DOMAIN 5

SECURITY+ EXAM CRAM

PROVEN FAST, EFFECTIVE & AFFORDABLE EXAM PREP

CompTIA
Security+

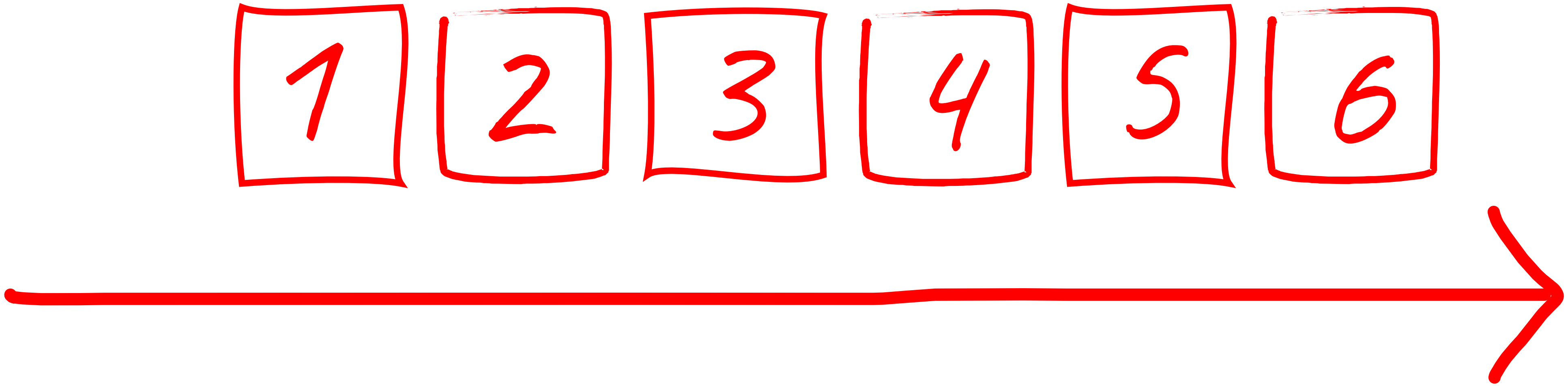
with Pete Zerger CISSP, vCISO, MVP

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	**14%**

INTRODUCTION: SERIES OVERVIEW

LESSONS IN THIS SERIES



Intro + one lesson for each exam domain

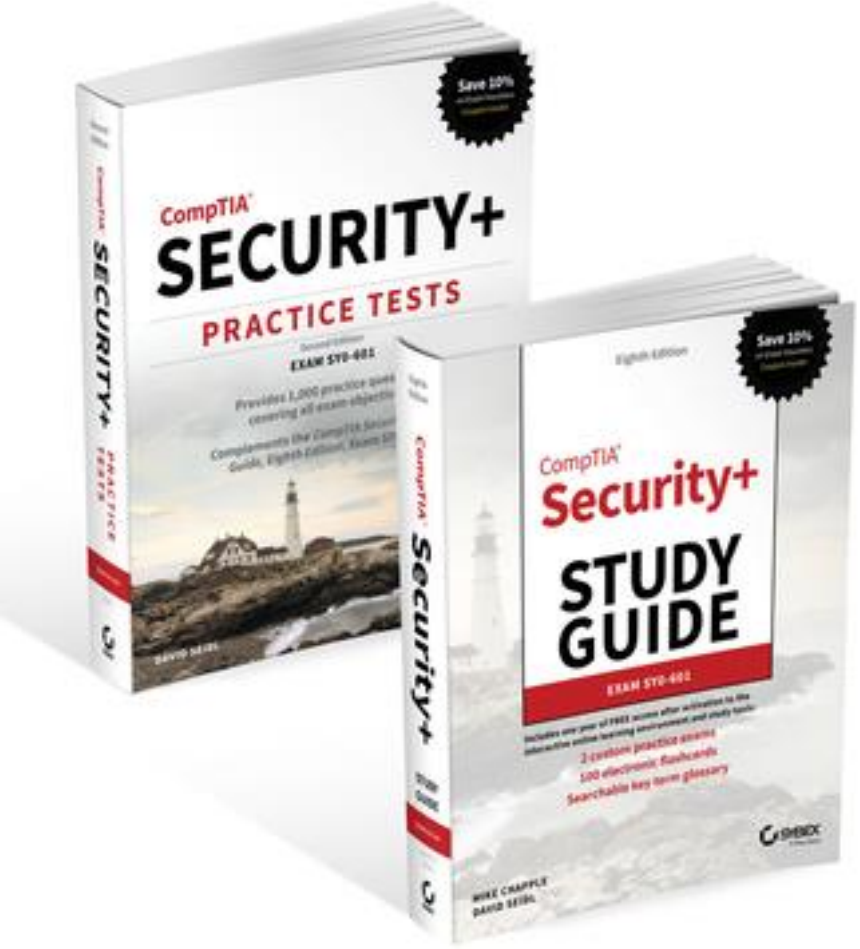
+ 5-10 shorter supplemental lessons

CompTIA Security+ Exam Cram

EXAM NUMBER: SY0-601

5.0 Governance, Risk, and Compliance

Covering all topics in the official
Security+ exam objectives

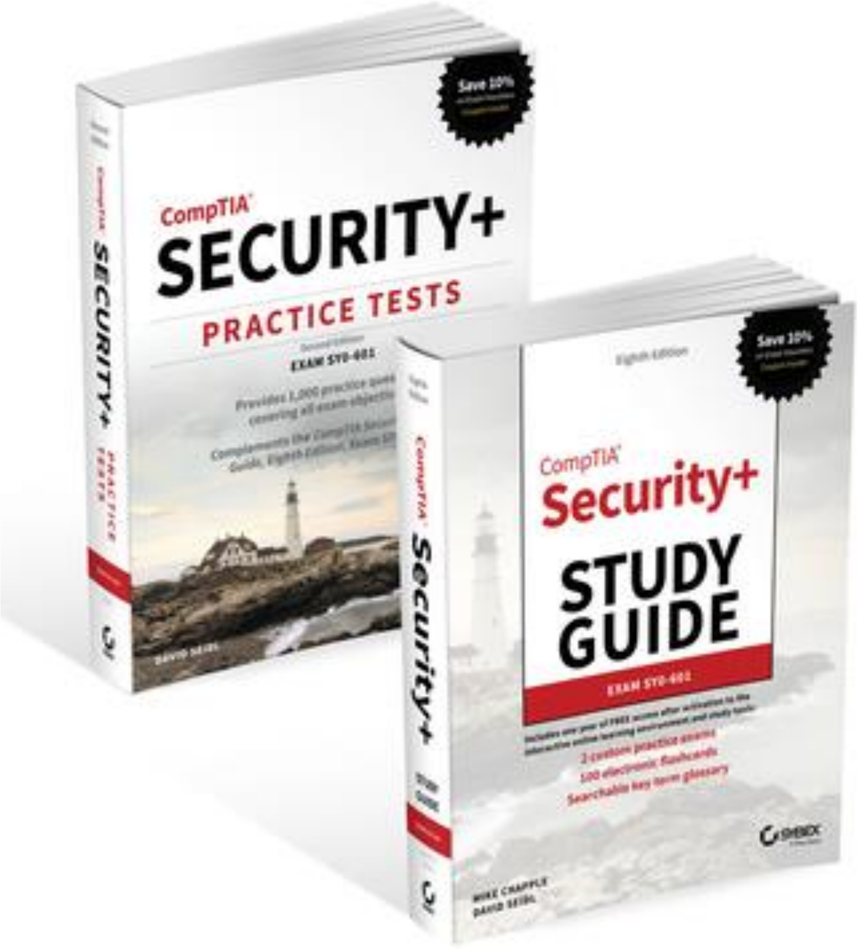


SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams



SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams

A pdf copy of the presentation is available in the video description!

SUBSCRIBE 🔔 👍

5.0 GOVERNANCE, RISK, AND COMPLIANCE

5.1 Compare and contrast various types of controls

- **Category**
  - Managerial
  - Operational
  - Technical

- **Control type**
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical

Know the security controls that fall into each category!

Security Controls

Security measures for countering and minimizing loss or unavailability of services or apps due to vulnerabilities

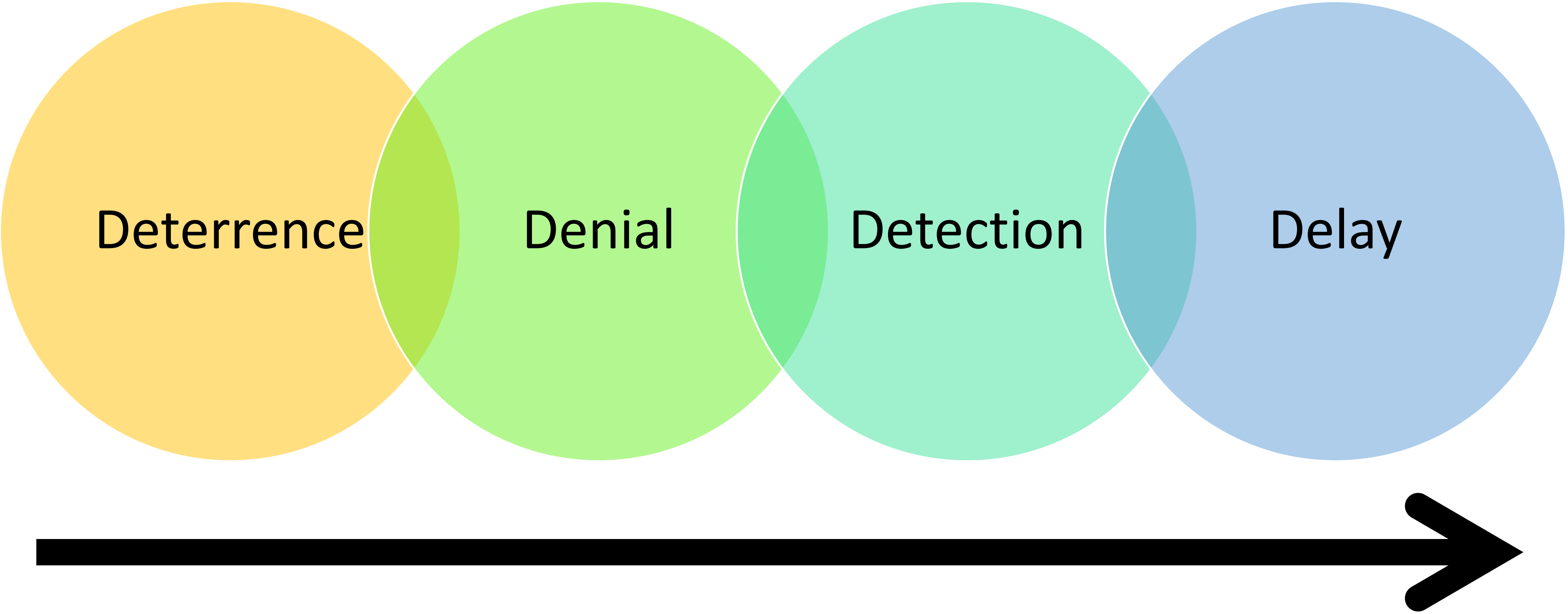
Security Controls

The terms **safeguards** and **countermeasure** may seem to be used interchangeably

Security Controls

safeguards are **proactive**
countermeasures are **reactive**

FUNCTIONAL ORDER OF SECURITY CONTROLS



Control Categories

There are three categories of security controls:

Managerial. Policies and procedures defined by org's security policy, other regulations and requirements.

Operational. are executed by company personnel during their day-to-day operations.

security awareness training, change mgmt, BCP

Technical. aka "logical", involves the hardware or software mechanisms implemented by IT team to reduce risk.

firewall rules, antivirus/malware, IDS/IPS, etc.

Control Types

Deterrent. Deployed to discourage violation of security policies.

Preventative. Deployed to thwart or stop unwanted or unauthorized activity from occurring.

Detective. Deployed to discover or detect unwanted or unauthorized activity.

Compensating. Provides options to other existing controls to aid in enforcement of security policies.

Control Types

Deterrent. Deployed to **discourage violation** of security policies.

Preventative. Deployed to thwart or **stop unwanted or unauthorized activity** from occurring.

Detective. Deployed to **discover or detect** unwanted or unauthorized activity.

Compensating. Provides **options to other existing controls** to aid in enforcement of security policies.

Control Types (cont)

Corrective. modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred.

Physical. a control you can physically touch.

Control Types (cont)

Corrective. modifies the environment to **return systems to normal** after an unwanted or unauthorized activity has occurred.

Physical. a control you can **physically touch**.

CONTROL TYPES

Preventative

deployed to stop unwanted or unauthorized activity from occurring,

EXAMPLES: fences, locks, biometrics, mantraps, alarm systems, job rotation, data classification, penetration testing, access control methods,

Deterrent

deployed to discourage the violation of security policies. A deterrent control picks up where prevention leaves off.

EXAMPLES: locks, fences, security badges, security guards, mantraps, security cameras, trespass or intrusion alarms, separation of duties, awareness training, encryption, auditing, and firewalls. .

CONTROL TYPES

Detective

deployed to discover unwanted or unauthorized activity. Often are after-the-fact controls rather than real-time controls.

EXAMPLES: security guards, guard dogs, motion detectors, job rotation, mandatory vacations, audit trails, intrusion detection systems, violation reports, honey pots, and incident investigations,

Physical

barriers deployed to prevent direct contact with systems or portions of a facility.

EXAMPLES: guards, fences, motion detectors, locked doors, sealed windows, lights, cable protections, laptop locks, swipe cards, guard dogs, video cameras, mantraps, and alarms.

CONTROL TYPES

Corrective

deployed to restore systems to normal after an unwanted or unauthorized activity has occurred. minimal capability to respond to access violations.

EXAMPLES: intrusion prevention systems, antivirus solutions, alarms, mantraps, business continuity planning, and security policies,

Compensating

deployed to provide options to other existing controls to aid in the enforcement and support of a security policy.

EXAMPLES: security policy, personnel supervision, monitoring, and work task procedures.

5.0 GOVERNANCE, RISK, AND COMPLIANCE

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture

- **Regulations, standards, and legislation**
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)
- **Key frameworks**
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/ Cybersecurity Framework (CSF)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
    - Cloud control matrix
    - Reference architecture
- **Benchmarks /secure configuration guides**
  - Platform/vendor-specific guides
  - Web server
  - OS
  - Application server
  - Network infrastructure devices

Defining Sensitive Data

Sensitive data is any information that isn’t public or unclassified.

Personally Identifiable Information (PII). any information that can identify an individual (name, SSN, birthdate/place, biometric records, etc)

Protected Health Information (PHI). health-related information that can be related to a specific person.

REGULATIONS, STANDARDS, AND LEGISLATION

GDPR

General Data Protection Regulation

Deals with the handling of data while maintaining privacy and rights of an individual.

It is international as it was created by the EU, which has 27 different countries as members.

GDPR applies to ANY company with customers in the EU

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements

Anonymization. The process of removing all relevant data so that it is impossible to identify original subject or person.

If done effectively, then GDPR is no longer relevant for the anonymized data.

Good only if you don't need the data!

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements

Anonymization. The process of removing all relevant data so that it is impossible to identify original subject or person.

If done effectively, then GDPR is no longer relevant for the anonymized data.

Pseudonymization. The process of using pseudonyms (aliases) to represent other data.

Can result in less stringent requirements than would otherwise apply under the GDPR.

Use if you need data and want to reduce exposure

National, Territory, and State Laws

Gramm-Leach-Bliley Act (GLBA)

focused on services of banks, lenders, and insurance

severely limited services they could provide and the information they could share with each other

LEGAL & REGULATORY

FISMA

Federal **I**nformation
Security **M**anagement **A**ct

Required formal infosec operations for federal gov't

Requires that government agencies include the activities of contractors in their security management programs

Repealed and replaced the Computer Security Act of 1987 and Government Information Security Reform Act of 2000

NIST responsible for developing the FISMA implementation guidelines

Any mention on exam will be brief. Remember it applies to "government"

Other US privacy laws

HIPAA (Health Insurance Portability and Accountability Act)

HITECH (Health Information Technology for Economic and Clinical Health) Widens scope of privacy protections under HIPAA

Gramm-Leach-Bliley Act (financial institutions)

Children's Online Privacy Protection Act (**COPPA**)

was designed to protect children under age 13

Electronic Communications Privacy Act (**ECPA**)

prohibits a third party from intercepting or
disclosing communications without authorization

PCI DSS

Payment **C**ard **I**ndustry
Data **S**ecurity **S**tandard

a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions

created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express

BASED ON 6 MAJOR OBJECTIVES

- a secure network must be maintained in which transactions can be conducted
- cardholder information must be protected wherever it is stored
- systems should be protected against the activities of malicious hackers
- cardholder data should be protected physically as well as electronically.
- networks must be constantly monitored and regularly tested
- a formal information security policy must be defined, maintained, and followed

KEY FRAMEWORKS

Center for Internet Security (CIS)

a not-for-profit organization that publishes information on cybersecurity best practices and threats.

has tools to help harden your environment and provide risk management.

provides benchmarks for different operating systems and provides controls to help secure your organization.

Details at https://www.cisecurity.org/cybersecurity-tools/.

National Institute of Standards and Technology (NIST)

Cyber Security Framework (**CSF**): NIST RMF/CSF a set of guidelines and best practices to help organizations build and improve their cybersecurity posture.

CSF is aimed at private industry (commercial businesses)

replaces NIST's **Risk Management Framework** (**RMF**) and was designed to focus on risk management for governmental agencies.

CSF available at https://www.nist.gov/cyberframework.
RMF available at https://csrc.nist.gov/projects/risk-management/rmf-overview.

KEY FRAMEWORKS

International Organization for Standardization (ISO)

develops global technical, industrial and commercial standards.

ISO standards for information systems include

ISO **27001** – Security techniques for *Information Security Management Systems*: an international standard on how to manage information security.
Available at https://www.iso.org/standard/54534.html

ISO **27002** – *Code of Practice for Information Security Controls*, which aims to improve the management of information.
Available at https://www.iso.org/standard/54533.html.

ISO **27701** – An extension to 27001/27002 for Privacy Information Management – provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS).
Available at https://www.iso.org/standard/71670.html.

ISO **31000** – provides principles, a framework and a process for managing risk for organizations of any size in any sector.
Available at https://www.iso.org/standard/65694.html.

Statements on Standards for Attestation Engagements (SSAE)

SSAE 18 is an audit standard to enhance the quality and usefulness of System and Organization Control (SOC) reports.

designed for larger organizations, such as cloud providers (*the cost of a Type 2 report can run $30,000 or more*).

SOC 2 Type 1

report that assesses the design of security processes at a specific point in time.

SOC 2 Type 2

(often written as “Type II”) assesses how effective those controls are over time by observing operations for six months.

KEY FRAMEWORKS

Cloud Security Alliance (CSA)

is a not-for-profit organization that produces resources to help **Cloud Service Providers (CSPs)**, like online training, webinars, discussion groups, and virtual summits.

Cloud Control Matrix (CCM)

is designed to provide a guide on security principles for cloud vendors and potential cloud customers to assess the overall risk of a cloud provider:

CSA Reference Architecture

contains best security practices for CSPs and examples, examines topics, such as

- Security and risk
- Presentation services
- Application services
- Information services
- IT Operation and Support (ITOS)
- Business Operation and Support Services (BOSS)

FOR THE EXAM: Remember CSA CCM helps potential customers measure the overall risk of a CSP.

BENCHMARKS/SECURE CONFIGURATION GUIDES

benchmarks are configuration baselines and best practices for securely configuring a system.

Platform-/Vendor-Specific Guides: released with new products so that they can be set up as securely as possible, making them less vulnerable to attack.

Web Servers: the two main web servers used by commercial companies are Microsoft's **Internet Information Server (IIS)**, and the Linux-based **Apache**.

because they are public-facing, they are prime targets for hackers.

to help reduce the risk, both Microsoft and Apache provide security guides to help security teams reduce the attack surface, making them more secure.

These guides advise updates being in place, unneeded services are disabled, and the operating system is hardened to minimize risk of security breach.

BENCHMARKS/SECURE CONFIGURATION GUIDES

benchmarks are configuration baselines and best practices for securely configuring a system.

Operating Systems: Most vendors, such as Microsoft, have guides that detail the best practices for installing their operating systems.

OS benchmarks are also available from CIS and others

Application Server: Vendors produce guides on how to configure application servers, such as email servers or database servers, to make them less vulnerable to attack.

Network Infrastructure Devices: companies like Cisco produce network devices and offer benchmarks for secure configuration.

benchmarks aim to ease process of securing a component, reduce attack footprint, and minimize risk of security breach.

5.0 GOVERNANCE, RISK, AND COMPLIANCE

5.3 Explain the importance of policies to organizational security

- **Personnel**
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
    - Gamification
    - Capture the flag
  - Phishing campaigns
    - Phishing simulations
    - Computer-based training (CBT)
    - Role-based training
- **Diversity of training techniques**
- **Third-party risk management**
  - Vendors
  - Supply chain
  - Business partners
  - Service level agreement (SLA)
  - Memorandum of understanding (MOU)
  - Measurement systems analysis (MSA)
  - Business partnership agreement (BPA)
  - End of life (EOL)
  - End of service life (EOSL)
  - NDA
- **Data**
  - Classification
  - Governance
  - Retention
- **Credential policies**
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts
- **Organizational policies**
  - Change management
  - Change control
  - Asset management

LIMITING ACCESS & DAMAGE

Need-to-know and the **principle of least privilege** are two standard IT security principles implemented in secure networks.

They limit access to data and systems so that users and other subjects have access only to what they require.

They help prevent security incidents

They help limit the scope of incidents when they occur.

💡 When these principles are not followed, security incidents **result in far greater damage** to an organization.

PREVENTING FRAUD AND COLLUSION

Collusion is an agreement among multiple persons to perform some unauthorized or illegal actions.

Separation of duties

a basic security principle that ensures that no single person can control all the elements of a critical function or system.

Job rotation

employees are rotated into different jobs, or tasks are assigned to different employees.

Implementing these policies **helps prevent fraud** by limiting actions individuals can do without colluding with others.

MONITORING PRIVILEGED OPERATIONS

Privileged entities are trusted, but they can abuse their privileges.

it’s important to monitor all assignment of privileges and the use of privileged operations.

Goal

to ensure that trusted employees do not abuse the special privileges they are granted.

Monitoring these operations can also detect many attacks because attackers commonly use special privileges

ESPIONAGE & SABOTAGE

Espionage

external

when a competitor tries to steal information, and they may use an internal employee.

Sabotage

insider

malicious insiders can perform sabotage against an org if they become disgruntled for some reason

PERSONNEL POLICIES

Clean Desk Policy

increases the physical security of data by requiring employees to limit what is on their desk to what they are working on at the present time.

Anything else is secured and out of sight

NDA

NON-DISCLOSURE AGREEMENT

a legal contract intended to cover confidentiality. The scope of an NDA will vary based on situation.

Always review terms before signing any NDA

Background Checks

All potential employees should be thoroughly screened with an extensive background check before being hired and granted network access.

Should part of employment screening policy

PERSONNEL

Acceptable Use Policy

describe how the employees in an organization can use company systems and resources, including software, hardware, and access.

Should include the consequences of misuse

Job Rotation

not allowing one person to be in one position for a long period of time.

Extended control of assets can result in fraud

Mandatory Vacation

requiring employees (especially those in sensitive areas) to take their vacations.

Replacement provides another measure of oversight

PERSONNEL

Separation of Duties

a basic security principle that ensures that no single person can control all the elements of a critical function or system.

Reduces likelihood of collusion amongst employees

Least Privilege

a subject should be given only those privileges necessary to complete their job-related tasks.

Can prevent or limit scope of security incidents and data theft

Social Media Analysis

Analysis of a potential employee's social media during the hiring process to understand more about an individual based on their Internet presence.

Helps identify cultural alignment, character concerns

PERSONNEL

Onboarding | process of integrating a new employee into a company and its culture, customers, etc.

Often includes review and signing of company policies (like AUP)

Offboarding | the process that leads to the formal separation between an employee and the company through resignation, termination, or retirement.

Includes return of equipment, access badge, and exit interview

Disabling user access in this process should be aligned between IT and HR.

PERSONNEL

Gamification

used in computer-based training (CBT) to provide employees with a question/challenge.

can helps to gauge learner retention of the information presented.

May promote competition by awarding points and a leader board

Capture the flag

a security related competition where someone is trying to hack into a resource to gain access to data.

Red team (offense) attempts to breach, while the **Blue** team (defense) defend resources.

Benefits may include skills development, team-building, employee morale

PERSONNEL

Phishing Simulations | false phishing emails sent to employees by IT using a service that measure response (pass/fail).

Fail often triggers just-in-time user training

Computer-based training | self-paced training available via computer, whether for job role or skills enhancement

May be "always available" and use measured

Role-based training | when the company carries out related training specific to a user's specific job role

Should include training on role-specific security awareness

Business Partnership Agreement (BPA)

is used between two companies who want to participate in a business venture to make a profit.

details how much each partner's contributions, rights and responsibilities, as well as the details of operations, decision-making, and sharing of profits.

also has rules for the partnership ending either at a given point or if one of the partners dies or moves on.

Memorandum of Understanding (MOU)

a formal agreement between two or more parties indicating their intention to work together toward a common goal.

similar to an SLA in that it defines the responsibilities of each party.

more formal alternative to handshake but lacks the binding power of a contract.

Memorandum of Agreement (MOA)

similar to an MOU but serves as a legal document and describes terms and details of the agreement.

MSA

Measurement Systems Analysis

provides a way for an organization to evaluate the quality of the process used in their measurement systems.

will assess the measurement process itself, and then calculate any uncertainty or variation in the measurement process.

evaluates the test method, instruments, and process to ensure the integrity of data used for analysis

MSA is an important element of Six Sigma methodology and of other **quality management systems**.

THIRD-PARTY RISK MANAGEMENT

NDA
NON-DISCLOSURE AGREEMENT

contract with vendors and suppliers not to disclose the company's confidential information.

A "mutual NDA" binds both parties in the agreement

EOL
END OF LIFE

point at which a vendor stops selling a product and may limit replacement parts and support.

EOL often specific to an older version

EOSL
END OF SERVICE LIFE

product is no longer sold by manufacturer, updates cease, and support agreements are not renewed.

considered the final phase of product life

Products are usually declared **EOL** before being declared **EOSL**.

Supply Chain

Today, most services are delivered through a chain of multiple entities

Supply Chain

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

Due diligence should be exercised in assessing vendor security posture, business practices, and reliability

Supply Chain

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

May include periodic attestation requiring vendors to confirm continued implementation of security practices

Supply Chain

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

A vulnerable vendor in the supply chain puts the organization at risk

Supply Chain Evaluation

When evaluating 3rd parties in the chain, consider:

On-Site Assessment . Visit organization, interview personnel, and observe their operating habits.

Document Exchange and Review . Investigate dataset and doc exchange, review processes.

Process/Policy Review . Request copies of their security policies, processes, or procedures.

Third-party Audit. Having an independent auditor provide an unbiased review of an entity’s security infrastructure.

SERVICE-LEVEL AGREEMENTS

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn’t meet expectations.

Generally used with vendors (external)

CREDENTIAL POLICIES

Personnel internal staff

Identity provider will be under management of IT (greater control).

Avoid using shared accounts unless necessary. breaks non-repudiation

Best practices for MFA, password complexity, and least privilege enforced.

Third-Party Business partners, vendors, suppliers

May include accounts from external identity providers (Azure AD, OAuth2, OpenID).

Should be required to use multi-factor authentication.

Additional conditions should be applied for sensitive operations.

Conditions might include location, device, connection method, etc.

Devices desktops, laptops, mobile, point-of-sale, IoT

Default passwords should be changed on devices with generic accounts.

For MDM managed devices, certificate authentication may be possible.

Access restricted for unknown/unmanaged and non-compliant devices

CREDENTIAL POLICIES

Service Accounts

are used to run applications/services such as antivirus.

May run as local service accounts with the same rights as a user.

A system account provides higher level of privilege, giving a service full control.

Administrator/Root Accounts

Administrator accounts (Windows) and root accounts (Linux) should be protected as they enable elevated access.

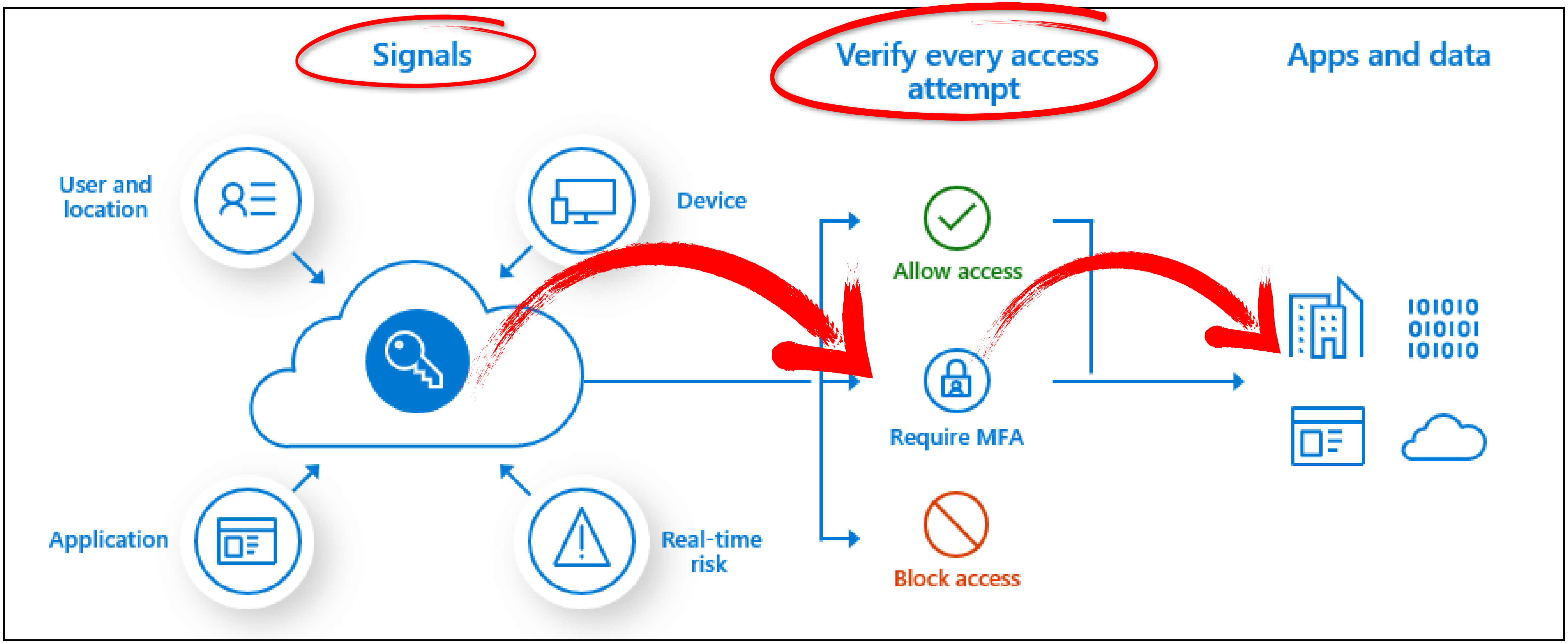
Require periodic password changes and enforce password complexity.

Admin users should have two accounts: a normal user account for day-to-day use and an admin account for administrative duties.

All accounts should have some form of multi-factor authentication enabled. SMS as a 2nd factor is discouraged

CONDITIONAL ACCESS

FROM DOMAIN 3 (3.7)



often possible in federation scenarios (SAML, OAuth, OpenID)

image credit: Microsoft

Configuration, Change & Asset Management

Can prevent security related incidents and outages

Configuration Management

ensures that systems are configured similarly, configurations are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Change Management

the policy outlining the procedures for processing changes

helps reduce risk associated with changes, including outages or weakened security from unauthorized changes.

requires changes to be requested, approved, tested, and documented.

Configuration, Change & Asset Management

Change Control

refers to the process of evaluating a change request within an organization and deciding if it should go ahead.

requests are sent to the **Change Advisory Board (CAB)** to ensure that it is beneficial to the company.

Change Management
policy that details how changes will be processed in an organization

Guidance on the process

Change Control
process of evaluating a change request to decide if it should be implemented

The process in action

Configuration, Change & Asset Management

Asset Management:

process where each asset belonging to the company is been tagged and recorded in an asset register.

maintain an up-to-date asset register to ease the process of tracking and maintaining assets.

includes periodic (usually annual) audits need to be carried out to ensure that all assets are accounted for.

Can help Security team identify unauthorized devices on your network.

Asset Classifications

Asset classifications should match the data classifications.

DATA POLICIES

Data policies ensure data is classified, handled, stored, and disposed of in accordance with applicable regulations.

Classification: the process of labeling data with relevant classifications, indicating level of sensitivity, such as top secret, secret, confidential, or sensitive data.

classification determines how the data is handled. Discussed in section 5.5

Governance: the oversight and management that describes security controls applied at each stage of the data-handling process, from creation to destruction.

details the processes used to manage, store, and dispose of data to ensure that the organization meets their compliance obligations.

Retention: Organizations do not want to hold data any longer than they need to, as unnecessary retention increases liability and risk

Org may have to retain data after its usefulness for regulatory compliance.

An example, one regulation requires hospitals retain PHI for at least 5 years.

5.0 GOVERNANCE, RISK, AND COMPLIANCE

5.4 Summarize risk management processes and concepts

- **Risk types**
  - External
  - Internal
  - Legacy systems
  - Multiparty
  - IP theft
  - Software compliance / licensing
- **Risk management strategies**
  - Acceptance
  - Avoidance
  - Transference
  - Cybersecurity insurance
  - Mitigation
- **Risk analysis**
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment
  - Risk control self-assessment
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite
  - Regulations that affect risk posture
  - Risk assessment types
    - Qualitative
    - Quantitative
  - Likelihood of occurrence
  - Impact
  - Asset value
  - Single-loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
- **Disasters**
  - Environmental
  - Person-made
  - Internal vs. external
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions
  - Identification of critical systems
  - Site risk assessment

RISK TYPES

The six types of risk you should know for the exam

External

Different threat actors, ranging from competitors and script kiddies to criminal syndicates and state actors.

Capabilities depend on tools, experience, and funding.

Other external environmental threats, such as fire and floods, and man-made threats, such as the accidental deletion of data or users.

Internal

A malicious insider, a threat actor who may be a dissatisfied employee (someone overlooked for a promotion).

Another internal threat is human error, which is when data is accidentally deleted.

RISK TYPES

Legacy Systems

Risks may include end of support and security patches because vendor has deemed that the system has reached the end of its service life.

As technologies improve, so do the hacking tools, and the legacy systems may have limited or no protection against them.

Vulnerabilities to legacy systems tend to increase over time

Multiparty

When a contractor wins a contract and then sub-contracts some of the parts of the contract to other companies, who in turn subcontract again.

With many parties being involved in a single contract, if any of them goes out of business, it cause disruption to the company.

Any party in the agreement with security issues could also put the company at risk.

Common in supply chains, these risks should be addressed in BIA

RISK TYPES

IP (Intellectual Property) Theft

If thieves steal your copyrighted material, trade secrets, and patents, it may result in a loss of revenue.

This data could be used in other countries where a legal route to recover your data or seek damages is impossible.

Data Loss Prevention (DLP) or document management systems can protect documents even if exfiltrated.

Software Compliance/Licensing

Software purchased from a disreputable source may not include valid licenses, could lead to a fine, or may contain malware.

This would be a licensing violation

Employees may use more copies of the company-purchased software than the licenses that you purchase, sometimes for personal use.

Sometimes called a "compliance violation"

RISK MANAGEMENT STRATEGIES

Response to Risk

Risk Acceptance. Do nothing, and you must accept the risk and potential loss if threat occurs.

Risk Mitigation. You do this by implementing a countermeasure and accepting the residual risk.

The act of reducing risk

Risk Transference. Transfer (assign) risk to 3rd party, like by purchasing insurance against damage.

Risk Avoidance. When costs of mitigating or accepting are higher than benefits of the service.

RISK MANAGEMENT STRATEGIES

Risk Appetite. Sometimes called *"risk tolerance"*, is the amount of risk that a company is willing to accept.

These terms are often used interchangeably, though many experts can articulate a difference.

Regulations that affect risk posture

regulations addressing data privacy and security that influence an organizations risk posture include:

-General Data Protection Regulation (**GDPR**)

-Sarbanes-Oxley Act (**SOX**),

-Health Insurance Portability Accountability Act (**HIPAA**)

-Payment Card Industry & Data Security Standard regulations (**PCI-DSS**)

RISK ANALYSIS

Risk Register

A tool in risk management and project management

Sometimes used to fulfill regulatory compliance but often to track potential issues that can derail intended outcomes.

Typically includes several details, including:

-Risk ID
-Description
-Probability
-Impact
-Severity
-Response
-Owner

Metrics in a risk register will vary from company to company.

Should be considered a living document and updated periodically (at least annually).

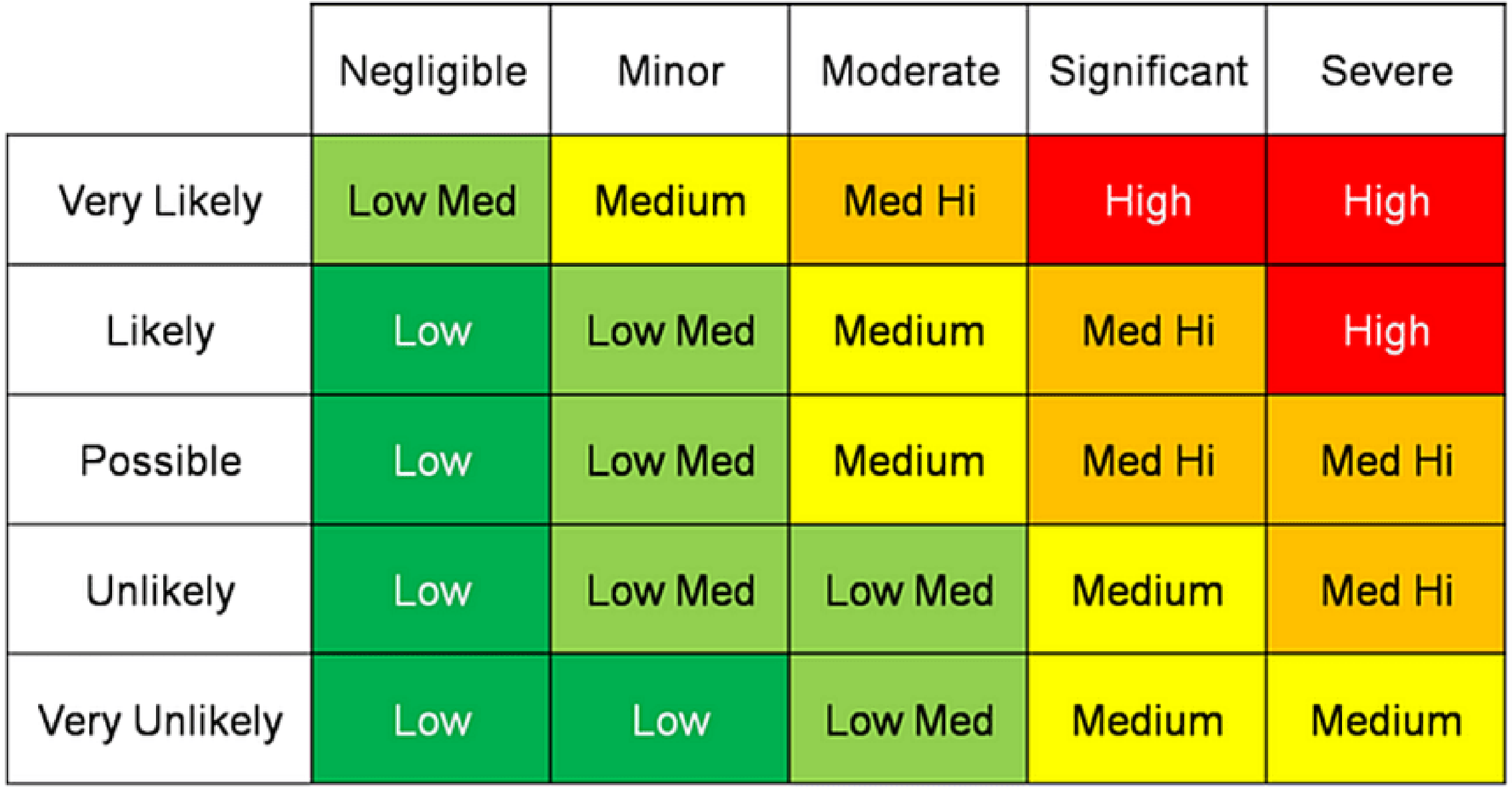
RISK MATRIX/HEAT MAP

A **risk matrix** is used to a provide visual representation of risks affecting a company.

A **heat map** shows the severity of the situation, with the most severe risks being in red.

Impact

Likelihood



	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

RISK ANALYSIS

Risk Control Assessment

occurs when a company periodically checks that the risk controls that they have in place are still effective with changing technology.

May involve an external auditor or expert

Risk Control Self-Assessment

conducted by employees within the company, often through survey or department-level review.

employees evaluate existing risk controls so management-level decision makers can decide if current controls are adequate.

A bottom-up approach often used in smaller organizations

Risk Awareness

the process of educating employees to increase their risk awareness and encourage them to identify, review and report concerns.

Can bring new insights into reducing risk from those most familiar!

TYPES OF RISK

Residual
Inherent
Total

RISK

TYPES OF RISK

Residual Risk

The risk that remains even with all conceivable safeguards in place.

Residual Risk

The risk management has chosen to accept rather than mitigate.

TYPES OF RISK

Inherent Risk

Newly identified risk not yet addressed with risk management strategies

Inherent Risk

The amount of risk that exists in the absence of controls.

Total Risk

The amount of risk an organization would face if **no safeguards** were implemented.

RISK MANAGEMENT

Residual
Inherent
Total
RISK

TYPES OF RISK

Residual	AFTER	✓
Inherent	BEFORE	✓
Total	WITHOUT	

Control Risk

the likelihood that cyber incidents will exploit vulnerabilities with an organization’s IT environment.

RISK ANALYSIS

Two ways to evaluate risk to assets: **qualitative** and **quantitative**

QUANTITATIVE

Assigns a dollar value to evaluate effectiveness of countermeasures

QUANTITATIVE

Assigns a **dollar value** to evaluate effectiveness of countermeasures

OBJECTIVE, uses formulas

QUANTITATIVE

Assigns a **dollar value** to evaluate effectiveness of countermeasures

To prioritize, often initially calculated using "impact x probability" score

QUALITATIVE

Uses a scoring system to rank threats and effectiveness of countermeasures

QUALITATIVE

Uses a **scoring system** to rank threats and effectiveness of countermeasures

SUBJECTIVE

QUALITATIVE

Uses a **scoring system** to rank threats and effectiveness of countermeasures

typically uses low/med/high or number scale

Formulas and Terms

Exposure Factor (EF). The % of value an asset lost due to an incident, represented in a **decimal**.

Single Loss Expectancy (SLE). How much would it cost you if it happened just ONE time?

SLE = Asset Value x Exposure Factor (SLE=AV*EF)

Annualized Rate of Occurrence (ARO). How many times does it happen in one year? Watch for AROs longer than 1 year!

Annualized Loss Expectancy (ALE). How much you will lose per year? ALE = SLE x ARO or AV x EF x ARO

Formulas and Terms

Annualized Rate of Occurrence (ARO). How many times does it happen in one year?

Watch for AROs longer than 1 year will be represented as a fraction. **EXAMPLE:** One occurrence every 5 years = 0.2

ARO = "Likelihood of occurrence"

Do not expect in-depth quantitative risk analysis on the exam. Do not worry about memorizing the formulas

Supporting Terms & Concepts

Asset Value (AV). Monetary value of the asset for which we are making calculations.

Safeguard Evaluation. Answers the question "is this safeguard cost effective?".

Organizations will not spend more than an asset's value to protect the asset!

Risk Analysis Steps (EXTRA CREDIT)

The six major steps in quantitative risk analysis

1. **Inventory assets** and assign a value *(asset value, or **AV**)*.
2. **Identify threats.** Research each asset and produce a list of all possible threats of each asset. *(and calculate **EF** and **SLE**)*
3. **Perform a threat analysis** to calculate the likelihood of each threat being realized within a single year. *(the **ARO** aka "likelihood of occ")*
4. **Estimate the potential loss** by calculating the *annualized loss expectancy* ***(ALE)***.
5. **Research countermeasures for each threat,** and then calculate the changes to **ARO** and **ALE** based on an applied countermeasure.
6. **Perform a cost/benefit analysis** of each countermeasure for each threat for each asset.

ENVIRONMENTAL (NATURAL) DISASTERS

Know the common types of **natural disasters** that may threaten an organization.

- Earthquakes
- Floods
- Storms
- Tsunamis
- Volcanic eruptions

PERSON-MADE DISASTERS

Know the common types of **person-made disasters** that may threaten an organization.

- Explosions
- Electrical fires
- Terrorist acts
- Power outages
- Other utility failures

INTERNAL VS EXTERNAL

How does disaster **location** factor in impact to the organization and influence DRP and BCP?

If an office is impacted, workers may be able to work from home.

Impact of an unavailable office will vary by type of business.

If a manufacturing facility, it may impact the organizations' ability to produce products.

Risks will vary by site, and impacts by site purpose

BUSINESS IMPACT ANALYSIS

Functional recovery plans

focuses on the steps required to restore critical business processes.

plans use structured walkthroughs, tabletop exercises, and simulations.

Single point of failure

any non-redundant part of a system that, if unavailable, would cause the entire system or service to fail.

undesirable in any system that requires high availability and reliability, such as supply chains, networks, and applications.

BUSINESS IMPACT ANALYSIS

Recovery Point Objective (RPO) | is the age of data that must be recovered from backup storage for normal operations to resume if a system or network goes down

Recovery Time Objective (RTO) | is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

SLAs between a company and customers will influence RPO and RTO

BCP DEFINITIONS

Important BCP-related definitions for the exam

Business Impact Analysis (BIA)
the process of assessing the impact of disasters to the business, including lost sales, recovery costs, etc.

BIA looks at financial loss following a disaster.

BCP (Business Continuity Plan)
the overall organizational plan for "how-to" continue business. Business-focused

DRP (Disaster Recovery Plan)
the plan for recovering from an IT disaster and having the IT infrastructure back in operation. Tech-focused

BUSINESS IMPACT ANALYSIS

Mission essential functions | part of business impact assessment that determines what the company's mission-essential (business-critical) functions are.

Identification of critical systems | the process of identifying the systems that are required to support mission essential functions of the organization.

BIA findings, including these areas, will influence BCP and DRP

Site Risk Assessment

Assesses the security risk of a specific location (site) planned for use (or in use) to meet a business purpose.

Site Risk Assessment

will assess a variety of risks from exposure to natural and person-made disasters and other events

...that may impact business operations or human safety

BCP DEFINITIONS

Important BCP-related definitions for the exam

MTBF (Mean Time Between Failures)

a time determination for how long a piece of IT infrastructure will continue to work before it fails.

MTTR (Mean Time to Repair)

a time determination for how long it will take to get a piece of hardware/software repaired and back on-line.

GOALS OF BCP AND DRP

What are the core **goals** of disaster recovery and business continuity planning?

Minimizing the effects of a disaster by:

Improving responsiveness by the employees in different situations.

Easing confusion by providing written procedures and participation in drills.

Helping **make logical decisions** during a crisis.

An auditor assessing BIA will likely focus primarily on **single points of failure**, **RPO** and **RTO** in assessing the efficacy of the organizations plan.

5.0 GOVERNANCE, RISK, AND COMPLIANCE

5.5 Explain privacy and sensitive data concepts in relation to security

- **Organizational consequences of privacy and data breaches**
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- **Notifications of breaches**
  - Escalation
  - Public notifications and disclosures
- **Data types**
  - Classifications
  - Public
  - Private
  - Sensitive
  - Confidential
  - Critical
  - Proprietary
  - Personally identifiable information (PII)
  - Health information
  - Financial information
  - Government data
  - Customer data
- **Privacy enhancing technologies**
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- **Roles and responsibilities**
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data protection officer (DPO)
- **Information life cycle**
- **Impact assessment**
- **Terms of agreement**
- **Privacy notice**

CONSEQUENCES OF PRIVACY AND DATA BREACHES

Reputational Damage effects may last for years!

can result in loss of customer trust and loss of revenue.

Identity theft

involves someone using a person's private information to impersonate that individual, usually for financial gain.

Intellectual Property (IP) Theft

might quickly cost customers, credit ratings, and brand reputation.

losing IP could mean forfeiture of first-to-market advantage, loss of profitability, or even an entire lines of business to competitors or counterfeiters.

Fines and may lead to lawsuits

failing to report a breach can result in fines that can reach into the millions of dollars.

GDPR outlines fines of up to 4% of a company's annual global revenues or 20 million euros for failing to report a breach.

ANY company with a customer in the EU is subject to GDPR

NOTIFICATIONS OF BREACHES

Data Breach Notifications/Laws

If a data breach occurs, failing to report a breach can result in fines that can reach into the millions of dollars.

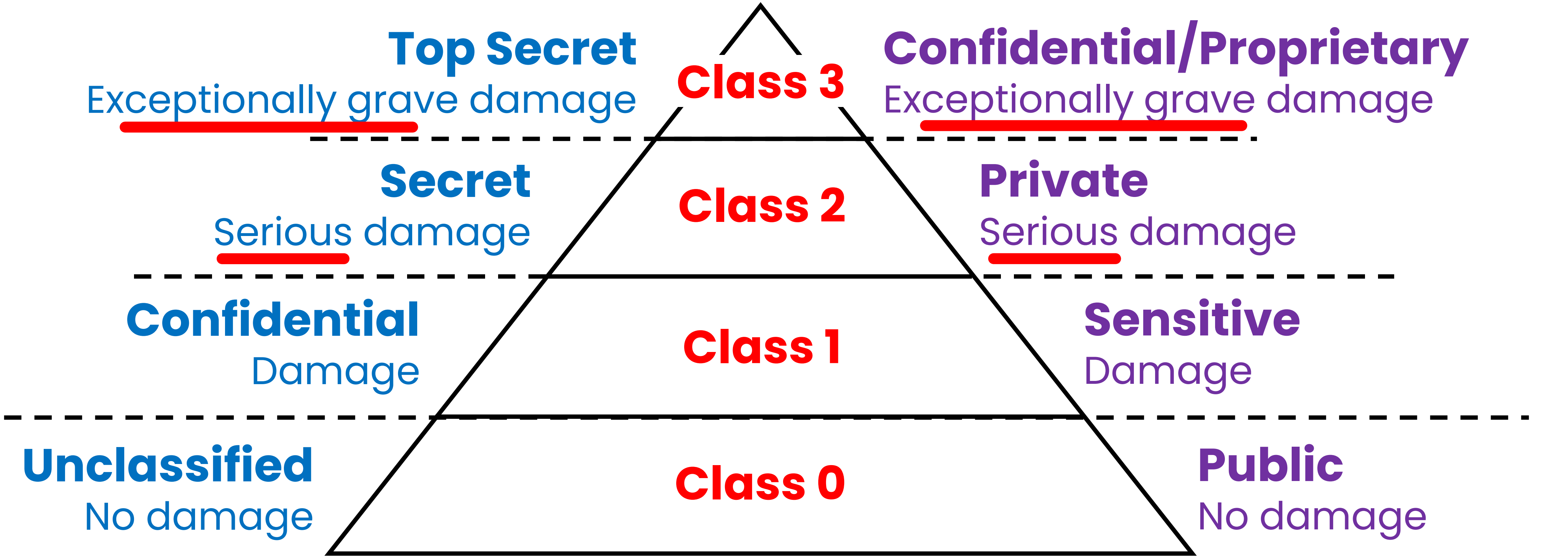
The EU sets their standard GDPR, and notifications of data breaches must be reported within 72 hours.

Escalations. to external sources, like law enforcement or outside experts to stop/investigate breach.

Other countries have their own reporting timescale.

Delays sometimes allowed for criminal investigation

DATA CLASSIFICATIONS



Government		Non-gov't (public)
Top Secret Exceptionally grave damage	**Class 3**	**Confidential/Proprietary** Exceptionally grave damage
Secret Serious damage	**Class 2**	**Private** Serious damage
Confidential Damage	**Class 1**	**Sensitive** Damage
Unclassified No damage	**Class 0**	**Public** No damage

Defining Sensitive Data

Sensitive data is any information that isn't public or unclassified.

Personally Identifiable Information (PII). any information that can identify an individual (name, SSN, birthdate/place, biometric records, etc)

Protected Health Information (PHI). and health-related information that can be related to a specific person. covered by HIPAA

DATA TYPES

Other sensitive data types you should know for the exam:

Critical Data: data that a company does not want to disclose; could also be classified and encrypted to prevent someone from reading it.

Proprietary Data: data generated by a company, such as its trade secrets, or work done by the R&D department.

Financial Information: data about a company's bank account, share capital, and any investments that it has made. It could also be credit card and payroll data.

Customer Data: data held about individual customers of an organization that should never be divulged.

Information of an account manager or representative at a business dealing with a customer is also classified as customer data.

Government Data: data collected by governmental agencies, and there are strict rules on how it can be shared, normally only internally.

government often have strict rules contractors must follow when the contract has finished, and the data used in the contract is to be disposed of.

→ They CANNOT simply delete the data!

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner. Usually a member of senior management. Can delegate some day-to-day duties. Cannot delegate total responsibility.

Data Custodian. Usually someone in the IT department. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

DATA ROLES AND RESPONSIBILITIES

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner. Usually a member of senior management. Can delegate some day-to-day duties. Cannot delegate total responsibility.

Data Custodian. Usually someone in the IT department. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

GDPR Terms and Requirements

Be prepared to answer questions on other roles

Data Processor. A natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller.

Data Controller. The person or entity that controls processing of the data.

Data Protection Officer (DPO). Under GDPR, the DPO is a mandatory appointment within an organization.

DPO ensures the organization complies with data regulations

PRIVACY ENHANCING TECHNOLOGIES

Tokenization

Stateless, stronger than encryption, keys not local

where meaningful data is replaced with a token that is generated randomly, and the original data is held in a vault.

Pseudo-Anonymization

Reversal requires access to another data source

de-identification procedure in which personally identifiable information (PII) fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

PRIVACY ENHANCING TECHNOLOGIES

Anonymization

process of removing all relevant data so that it is impossible to identify original subject or person.

Only effective if you do NOT need the identity data!

Data minimization

only necessary data required to fulfill the specific purpose should be collected

Collect "the minimum amount" to meet the stated purpose and manage retention to meet regulations

Data masking

when only partial data is left in a data field.

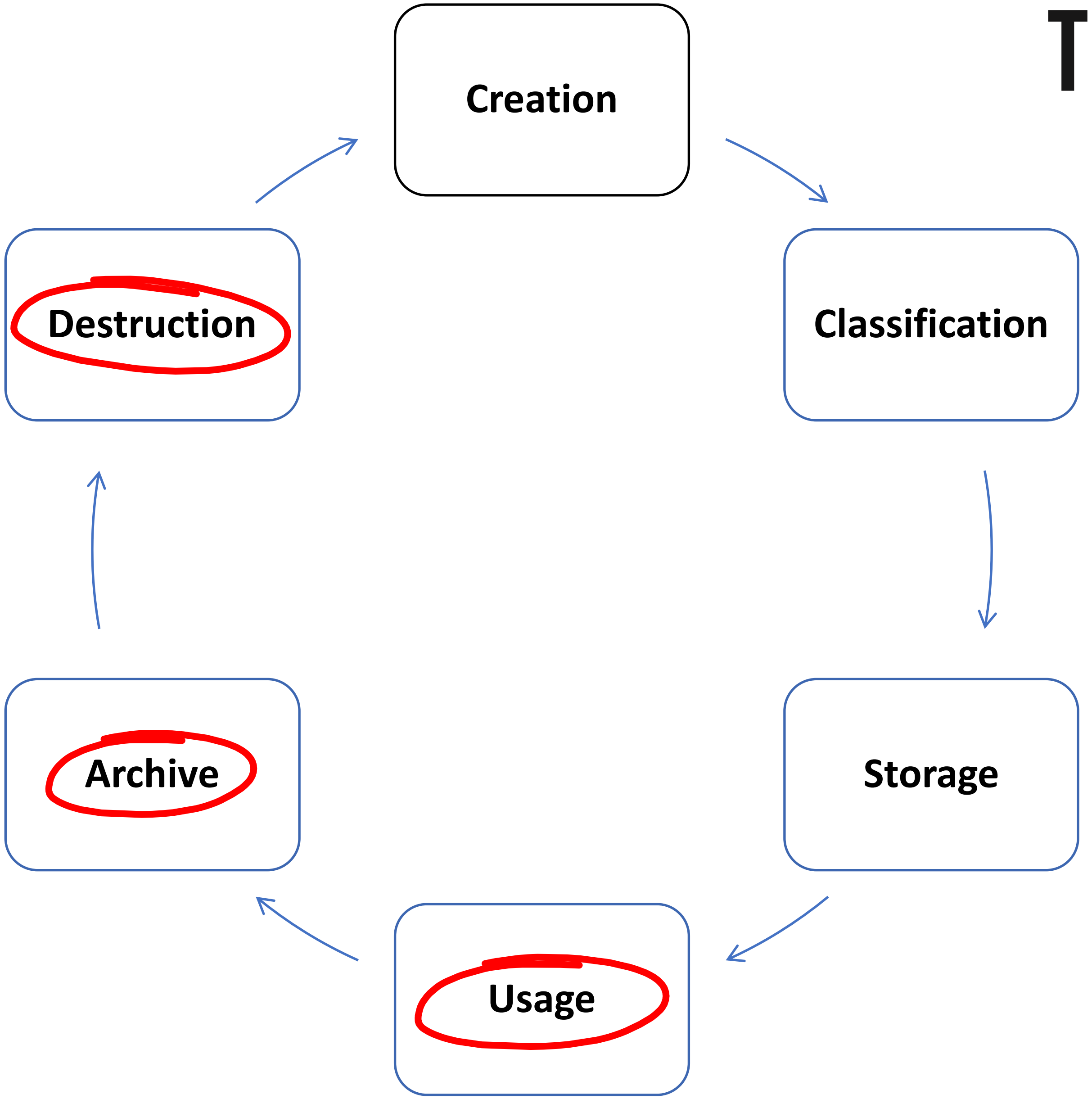
for example, a credit card may be shown as

**** **** **** 1234

Commonly implemented within the database tier, but also possible in code of frontend applications

THE INFORMATION LIFECYCLE

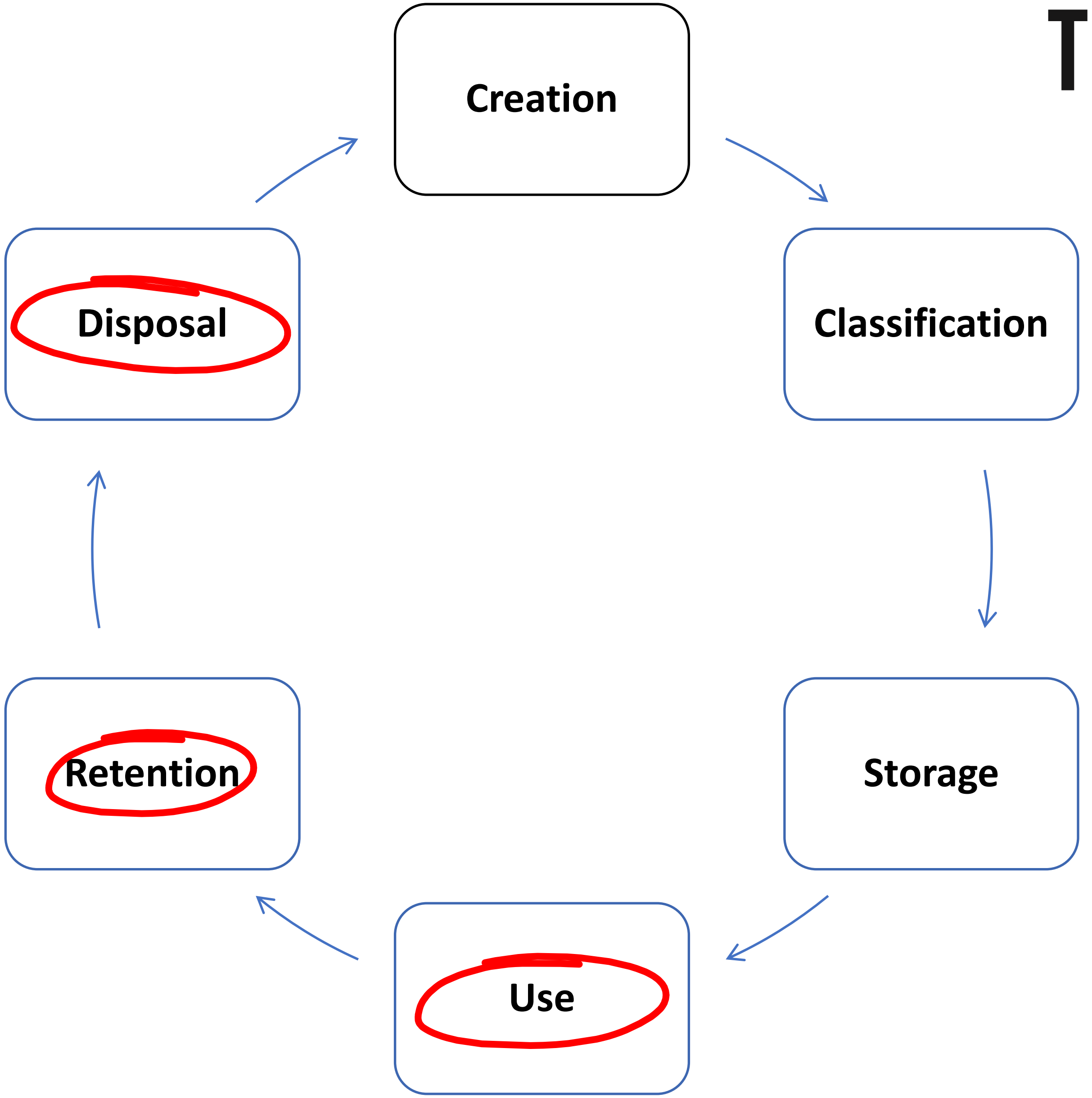
What we covered in DOMAIN 4



What do you need for the exam?

THE INFORMATION LIFECYCLE

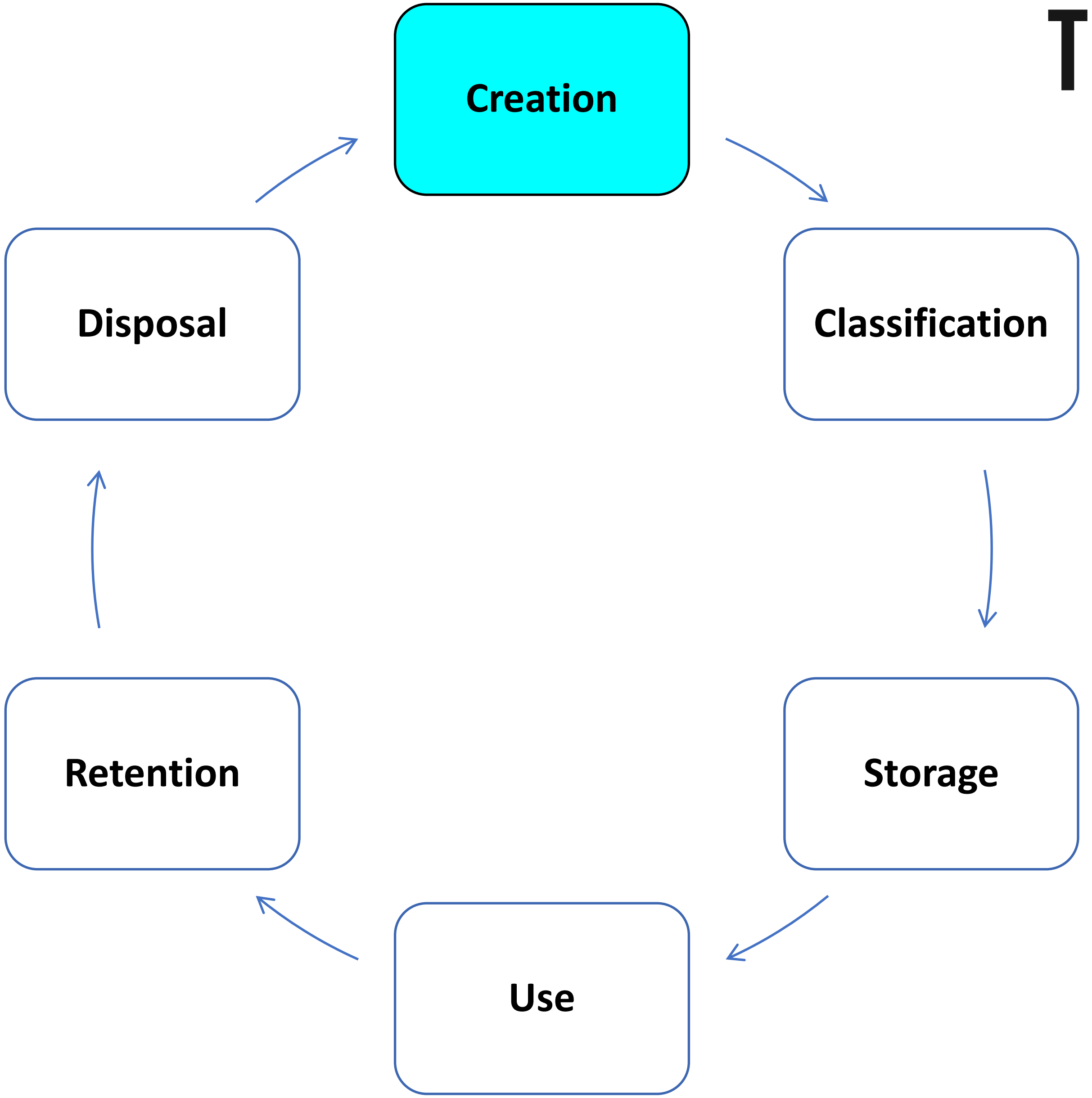
What we covered in DOMAIN 4



What you need for exam day is simpler than this!

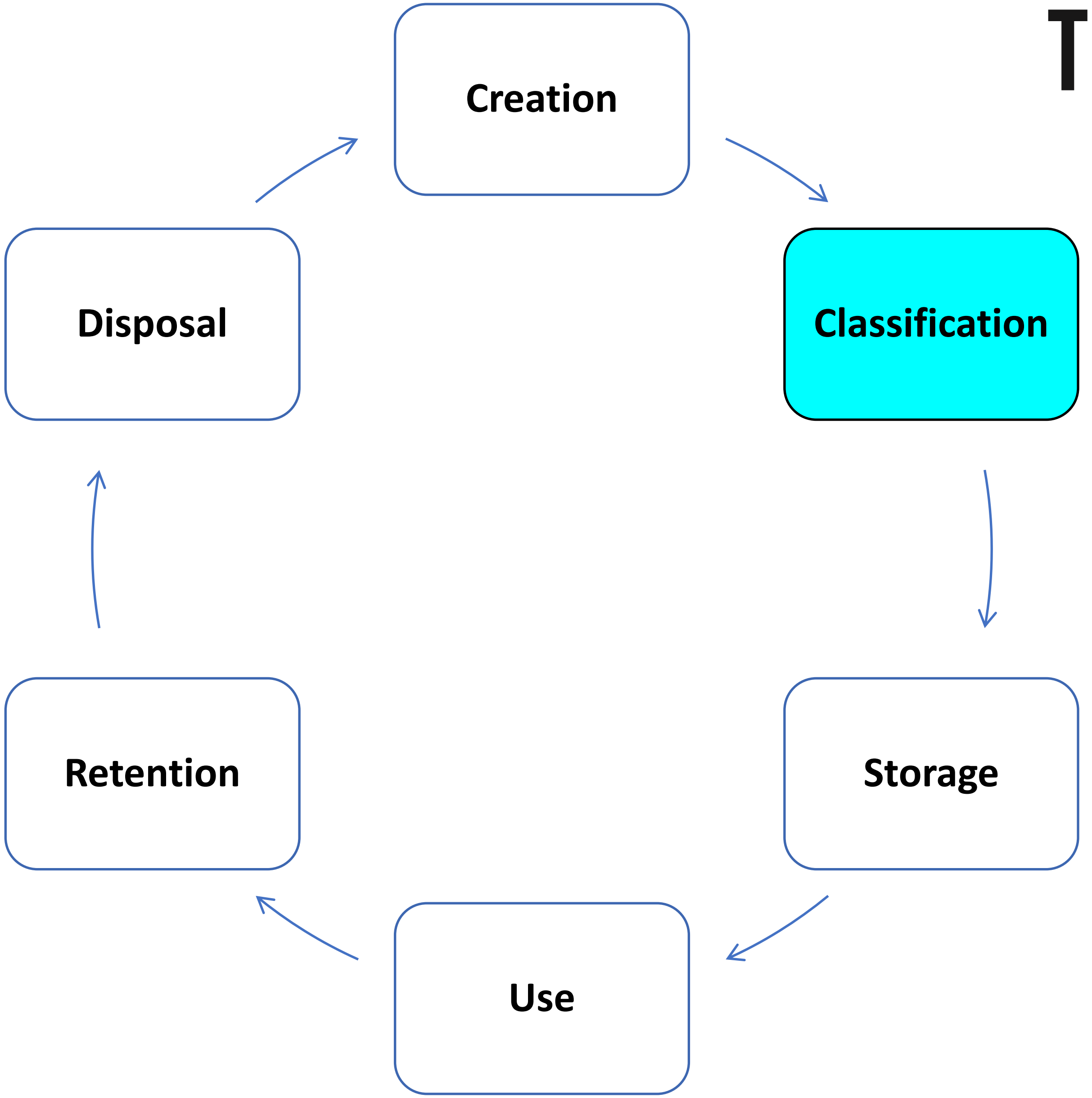
THE INFORMATION LIFECYCLE

What we covered in DOMAIN 4



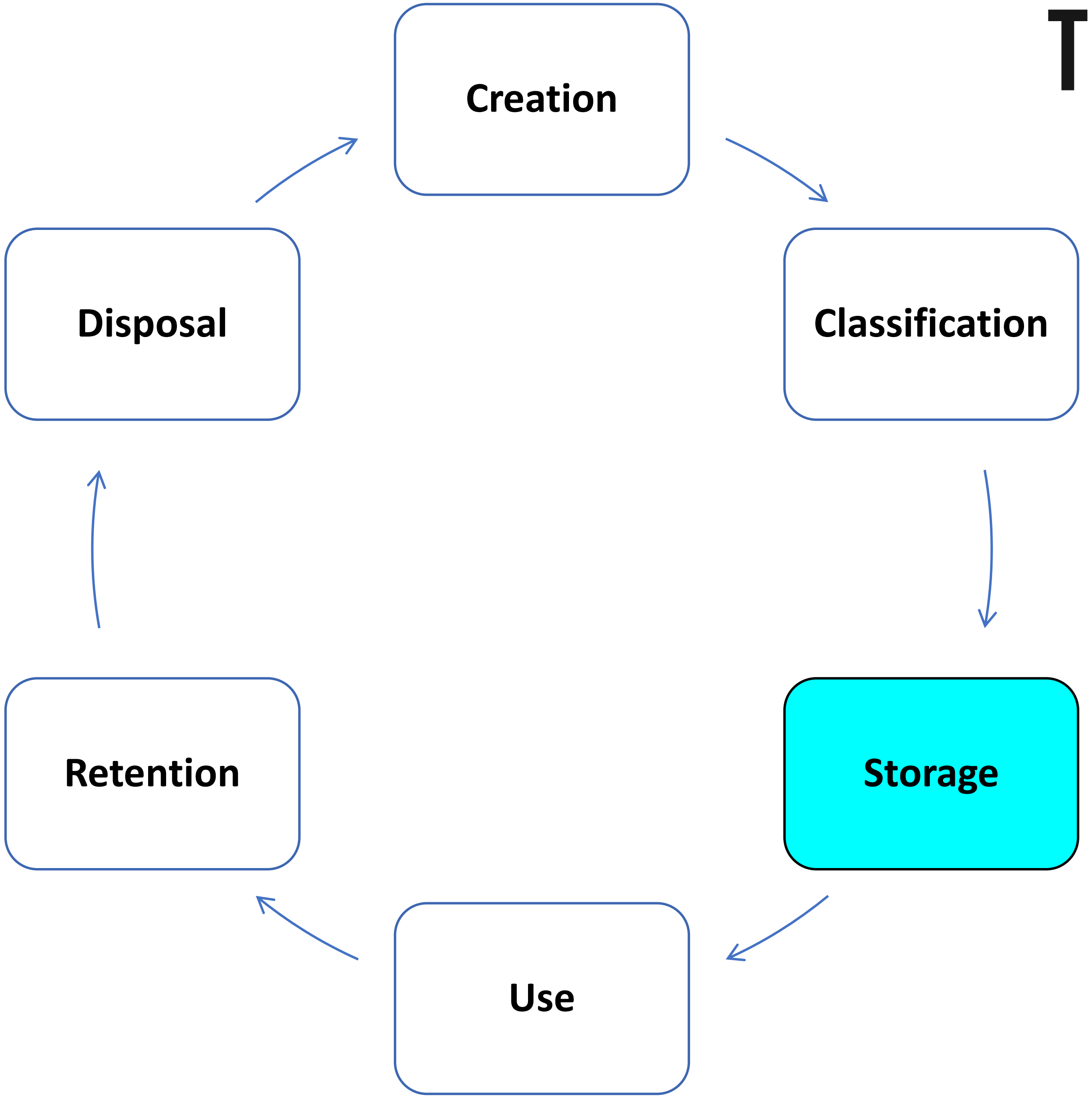
THE INFORMATION LIFECYCLE

What we covered in DOMAIN 4



THE INFORMATION LIFECYCLE

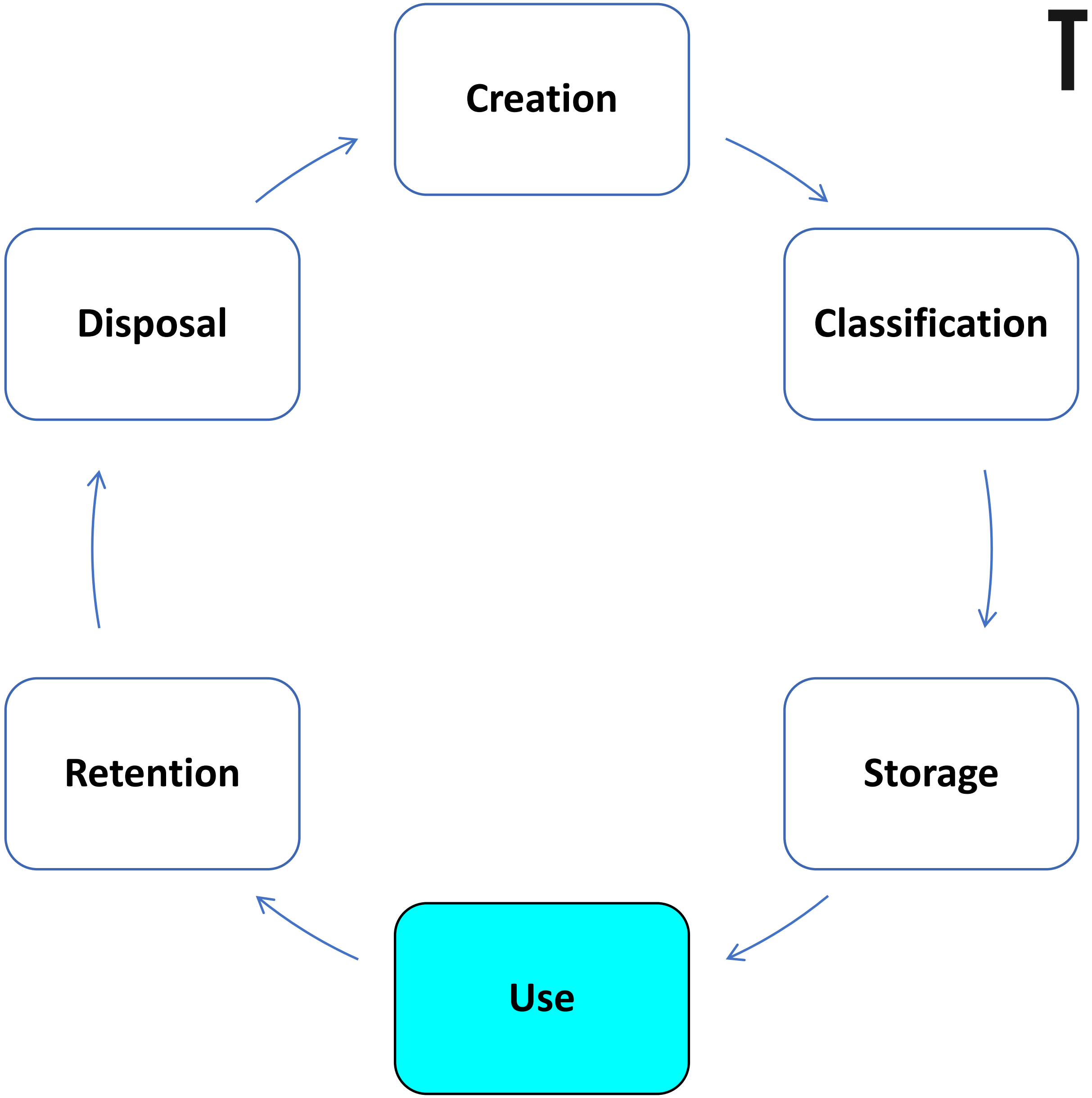
What we covered in DOMAIN 4



Data should be **protected** by adequate security controls based on its classification.

THE INFORMATION LIFECYCLE

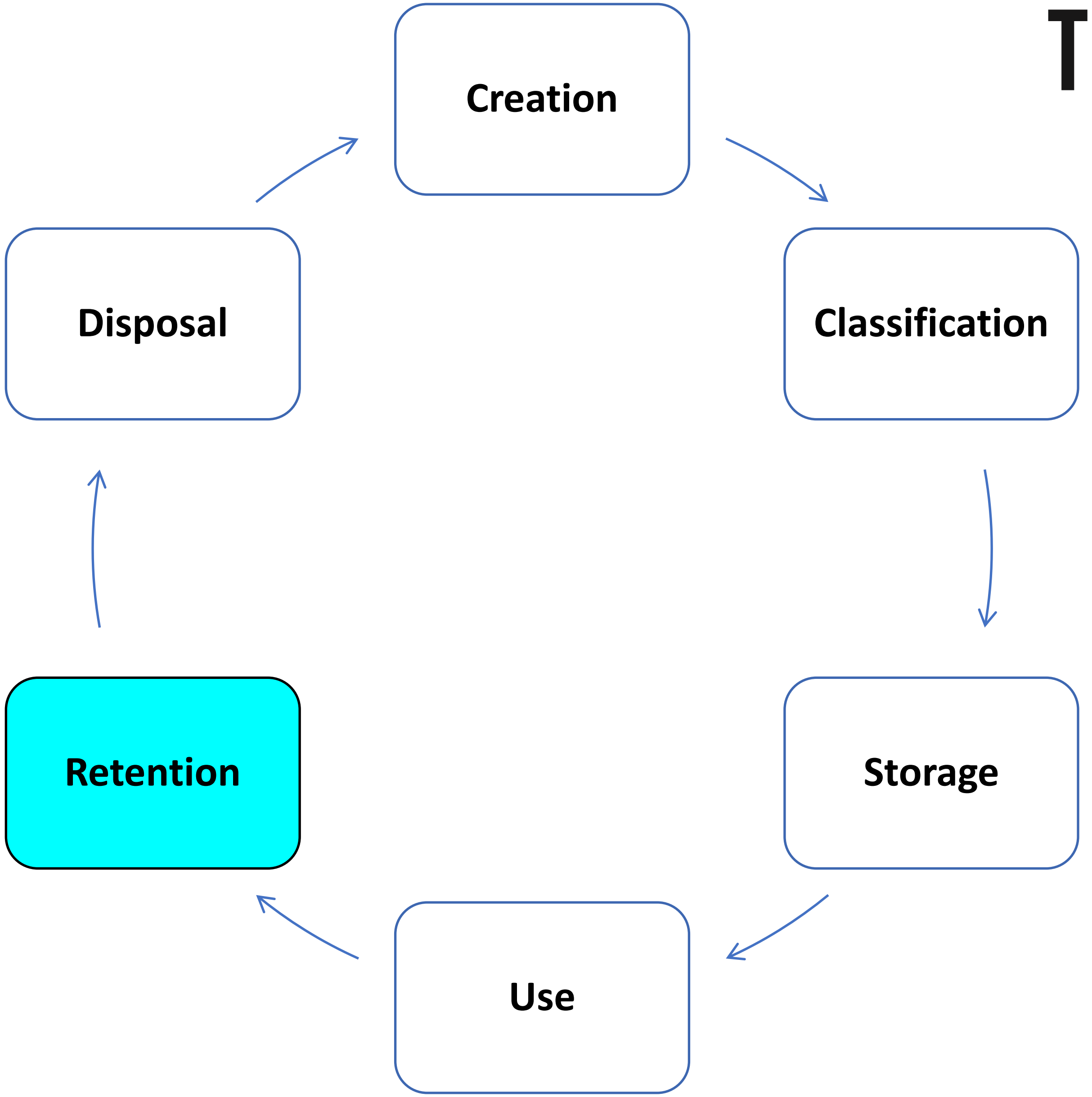
What we covered in DOMAIN 4



refers to anytime data is in use or in transit over a network

THE INFORMATION LIFECYCLE

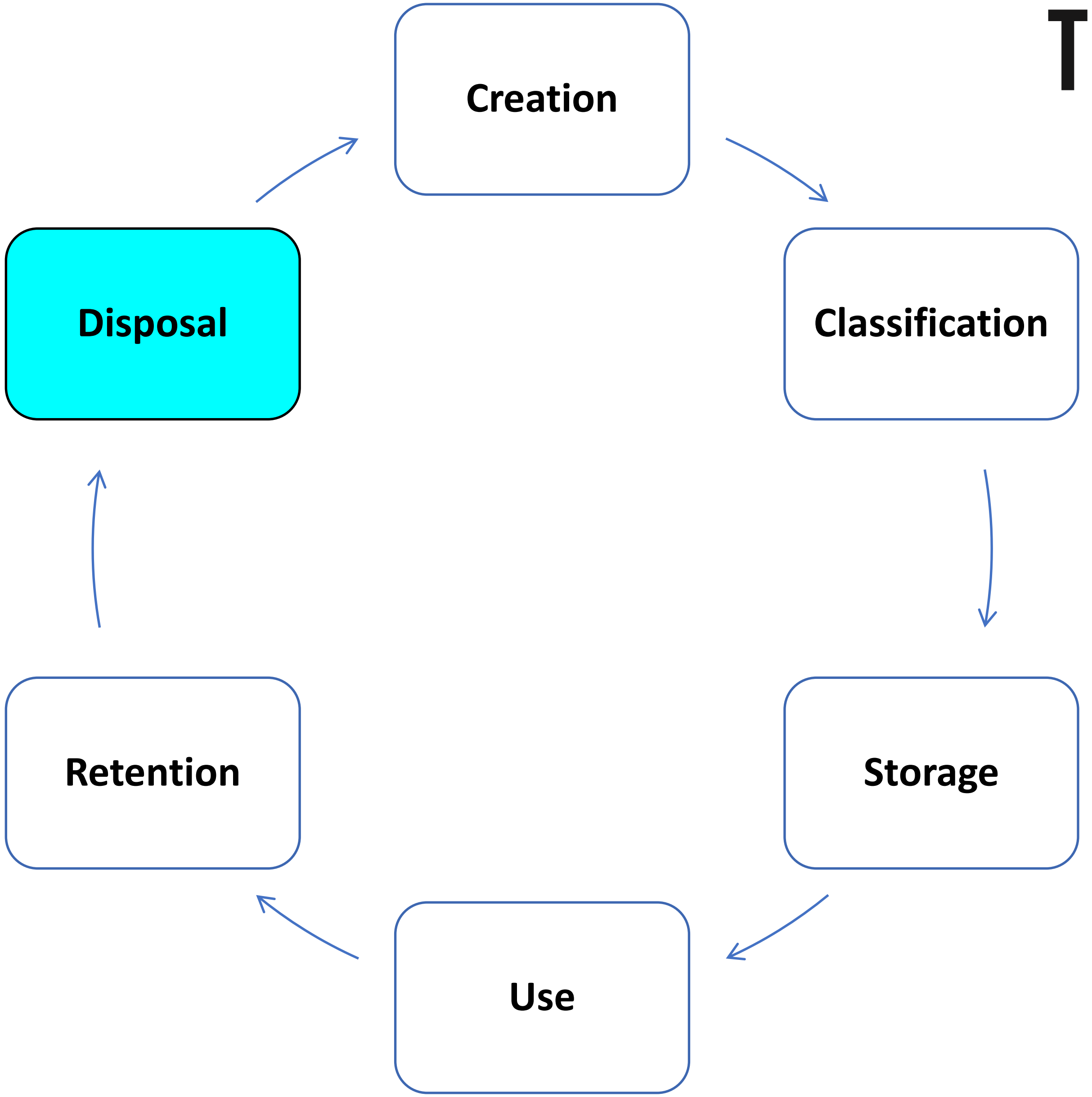
What we covered in DOMAIN 4



archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

THE INFORMATION LIFECYCLE

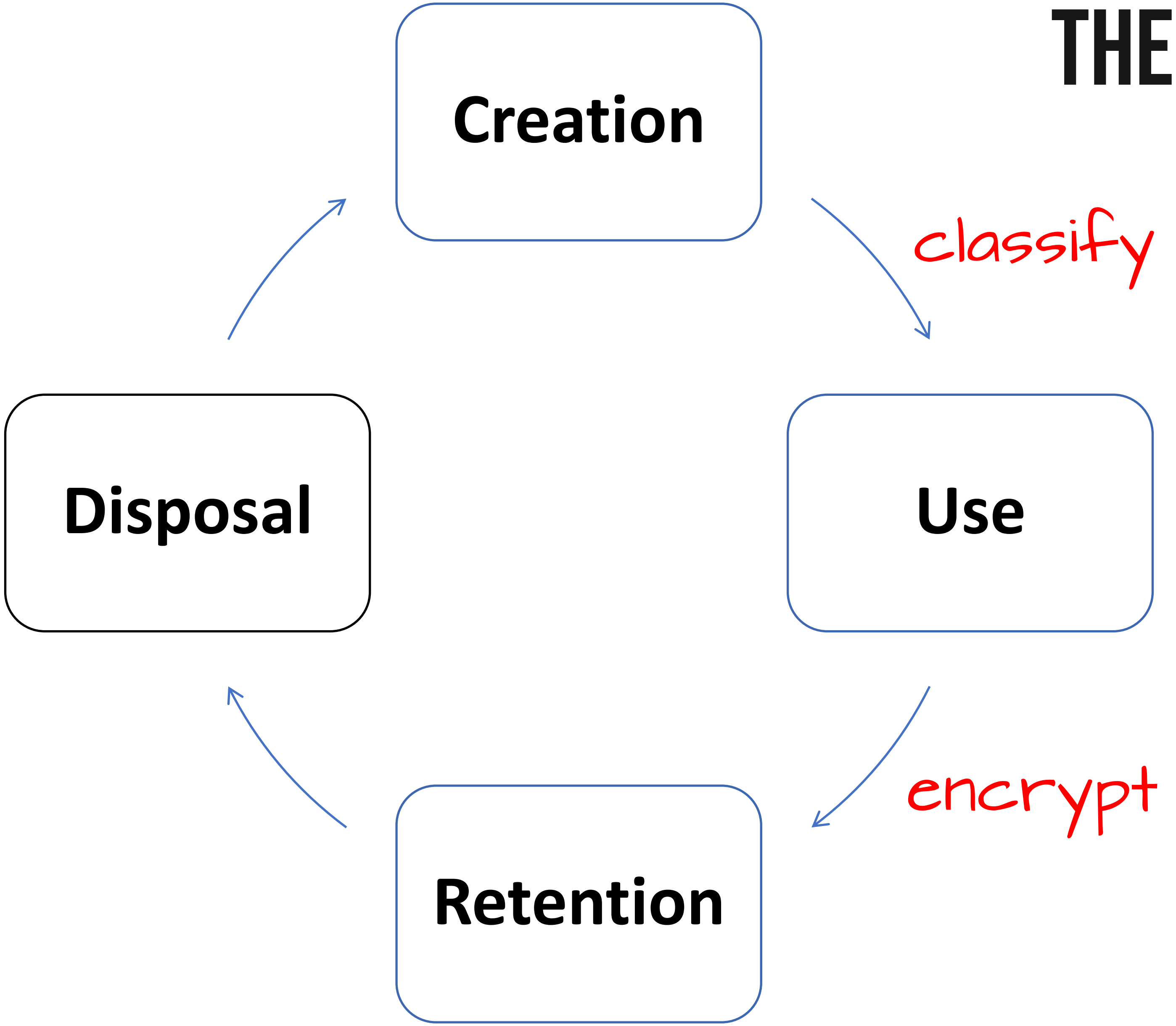
What we covered in DOMAIN 4



When data is no longer needed, it should be destroyed in such a way that it is not readable.

THE INFORMATION LIFECYCLE

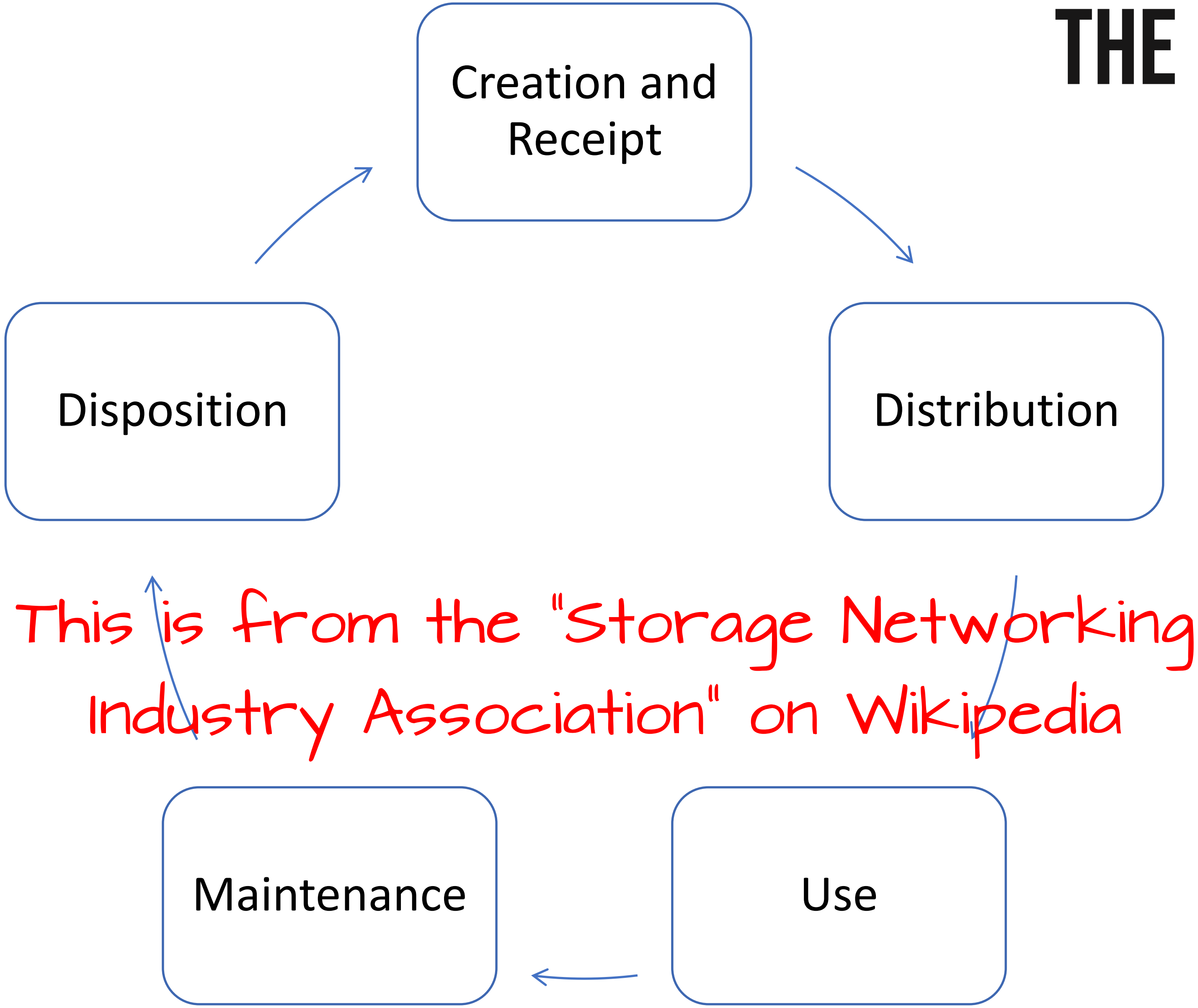
For the Security+ exam



One study guide presented this.

THE INFORMATION LIFECYCLE

For the Security+ exam



This is from the "Storage Networking Industry Association" on Wikipedia

Others showed this as the info lifecycle

THE INFORMATION LIFECYCLE

For the Security+ exam

This is the diagram from the official study guide (no diagram)

IMPACT ASSESSMENT

Impact Assessment

Assesses the potential impact to data security and privacy.

Can help Security identify appropriate security controls.

Should be conducted for new services, projects, and initiatives.

Helps the company avoid data breach!

Enables proactive identify and remediate issues before they become a production issue

TERMS OF AGREEMENT

Terms of Agreement Protects the company

May also be called “terms of service” or “terms and conditions”

Tells the customer what will be legally required of them if they subscribe to your service or download and use your mobile app.

User must agree to the terms to use the service.

NOT required by law, but reduces risk to the company

Privacy Notice Protects the customer (user)

May also be called “privacy policy”

Documents handling of personal data, answers questions like:

-What data is collected and for what purpose?

-With whom will data be shared?

Required by law in many regions/countries

INSIDE CLOUD

AND SECURITY

THANKS

FOR WATCHING!