximum Tolerable Downtime Maximum Tolerable Outage	Maximum time a process/service can be unavailable without causing significant harm to the business
RTO	Recovery Time Objective	Amount of time allocated for system recovery <ul style="list-style-type: none">- Must be less than the maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business process
RPO	Recovery Point Objective	Acceptable data loss <ul style="list-style-type: none">- The point in time, prior to a disruption or system outage that data can be recovered

Employee Lifecycle (very simplified)



User Security Controls

Control	Description
Policy/Agreements	Confidentiality Agreement, Acceptable Use Policy and Agreement (AUP)
Training	Ongoing education, training and awareness programs
Job Rotation	Rotating assignments
Mandatory Vacation	Requiring employees to take a set amount of vacation time
Separation of Duties	Breaking a task into segments so that no one subject is in complete control
Dual Control	Requiring more than one subject or key to complete a specific task
Clean Desk	Requirement to never leave confidential data (paper, monitor, whiteboard) unattended or within view of unauthorized personnel

Personnel Agreements

Agreement	Objective
Confidentiality / Non-disclosure (NDA)	<p>Protects data from unauthorized disclosure</p> <ul style="list-style-type: none">• Establish data ownership• Protect information from disclosure• Prevent forfeiture of patent rights• Define handling standards including disposal
Acceptable Use Policy (AUP) Agreement	<p>Sets forth proper use of information systems, handling standards, monitoring, and privacy expectations</p> <ul style="list-style-type: none">• An AUP should be written in language that can be easily and unequivocally understood• By signing the associated agreement, the user acknowledges, understands, and agrees to the stated rules and obligations

Third-Party Relationships

Third parties include vendors, service providers, business partners, consultants, and contractors.

Third-party oversight activities include (but not limited to):

- Conducting a due diligence investigation related to service provider selection and subsequent business activities.
- Conducting a risk assessment to ensure that the relationship is consistent with the overall business strategy.
- Requiring nondisclosure agreements.
- Codifying service relationships.
- Monitoring the service provider through appropriate audits and tests.
- Coordinating incident response protocols and contractual notification.
- Reviewing on a scheduled basis third-party arrangement's performance and adherence to contractual obligations.

Third-party Agreements

Agreement Type	Objective
Confidentiality / Non-disclosure (NDA)	Protects data from unauthorized disclosure
Service Level Agreement (SLA)	Codifies service and support requirements
Interconnection Security Agreement (ISA)	Documents technical requirements
Memorandum of Understanding (MOU) Also known as a MOA	Cooperative agreement—often a pre-contract placeholder
Business Associate Agreement (BAA)	HIPAA related agreement to protect personal health information (PHI)
Business Partner Agreement (BPA)	Business relationship contract

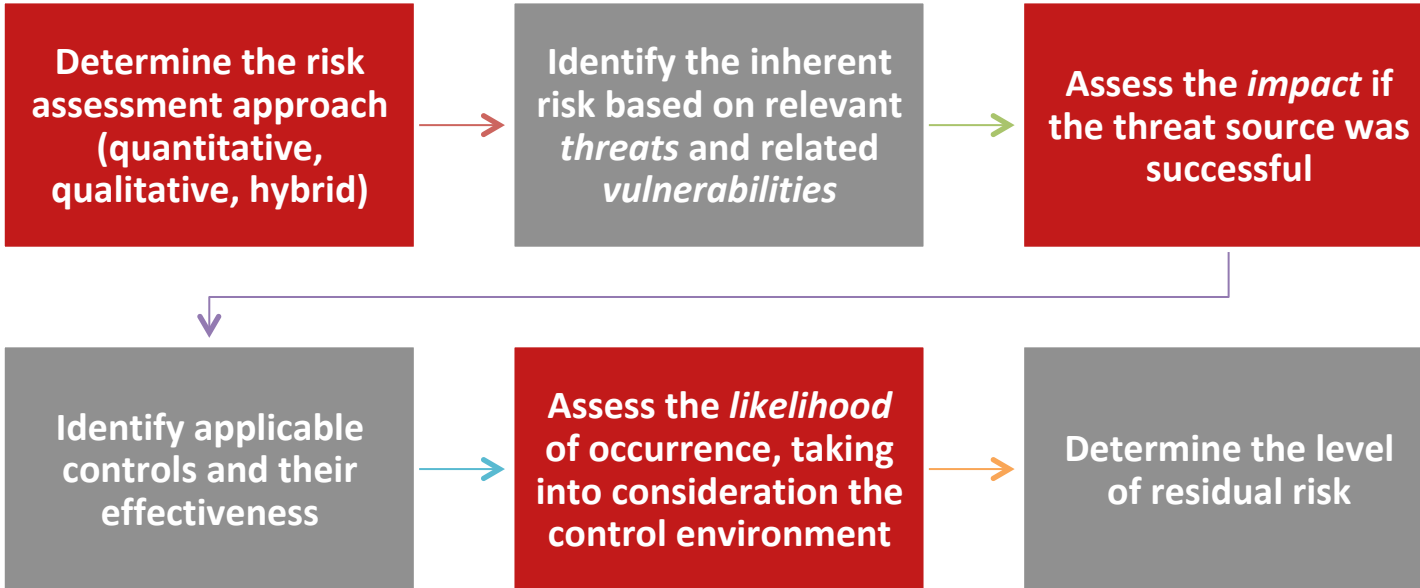
Risk is defined as uncertainty of outcome, whether positive opportunity or negative threat, of actions and events.

- *Risk assessment* evaluates the combination of the *likelihood* of occurrence, and the adverse *impact* if the circumstance or event occurs.
- *Risk appetite* is the level of risk that an organization is comfortable with.
- *Risk management* implies that actions are being taken to either mitigate the impact of a undesirable or unfavorable outcome and/or enhance the likelihood of a positive outcome (inline with the risk appetite).

I Risk Assessment Approaches

Qualitative	<i>Qualitative</i> risk assessments use descriptive terminology such as high, medium, and low or normal, elevated, and severe
Quantitative	<i>Quantitative</i> risk assessments assign numeric and monetary values to all elements of the assessment
Key elements of both are <i>likelihood of occurrence</i> and <i>impact</i>	

Risk Assessment Workflow



Quantitative Risk Assessment Elements


Quantitative risk assessment elements include:

- Asset value (AV) expressed in \$.
- Exposure factor (EF) expressed as a %.
- Single loss expectancy (SLE) expressed in \$.
- Annualized rate of occurrence (ARO) expressed as a #.
- Annualized loss expectancy (ALE) expressed in \$.

I Quantitative Formulas

Formulas	Example
$SLE (\\$) = AV (\\$) \times EF (\%)$ Single Loss Expectancy = Asset Value x Exposure Factor	Revenue from one hour of e-commerce is \$20,000 (AV). A DDoS attack could disrupt 85% (EF) of online activity. $\$20,000 (AV) \times .85 (EF) = \$17,000 (SLE)$ The cost of an hour of DDoS disruption is \$17,000
$ALE (\\$) = SLE (\\$) \times ARO (\#)$ Annualized Loss Expectancy = Single Loss Expectancy x Annualized Rate of Occurrence	Single Loss Expectancy (for an hour of DDoS disruption) is \$17,000. Based on the current threat and controls environment it is expected that there will be 5 hour(ARO) of DDoS disruption per year. $\$17,000 (SLE) \times 5 (ARO) = \$85,000 (ALE)$

Risk Treatment Options

Option	Description
Ignore	Act as if the risk doesn't exist 
Avoid	Eliminate the cause or terminate the associated activity
Mitigate	Reduce the impact or likelihood by implementing controls or safeguards
Share	Spread the risk among multiple parties
Transfer	Assign the risk to another party via insurance or contractual agreement (subject to legal and regulatory constraints)
Accept	Acknowledge the risk and monitor it

I Controls, Countermeasures, and Safeguards

A *control* (sometimes called the countermeasure or safeguard) is a tactic, mechanism, or strategy that either:

- Reduces or eliminates a vulnerability (weakness).
- Reduces or eliminates the likelihood that a threat agent will be able to exploit a vulnerability.
- Reduces or eliminates the impact of an exploit.

Control Classifications

Deterrent	Preventive	Detective	Corrective
Deterrent controls discourage a threat agent from acting.	Preventive controls stop a threat agent from being successful.	Detective controls identify and report a threat agent, action, or incident.	Corrective controls minimize the impact of a threat agent, or modify or fix a situation (recovery).
Note: A control can (and often does) have multiple classifications depending upon context			
Compensating	Compensating controls are alternate controls designed to accomplish the intent of the original controls as closely as possible, when the originally designed controls cannot be used due to limitations of the environment or financial constraints.		

I Control Implementations

	Administrative	Physical	Technical (Logical)
Description	Controls relating to the oversight, laws, rules, and regulations	Controls that can have a material structure (seen, heard, touched)	Controls provided through the use of technology and/or a digital device
Example	Policies, procedures, training, audits, compliance reporting	Gate, alarm, guard, barricade, door, lock, CCTV, ID card	Encryption, ACLs, firewall rules, anti-virus software, biometric authentication

J Threat Primer

Term	Description
Threat	Potential danger
Threat Actor	Adversaries with malicious intent
Vulnerability	A weakness in a system, process or person
Exploit	Successfully taking advantage of a vulnerability
Targeted Attack	Threat actor chooses a target for a specific objective
Opportunistic Attack	Threat actor takes advantage of a vulnerable target (not previously known to them)
Incident	Event that compromises the confidentiality, integrity, and/or availability of information or information system
Threat Modeling	Approach to identifying and categorizing potential threats

J Threat Modeling

Threat modeling is an approach to identifying and categorizing potential threats:

- *Attacker-centric* threat models starts with identifying an attacker and the evaluates the attacker's goals and potential techniques.
- *Architecture-centric* threat models focus on system design and potential attacks against each component.
- *Asset-centric* threat models begin by identifying asset value and motivation of threat agents.

J Threat Analysis

	Question	Factor
1	Why would an adversary target my organization?	Motivation
2	How hard would it be for an adversary to achieve their objective?	Workfactor
3	Are we aware of the latest threats, tools, and techniques?	Threat Intelligence
4	Would we know if we were being attacked?	Threat Detection
5	Are we prepared to respond to an attack?	Resiliency

Attack Vectors

Category	Description
Social Engineering	Disruption, manipulation, or compromise of human beings
Application and Service	Disruption, manipulation, or compromise of network or host transmission, services, application, or data
Wireless	Disruption, manipulation, or compromise of wireless transmission or devices
Cryptographic	Disruption, manipulation, or compromise of cryptographic algorithms, protocols, services, applications, or data
Hardware	Disruption, manipulation, or compromise of hardware/firmware elements

Controls are typically applied in multiple layers because no one control can protect an asset from every type of threat:

- This architecture is referred to as *defense in depth* or *layered security*.

Supply Chain Risk Management

Critical supply chain vendors and service providers should be included in the organizational risk management program.

Expectations must be communicated.

- Use clear and consistent language in describing security requirements and expectations.
- Provide baseline security requirements for products and services.
- Embed requirements in contracts and service-level agreements.

Supply Chain Assurance

Assurance mechanisms include due diligence, inspection, assessment, and audit reports.

- Most common information technology and security related independent audit report is a AICPA SSAE 18 SOC (formally SAS70 / SSAE 16).

Shared Responsibility

No individual, business, or government entity is solely responsible for cyber security. Everyone has a role to play.

- It is important to keep in mind that most individuals either aren't aware of potential dangers and/or security and privacy best practices.
- On-going education is essential.
- Educational programs should stress that individual actions matter and that adherence to best practices, policies, and regulations are critical (and expected).
- Educational programs should be tailored to roles and audience.

The NISA SETA Model

SETA - Security Education, Training, and Awareness

Security	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Awareness
Teaching Method	Discussion , seminar, reading	Lecture, case study, hands-on	Interactive, video, posters, games
Test Measure	Essay	Problem solving	True or false, multiple choice
Impact Timeframe	Long-term	Intermediate	Short-term

Domain 1 Security & Risk Management

A. Understanding and applying the concepts of confidentiality, integrity and availability	G. Understanding business continuity requirements
B. Applying security governance principles	H. Contribute to personnel security policies
C. Compliance requirements	I. Understand and apply risk management concepts
D. Legal and regulatory issues in a global context	J. Understand and apply threat modeling
E. Understanding professional ethics	K. Integrate security risk considerations into acquisition strategy and practice
F. Developing and implementing policies, standards, procedures	L. Establish and manage information security education, training and awareness

Assessment Q1

Which statement best describes data integrity?

- A. The system works as intended.
- B. Code is bug free.
- C. Resource utilization is logged and monitored.
- D. Information can be trusted to be complete, consistent and accurate.

Assessment Q2

At a minimum, this employee agreement should include rules for how to interact with information systems, sanctions for violations, and incident reporting instructions.

- A. Acceptable Use Policy Agreement
- B. Non-disclosure Agreement
- C. Employment Agreement
- D. Confidentiality Agreement

.

Assessment Q3

Which statement below does not describe a control?

- A. A tactic or strategy that reduces or eliminates vulnerability.
- B. A tactic or strategy that reduces or eliminates likelihood of exploit.
- C. A tactic or strategy that reduces or eliminates impact of exploit.
- D. A tactic or strategy that reduces or eliminates expense.

Assessment Q4

Which of the following quantitative risk assessment formulas is true?

- A. $AV = EF * \text{Cost of Asset}$
- B. $ALE = SLE * ARO$
- C. $SLE = EF * ARO$
- D. $ARO = EF * SLE$

Assessment Q5

Maximum tolerable downtime (MTD) relates to _____.

Recovery point objectives (RPO) relates to _____.

- A. business functions, system resources
- B. system resources, data loss
- C. length of outage, system resources
- D. business functions, data loss

Break Time

10 minute break!

A large, light gray play button icon with a white triangle pointing right, centered within a circle. The circle has a thick white border and a gray shadow.

DAY 1 Segment #2

Domain 2: Asset Security

Domain 2 Asset Security

A. Classify information and supporting assets (e.g. sensitivity, criticality)	D. Ensure appropriate retention (media, hardware, personnel)
B. Determine and maintain ownership (e.g. data owners, system owners, business/mission owners)	E. Ensure data security controls (e.g. data at rest, data in transit)
C. Protect privacy	F. Establish handling requirements (markings, labels, storage, destruction of sensitive information)

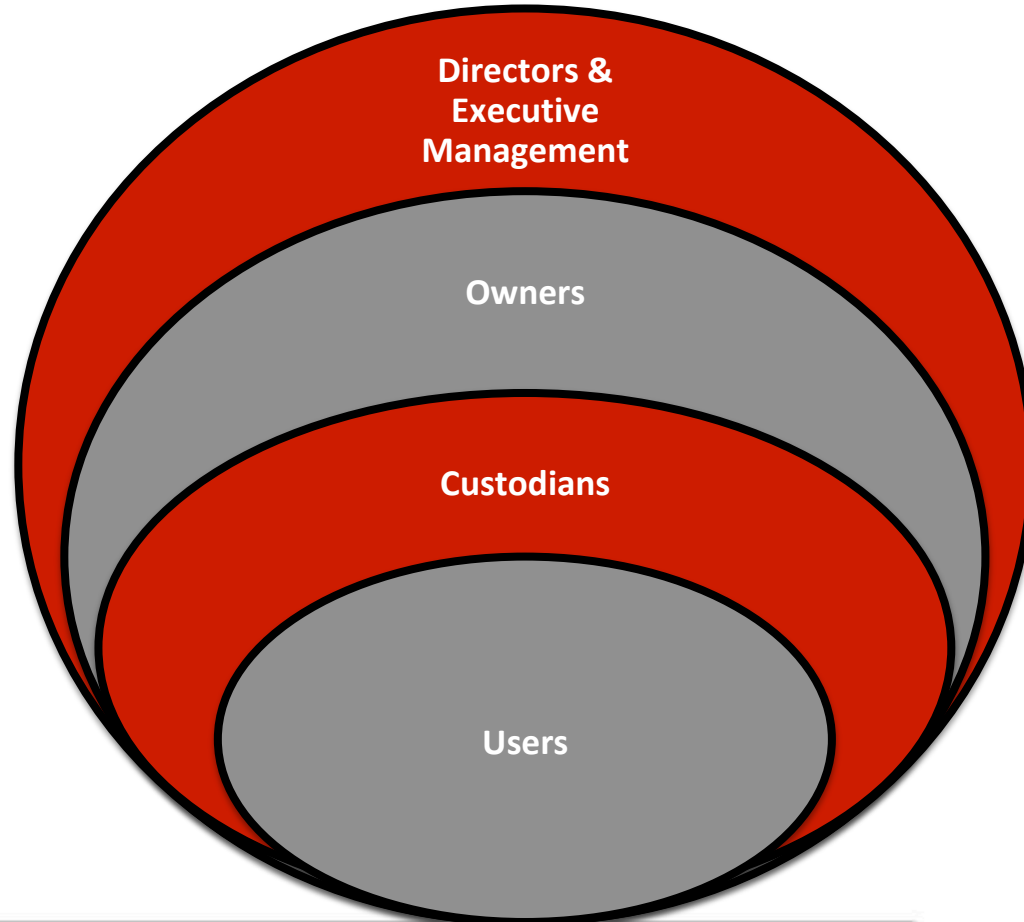
Asset Classification

The purpose of asset classification is to ensure that assets are properly identified and protected throughout their lifecycle.

Asset classifications inform handling instructions, control decisions, audit scope, and regulatory compliance activities.

- Information assets are generally classified by content *sensitivity* (e.g. top secret, secret, classified, SBU).
- Infrastructure and physical assets are generally classified by *criticality* of the services they provide.

Asset Ecosystem



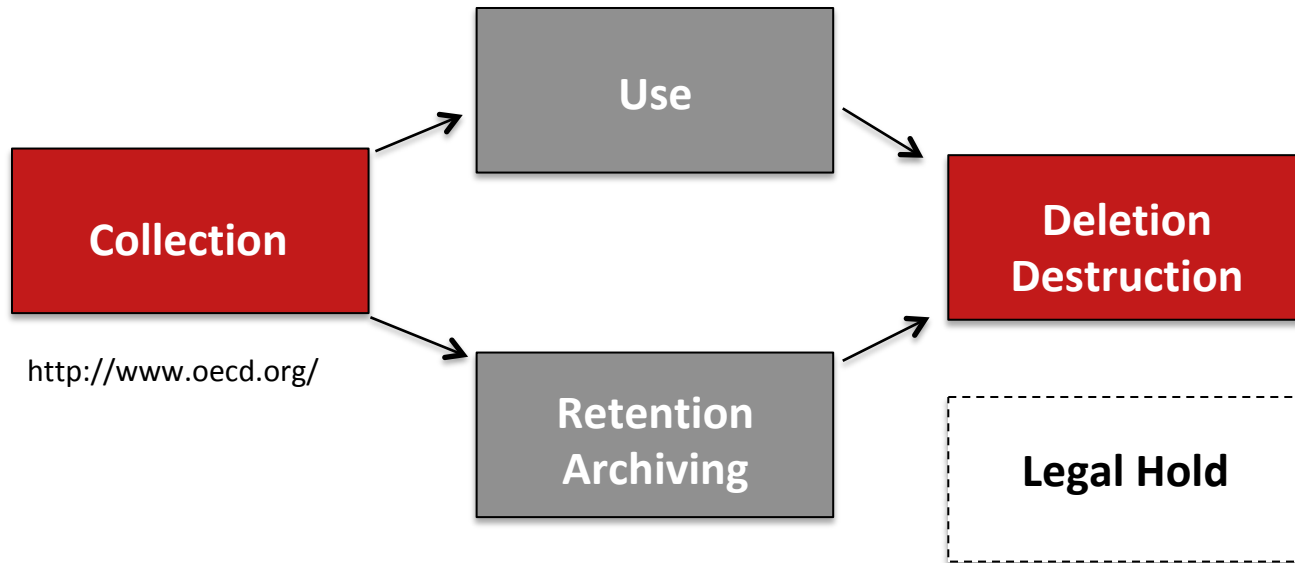
Roles and Responsibilities

Role	Responsibility
Directors & Executive management	Responsible for governance and oversight. From a legal and regulatory perspective, they are ultimately responsible for the actions (or inaction) of the organization.
Privacy Officer	Responsible for identification of and ensuring compliance with applicable organizational, regulatory, and contractual requirements.
Owners Stewards	Responsible for decisions related to classification, access control, and protection.
Custodians	Responsible for implementing, managing, and monitoring controls.
Users	Responsible for treating data and interacting with information systems in accordance with organizational policy and standards.

Privacy is the right of the individual to control their personal data.

- Data collection should be restricted.
- Data owners have a responsibility to respect and enforce privacy principles.
- Data processes should ensure enforcement of privacy and data integrity.
- Data remanence techniques should be used to permanently delete data,

Information Lifecycle



Retention and Archiving

Retention is a protocol (set of rules) within an organization that dictates types of unaltered data that must be kept and for how long.

- Legal and regulatory requirement must be considered.

Archiving is the process of securely storing unaltered data for later potential retrieval.

- Backup and replication is the process of making copies of data to ensure recoverability. They are distinct processes.

Legal Hold

A *legal hold* is the requirement for a organization to preserve all forms of relevant information when litigation, audit, or government investigation is reasonably anticipated. The objective is to avoid evidence spoliation.

- A legal hold supersedes organizational retention policies.

Data Remanence

Data remanence is the residual representation of digital data that remains even after attempts have been made to remove or erase the data. Techniques to counter data remanence include:

- *Clearing* which is the removal of data in such a way that data cannot be recovered using normal system functions or recovery utilities.
- *Purging/sanitizing* which is the removal of data that cannot be reconstructed by any known technique.
- *Destruction* which is the physical act of destroying media in such a way that it cannot be reconstructed.

Anti-Remanence Techniques

Technique	Description	Result
Wiping	Overwrites all addressable storage and indexing locations multiple times	Clearing
Degaussing	Using a electromagnetic field to destroy all magnetically recorded data	Purging
Crypto-shredding	Encrypting remaining data	Purging
Shredding	Physically breaking media into pieces	Destruction
Pulverizing	Reducing media to dust	Destruction
Pulping	Chemical altering media	Destruction
Burning	Incinerating media	Destruction

Data Security Controls

Data security control decisions are generally related to data classification and data state (point in time).

- Data at rest (persistent storage - e.g. disk, tape)
- Data in use (CPU processing or in RAM)
- Data in transit (transmission)

Handling Standards

Handling standards inform custodians and users how to treat the information they use and systems they interact with.

- Handling standards are generally related to classification, data state, and legal or regulatory requirements.
- Assets should be labelled so that users recognize the classification and can apply the appropriate handling standard.
 - Labeling is influenced by the intended audience.
 - Labels can be digital, print, audio, or visual.
 - Noted on or in a document (e.g. CONFIDENTIAL)
 - Written on or attached to media

Domain 2 Asset Security

A. Classify information and supporting assets (e.g. sensitivity, criticality)	D. Ensure appropriate retention (media, hardware, personnel)
B. Determine and maintain ownership (e.g. data owners, system owners, business/mission owners)	E. Ensure data security controls (e.g. data at rest, data in transit)
C. Protect privacy	F. Establish handling requirements (markings, labels, storage, destruction of sensitive information)

Assessment Q1

_____ is the right of an individual to control the use of his or her personal information.

- A. Security
- B. First amendment
- C. Habeas Corpus
- D. Privacy

Assessment Q2

An individual or group that is responsible for assigning classification level and authorizing rights and permissions is known as a _____.

- A. owner
- B. executive
- C. custodian
- D. administrator

Assessment Q3

eDiscovery best relates to the process of _____?

- A. electronic archiving
- B. searching and producing electronic data for use in a civil or criminal case
- C. storage of documents
- D. finding and protecting NPPI

Assessment Q4

The residual representations of digital data even after attempts to remove or erase is known as _____?

- A. data clusters
- B. data remanence
- C. data bits
- D. data slack

Assessment Q5

Which of the following is the most important reason an information asset should have data classification label?

- A. Inventory control
- B. User recognition
- C. Regulatory compliance
- D. Asset management

Break Time

- 5 minute break!

A large, light gray play button icon is positioned on the left side of the slide. It consists of a white right-pointing triangle centered within a series of concentric circles, all rendered in a light gray color.

DAY 1 Segment #3

Domain 3: Security Engineering

Domain 3 Security Engineering

A. Implement and manage engineering processes using secure design principles	G. Assess and mitigate vulnerabilities in mobile systems
B. Understand the fundamental concepts of security models	H. Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems
C. Select controls and countermeasures based on system security evaluation models	I. Apply cryptography
D. Understand security capabilities of information systems	J. Apply secure principles to site and facility design
E. Assess and mitigate vulnerabilities of security architectures, designs, and solution elements	K. Design and implement physical security
F. Assess and mitigate vulnerabilities in web-based systems	



Secure Design Principle | Lifecycle Relationship NIST SP 800-27A

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

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✓✓	✓✓	✓✓	✓✓	✓

Discussion: Security must be considered in information system design. Experience has shown it to be both difficult and costly to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.

Information Security Models

Information security models focus on interactions and provides structure and rules to be followed to accomplish a specific objective (e.g. confidentiality, integrity, and availability).

- Foundational (lower level) models include State Machine, Non-Interference, and Information Flow.
- Relationship (higher level) models include Bell-LaPadula, Biba, Clark-Wilson, and Brewer Nash.

Foundational Models

Model	Description
Foundational	If any of the lower level models are proven false, then the security of the system cannot be relied upon regardless of the implementation of higher level security models
State	Conceptual model that ensures no matter what activity is taking place within a system, it is always trustworthy.
Non-interference (multilevel)	Whatever happens at one security level does not directly or indirectly affect the security environment of other levels.
Information Flow (multilevel)	Information will flow only in ways that do not violate the security policy of the system.

Relationship Models

Bell-LaPadula	Subjects cannot read [simple] data that has a higher classification . Subjects cannot write [*] to an object at a lower security level.	Confidentiality
Biba	Subjects cannot read [simple] data that has a lower classification. Subjects cannot write [*] to an object at a higher security level.	Integrity
Clark-Wilson	Well formed transactions ensure that a user cannot alter data arbitrarily. Instead data can only be altered in specified way in order to preserve its internal consistency (<i>access triple</i>).	Integrity
Brewer-Nash	Context-oriented commercial model designed to defend against conflicts of interest. Access controls that change dynamically depending upon a user's previous actions.	Conflict

Security Evaluation Objectives

A Trusted System has undergone sufficient benchmark testing, verification, and validation (by a independent third-party) to ensure that the product meets the users requirements.

- *Functionality* is verification that a security control exists and that it works correctly at least once.
- *Assurance* is a degree of confidence that the system will act in a correct and predictable manner in every computing situation (trustworthy computing).

Security Evaluation Criteria

TCSEC	Developed in 1983, Trusted Computing System Evaluation Criteria (<i>TCSEC</i>) was used to evaluate, classify, and select systems for the DoD based upon confidentiality requirements. Superseded by the Common Criteria.	Original publication as the <i>orange book</i> . Expanded to 20+ books known as the <i>rainbow series</i> .
ITSEC	Developed in 1991 by a consortium of European nations, <i>IT Security Evaluation Criteria</i> (ITSEC) is used to evaluate the functionality and assurance of a computer system based upon a vendor defined set of requirements.	Functionality and assurance evaluated independently and separately.
Common Criteria	Developed in 1993 by the ISO, the <i>Common Criteria</i> provides a universal structure and language for expressing product and system requirements	The Common Criteria evaluates products against a protection profile and results are published.

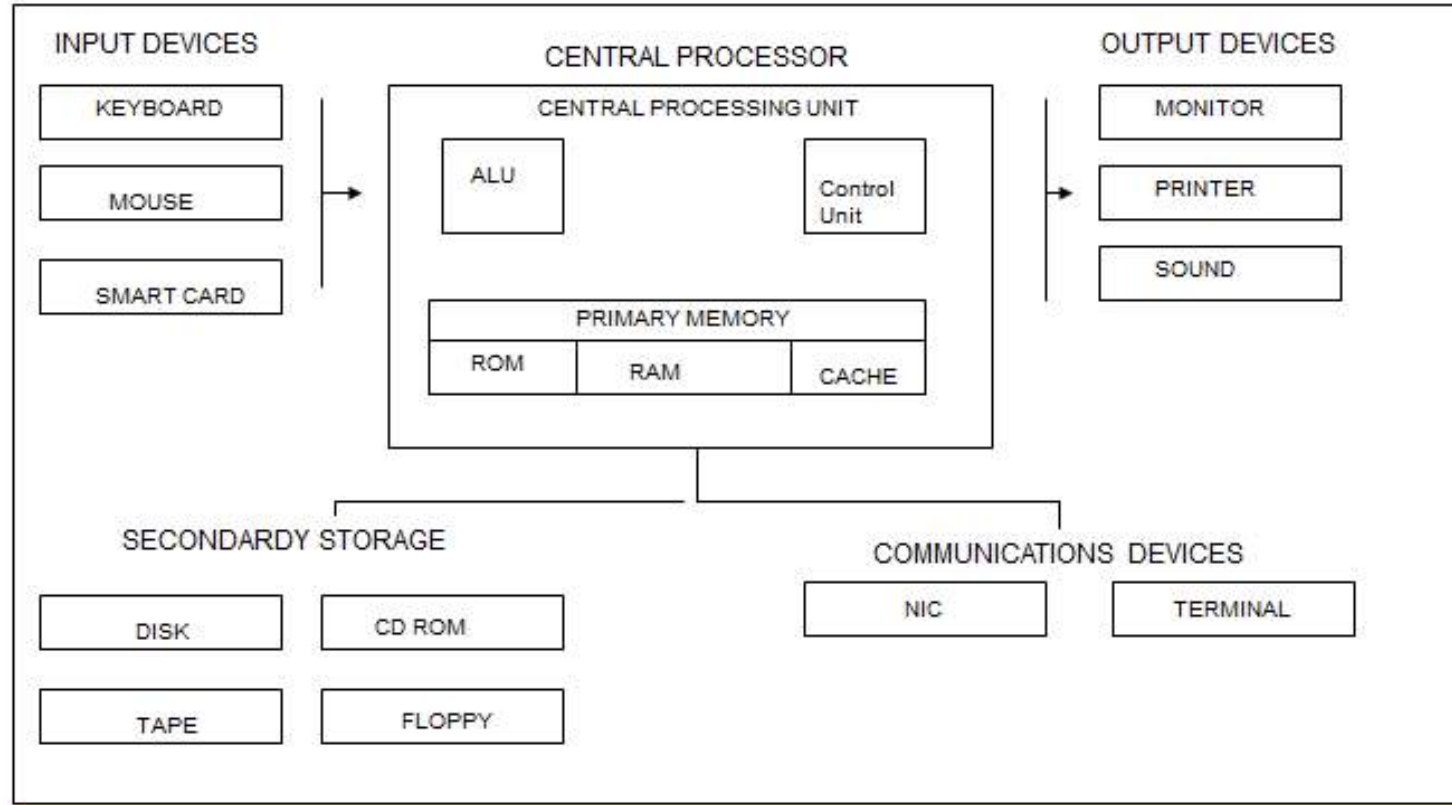
Trusted Computing Base

Information systems security architecture includes all elements of a system including operating system, hardware, software, and network components.

- Any vulnerable element can make the entire system untrustworthy.
- Any vulnerable element can result in exploitation.

Trusted Computing Base is the combination of all the security mechanisms within a computer including hardware, software, and firmware.

Component Level Consideration



Single Point of Failure

Single point of failure (SPOF) can be any technology component whose failure impacts the availability of the entire system.

- SPOFs can be anywhere in the dependency chain.
- Need to identify SPOF and their business impact.
- Investments in system survivability using high availability and fault-tolerant technologies.

Architecture Vulnerability

Configuration	Description	Advantage	Vulnerability
Centralized	Centralized processing	Tightly controlled	Impact to entire platform
Client/Server	Inherent trust	Flexibility	Every connection a potential attack conduit
Distributed	No central authority	Distributed ownership	Distributed management
Large Scale (Parallel)	Disparate systems working in concert (e.g. cluster)	Force multiplier effect (increase in capability)	Data aggregation
Grid	Sharing of CPU and other resources across a network	Power (e.g. seti@home project)	Distributed management and authentication
ICS /SCADA	Embedded systems that monitor and control industrial processes	Power complex systems such as electric grid	Weak authentication, outdated OS, inability to patch, remote access

Cloud Deployment Models

Model	Description	Considerations
Public Cloud	Provisioned for <i>public</i> use	Location Multitenancy
Community Cloud	Provisioned for the exclusive use by a <i>well defined group</i>	Multitenancy
Private Cloud	Provisioned for the exclusive use of a <i>single organization</i>	Scalability

Cloud Service Models - SaaS

Model	Provided	Impact	Considerations
SaaS Software as a Service	Computing Resources + Operating System + Application	<p>The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities</p> <p>The customer uses the provider's applications running on a cloud infrastructure</p> <p>The customer has control over limited user-specific application configuration</p>	<ul style="list-style-type: none">• Availability• Maintenance• Vulnerability Management• Confidentiality• Privacy• Data Ownership• Multitenancy• Testing

Cloud Service Models - PaaS

Model	Provided	Customer Impact	Considerations
PaaS Platform as a Service	Computing Resources + Operating System + (optionally, database)	<p>The customer does not manage or control the underlying cloud infrastructure, operating system, programming languages, tools, and platform</p> <p>The customer deploys onto the cloud infrastructure created or acquired applications</p> <p>The customer has control over deployed applications and possibly configuration settings for the application-hosting environment</p>	<ul style="list-style-type: none">• Availability• Maintenance• Vulnerability Management• Confidentiality• Privacy• Data Ownership

Cloud Service Models—IaaS

Model	Provided	Customer Impact	Considerations
IaaS Infrastructure as a Service	“Bare metal” Computing Resources	<p>The customer does not manage or control the underlying cloud infrastructure</p> <p>The customer can provision processing, storage, networks, and other fundamental computing resources</p> <p>The customer has control over the operating system, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls)</p>	<ul style="list-style-type: none">• Availability• Maintenance• Vulnerability Management

Web Vulnerabilities

Web systems are particularly vulnerable due to their level of exposure, accessibility, and rapid rate of change.

- Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, database, framework, and custom code.
- System owners, developers, and system administrators need to work together to ensure that the entire stack is configured properly.
- Resource <http://www.owasp.org>

Improper Input/output Validation

Vulnerability	Description	Impact
Injection	Tricking an application into including unintended commands in the data sent to an interpreter (e.g. OS, LDAP, SQL).	Can result in database, schema, account, and/or operating system access.
Cross-Site Scripting	Injection of malicious code into a vulnerable web application or back-end database that will execute scripts in a victim's browser.	Can result in user session hijack, redirection to malware distribution site, or bypassing access controls.
Cross-Site Request Forgery (CSRF/ XSRF)	Tricking a web browser into executing a malicious action on trusted site for which the user is currently authenticated. CSRF exploits the trust that a site has in a user's browser.	Can result in data theft, unauthorized funds transfers, credential modifications, or stolen session cookies.

Improper Error Handling

Vulnerability	Description	Impact
Error Messages	Generation of error messages are reveal implementation or debugging details	Disclosure Recon “clues”
Default messages	Divulge system information e.g. “Invalid user name”	Disclosure Recon “clues”

OWASP Mobile Top 10 Vulnerabilities

M1: Weak Server Side Controls

M2: Insecure Data Storage

M3: Insufficient Transport Layer Protection

M4: Unintended Data Leakage

M5: Poor Authorization and Authentication

M6: Broken Cryptography

M7: Client Side Injection

M8: Security Decision Via Untrusted Inputs

M9: Improper Session Handling

M10: Lack of Binary Protections

Embedded System (IoT)

An embedded system is an electronic product that contains a microprocessor and software designed to perform a specific task. An embedded system can either be fixed or programmable.

- Embedded systems are found in consumer, cooking, industrial, automotive, medical, commercial, and military applications.
- Embedded systems range from very small personal devices to large-scale environments. For example, digital watches, health meters, printers/MFDs, camera systems, routers, sensor traffic lights, automotive safety, and industrial control systems.
- The Internet of Things (IoT) sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks provide a pathway for attack.

I Cryptography

Cryptography is the science of secret writing that enables an entity to store transmit data, and process in a form that is only available to an intended recipient.

Primary cryptographic use cases and corresponding techniques include:

- **Confidentiality (encryption)**
- **Integrity (hashing)**
- **Non-repudiation (digital signatures)**
- **Authentication (digital certificate)**
- **Obfuscation (encryption, steganography)**

Cryptographic Terminology — Cipher

Term	Description
Plaintext (cleartext)	Human readable text
Ciphertext	Encrypted and/or human unreadable text
Cipher	A technique that transforms plaintext into ciphertext and back to cleartext
Algorithm	A cryptographic algorithm is a mathematically complex modern cipher
Stream Cipher	Algorithm that works with one bit at a time
Block Cipher	Algorithm that works with blocks of data

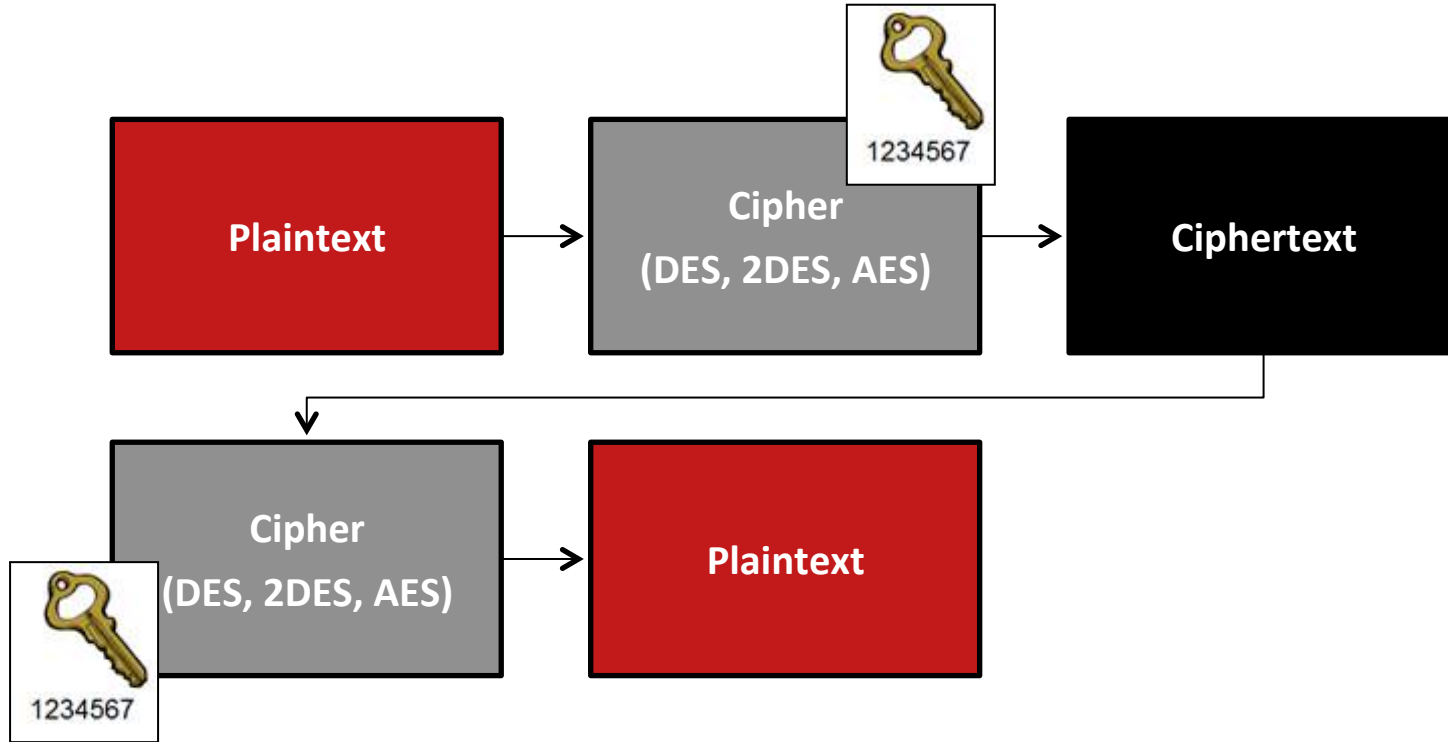
Cipher Terminology - Techniques

Technique	Description
Substitution Cipher	<i>Substitution cipher</i> replaces one character or bit for another character or bit.
Transposition Cipher	<i>Transposition cipher</i> moves characters or bits to another place within the message block.
Confusion	<i>Confusion</i> is the process of changing the values Complex substitution functions are used to create confusion
Diffusion	<i>Diffusion</i> is the process of changing the order Sending bits through multiple rounds of transposition is used to create diffusion.

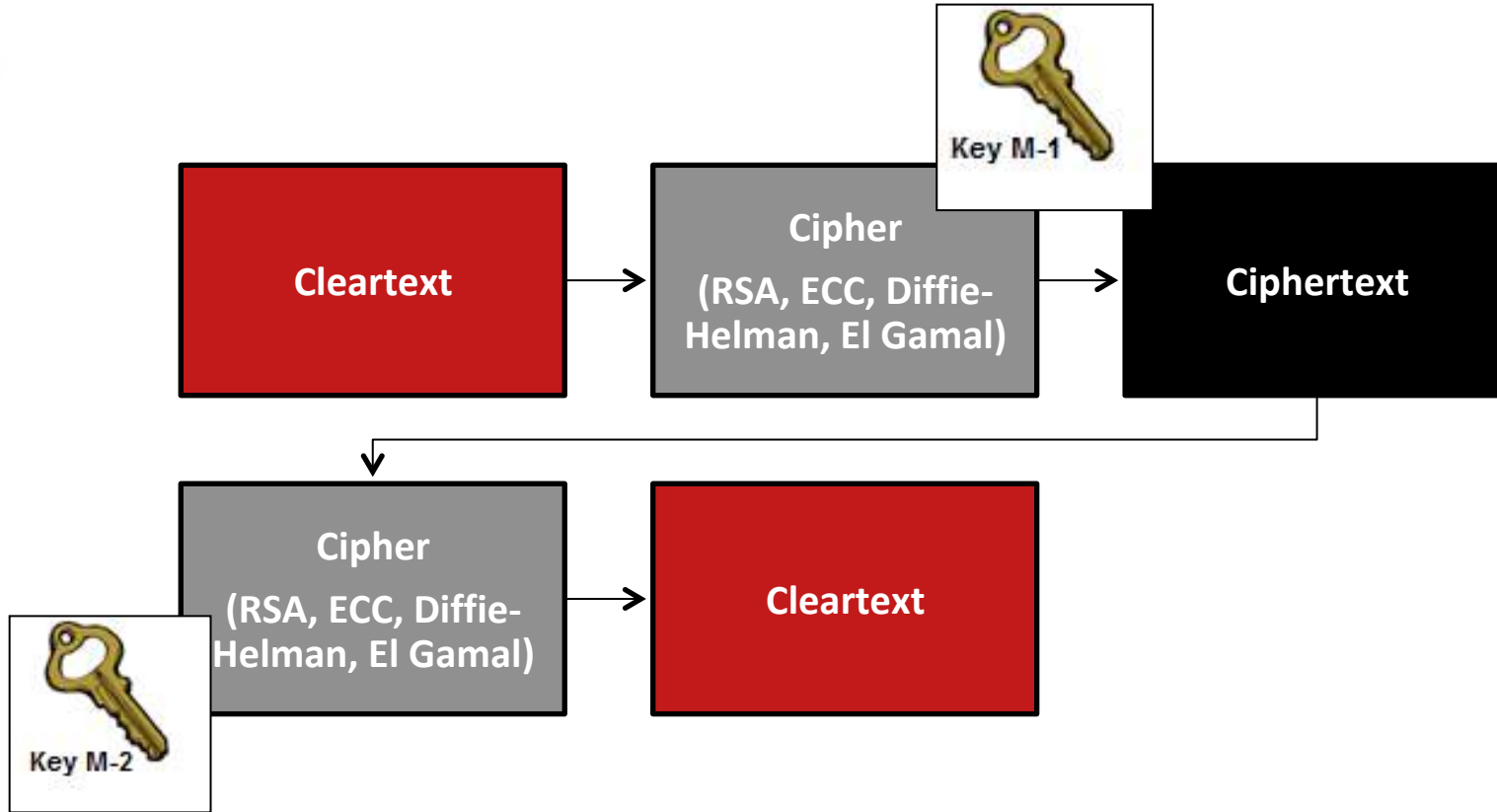
Cryptographic Terminology - Key

Term	Description
Key / Cryptovvariable	Secret value used with an algorithm <ul style="list-style-type: none">The key dictates what parts of the algorithm will be used, in what order, and with what values
Key Space	Number of possible key combinations <ul style="list-style-type: none">e.g. 256-bit = $2^{256} = 1.1578 \times 10^{77}$ possible keys
Key Stretching	The initial key is fed into an algorithm that outputs an <i>enhanced</i> (stronger) key.
Symmetric	Using a single key
Asymmetric	Using two mathematically related keys (public / private)
Public Key	Key that is publicly distributed
Private key	Corresponding key that is secured by the owner.

Symmetric Encryption Illustration



Asymmetric Illustration



Key Pairs in Action for Encryption



Alice has a key pair.

- She freely distributes her public key.
- She securely stores her private key.



Bob has a key pair.

- He freely distributes his public key.
- He securely stores his private key.

Message Flow – Hybrid Solution

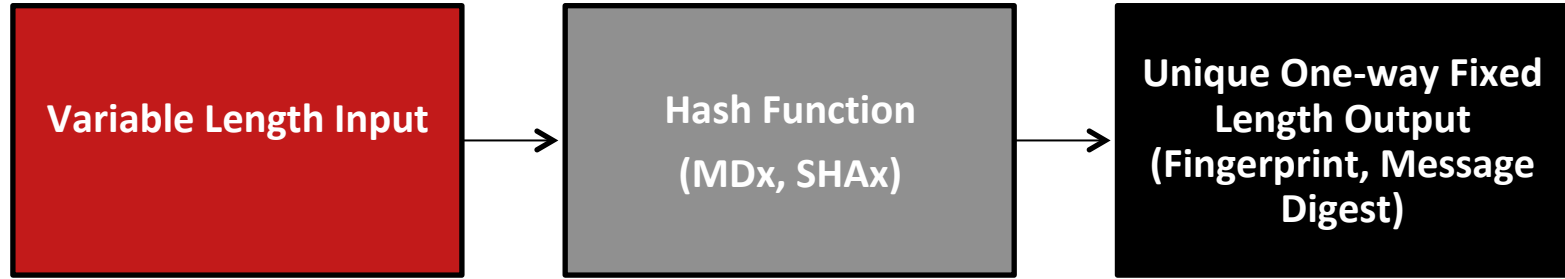


Alice wants to send Bob a encrypted message:



Hashing

Hashing produces a visual representation of a data set.



*The original message remains intact.

Message Digest in Action



Alice puts message through a hashing algorithm and generates a message digest (hash) value

Alice sends message and message digest to Bob



Bob receives the message and the message digest

Bob puts message through a hashing algorithm and generates a message digest (hash) value

Bob compares both message digests

If the message digests are the same—the message was not modified in transmission

If the message digests are different—the message was modified in transmission


I Hash Attacks

Attack	Description
Birthday	Exploits the mathematics behind the birthday problem in probability theory to cause a collision (two inputs producing the same hash value)
Rainbow Table	Comparing a table of known inputs/outputs to unknown outputs

Digital Signature

A *digital signature* is a message digest that has been encrypted using a private key and digital signature algorithm (RSA, DSA).


Digital Signature in Action



Alice puts a message through a hashing algorithm and generates a message digest (hash) value

Alice encrypts the message digest with her **PRIVATE** key

Alice sends plain text message and message digest to Bob



Bob receives the message and the message digest

Bob decrypts the message digest using Alice's **PUBLIC** key proving authenticity (non-repudiation)

Bob puts the plain text message through the same hashing algorithm and generates a message digest

Bob compares both message digests

If the message digests are the same—the message was not modified in transmission

If the message digests are different—the message was modified in transmission

Digital Certificates

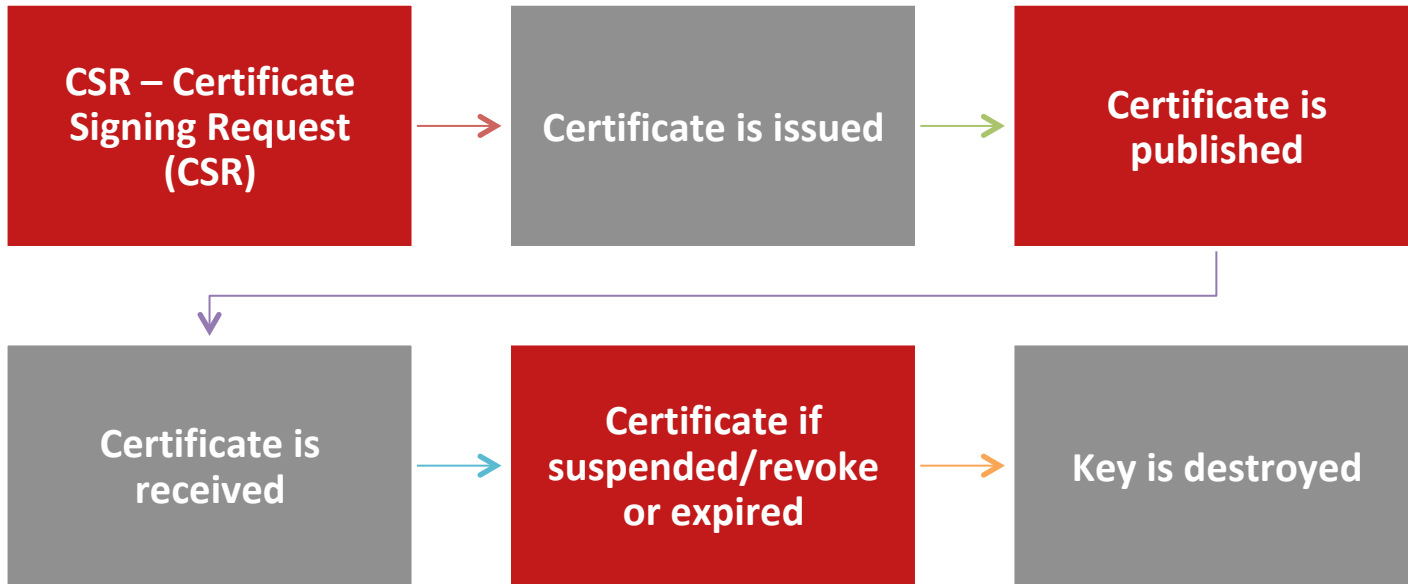
Digital Certificates are the mechanism used to generate a private key and to associate a public key with a collection of components sufficient to authenticate the claimed owner.

- The X.509 standard defines the certificate format and fields for public keys.
- The X.509 standard defines the distribution procedures.
- The current version of X.509 for certificates is v3.

I Types of Digital Certificates (Use)

Type	User
Personal	Verifies a user identity (generally used for email)
Server (Machine/Computer)	Verifies a server identity
Domain Validation	Verifies a web domain <ul style="list-style-type: none">• Wildcard certificate can be used with multiple subdomains of a domain (e.g. *.example.com)
Organization	Verifies a web domain and a organization
Extended Validation	Verifies a web domain and a organization subject to additional vetting (a.k.a. “green bar”)
Code / Object signing	Verifies origination/ownership as well as object integrity
Trusted/Intermediate	Identifies root and intermediate Certificate Authorities

Certificate Lifecycle



Crypto Attack Categories

Intention is to break a cryptosystem and find the plaintext from the ciphertext. The attacker's objective is to identify the key.

Object	Description
Ciphertext Only	A sample of ciphertext is available without the plaintext associated with it.
Known Plaintext	A sample of ciphertext and the corresponding known plaintext is available.
Chosen Plaintext	Can choose the plaintext to get encrypted and obtain the corresponding ciphertext.
Chosen Ciphertext	Can select the ciphertext and obtain the corresponding plaintext

Key Attacks

Attack	Description
Brute Force	Every possible key is tested (online/offline)
Dictionary	List of known keys tested
Frequency	Looking for patterns to reveal the key

Building and facility security focuses primarily on preventive, deterrent, and detective access controls and workplace safety.

Physical security is based upon a layered defense model.

- *Obstacles* to frustrate trivial attackers and delay serious ones
- *Detective controls* make it likely that attacks will be noticed
- *Response mechanisms* to repel, catch, or frustrate attackers

I Building Security

Control	Description
Lighting	<p>Lighting for personnel safety and intruder deterrence</p> <ul style="list-style-type: none">• Intruders are less likely to enter well-lit areas• Lighting can be continuous, motion triggered, random, timed, or standby• Lighting should be damper proof and have a backup power supply
Signs	<p>Signs for personnel safety and intruder deterrence</p> <ul style="list-style-type: none">• Warning signs indicate surveillance (“someone is paying attention”)
Physical Barrier	<p>Fences, walls , gates, barricades, bollards, and mantraps define the perimeter.</p> <ul style="list-style-type: none">• They serve to prevent, deter, or delay (increase workfactor) an attack.
Surveillance	<p>Surveillance technologies such as IDS/IPS, closed-circuit TV (CCTV) and camera systems can be used to monitor, detect (and report) suspicious, abnormal, or unwanted behavior.</p>
Security Guards	<p>Security personnel may be stationed at checkpoints, patrol the area, manage surveillance, and respond to breaches and/or suspicious activity.</p>

Environmental Impact

Computers, electronic equipment, and transmission media are sensitive to environmental factors such as heat, humidity, air flow, and power quality.

- Environmental imbalance can impact stability, availability, and integrity.

Environmental Security

Heat	Acceptable temperature is between 70–74 degrees.
Humidity	Acceptable relative humidity is between 45–60%.
Air Flow	Hot Aisle / Cold Aisle configuration for data center racks
Power	Electrical power supplied to electronic devices must have consistent voltage and a minimum of interference. Devices need to be protected against surges, spikes, sags, brownouts and blackouts.
EMI\RFI	Equipment should have limited exposure to magnets, fluorescents lights, electric motors, space heaters, and wireless access points. Copper and coax cable should be shielded.
Fire	Fire protection is comprised of four elements – prevention, detection, containment and suppression.

Domain 3 Security Engineering

A. Implement and manage engineering processes using secure design principles	G. Assess and mitigate vulnerabilities in mobile systems
B. Understand the fundamental concepts of security models	H. Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems
C. Select controls and countermeasures based on system security evaluation models	I. Apply cryptography
D. Understand security capabilities of information systems	J. Apply secure principles to site and facility design
E. Assess and mitigate vulnerabilities of security architectures, designs, and solution elements	K. Design and implement physical security
F. Assess and mitigate vulnerabilities in web-based systems	



Assessment Q1

The rules for this conceptual model are – no read up and no write down. This is the _____ model and the objective is _____.

- A. Biba, integrity
- B. Bell-LaPadula, confidentiality
- C. Biba, confidentiality
- D. Bell-LaPadula, integrity

Assessment Q2

A buffer is an allocated segment of _____.

- A. processing time
- B. BIOS
- C. memory
- D. slack space

Assessment Q3

A consequence of an attacker injecting instructions into a running process is that _____.

- A. the process will shut down
- B. the process will carry out the instructions
- C. the process send an alert
- D. the process will fail-secure

Assessment Q1

Which of the following is not a true statement?

- A. The strength of a cryptosystem is a combination of the algorithm, the length of the key and public knowledge of the key.
- B. Work factor is the time and effort it takes to break a cryptosystem.
- C. Keyspace is the number of possible crypto-variable combinations.
- D. Longer keys are harder to break but require more processing power

Assessment Q5

A _____ is a message digest that has been encrypted using a private key.

- A. Salt
- B. Digital certificate
- C. Digital signature
- D. HMAC

A large, light gray play button icon with a white triangle pointing right, centered within a circle. The circle has a thick white border and a gray shadow.

Day 1 Segment #4

Test Taking Strategies

New Test Format

Effective Dec. 18, 2017 (ISC)² introduced Computerized Adaptive Testing (CAT).

- This more precise evaluation reduces the maximum exam administration time from 6 hours to 3 hours, and it reduces the items necessary to accurately assess a candidate's ability from 250 items on a linear, fixed-form exam to as little as 100 items (to a maximum of 150) on the CISSP CAT exam.
- You cannot review a question.
- 25 unscored questions will be included.
- The exam content outline and passing standard for both versions of the examination are exactly the same. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format.

Test Taking Strategies

1. Read the (ISC)² announcement and FAQ's found on their website <https://www.isc2.org/Certifications/CISSP/CISSP-CAT>
2. Don't panic if you are unsure about an answer. Make the best decision possible. Remember there are 25 unscored questions.
3. Don't rush. Read for comprehension.
4. Watch out for double negatives.
5. Read every answer option.
6. Don't argue with the answers. Determine what the question wants and then give it the best answer of what it provided.

The Zen of Test Taking

Relax. Breathe deeply. Enjoy

- Remind yourself that you're prepared.
- Approach the test with a positive – can do attitude.
- Don't think of the exam as chore – envision it is an opportunity to validate your knowledge and experience.
- Be sure to play to your strengths - Schedule your exam for your best time of day - wear comfortable clothing.
- Promise yourself a wonderful indulgence at the completion of this journey.

Day -2

Join me tomorrow for Part II of the CISSP Crash Course.

Segment 1: Domain 4 Communications and Network Security

Segment 2: Domain 5 Identity and Access Management

Segment 3: Domain 6 Security Assessment and Testing

Segment 4: Domain 7 Security Operations

Segment 5: Domain 8 Software Development Testing

Segment 6: Preparing for Test Day!

See ya tomorrow!