CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 7

Security Operations

INSIDE CLOUD AND SECURITY

INTRODUCTION: CISSP EXAM DOMAINS

DOMAINS	WEIGHT	
1. Security and Risk Management	15%	
2. Asset Security	10%	
3. Security Architecture and Engineering	13%	
4. Communication and Network Security	14%	
5. Identity and Access Management	13%	
6. Security Assessment and Testing	12%	
7. Security Operations	13%	(this video)
8. Software Development Security	10%	

Exam Outline

7.1 Understand and comply with investigations

7.2 Conduct logging and monitoring activities

7.3 Perform Configuration Management

7.4 Apply foundational security operations concepts

7.5 Apply resource protection

7.6 Conduct incident management

7.7 Operate and maintain detective and preventative measures

Exam Outline

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.10 Implement recovery strategies

7.11 Implement Disaster Recovery (DR) processes

Exam Outline

7.12 Test Disaster Recovery Plans (DRP)

7.13 Participate in Business Continuity (BC) planning and exercises

7.14 Implement and manage physical security

7.15 Address personnel safety and security concerns

WHAT'S NEW IN DOMAIN 7?

7.4 Securely provisioning resources ← REMOVED

New technologies (in existing sub-domains):

- threat feeds
- user and entity behavior analytics (UEBA)
- next generation firewalls
- web application firewalls
- use of machine learning and artificial intelligence

covering all these now!

MODERN FIREWALLS

Covered with other FW types in DOMAIN 4

Firewalls

Web Application

aka "WAF"

protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

typically protects web applications from attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewalls

Next Generation

aka "NGFW"

a "deep-packet inspection" firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

INTELLIGENCE IN THREAT MODELING

UEBA

User and Entity Behavior Analytics

entity behavior is collected and input into a threat model

model establishes a baseline of "normal" based on historical data

enables analysis to uncover more details around anomalous events

'automated investigation' also exists in some platforms

INTELLIGENCE IN THREAT MODELING

Threat Intelligence

threat feeds

Activities an organization undertakes to educate itself about changes in the threat landscape

often a feed containing malicious entities ingested by cybersecurity tools

A single feed may be comprised of many sources, including open-source intelligence

entity = IP, website, threat actor, file hash, and more

THE ROLE OF AI & ML

Analyzing and improving cybersecurity posture is no longer a human-scale problem. Artificial Intelligence (AI) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.

THE ROLE OF AI & ML

Along with AI, machine learning (ML) has become critical technologies in information security, in quickly analyzing millions of events and identify many different types of threats

THE ROLE OF AI & ML

Histories of behavior build profiles on users, assets, and networks, allowing AI to detect and respond to deviations from established norms.

know that AI and ML factor in anti-malware, SIEM, IPS/IDS, and IDaaS, and more

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.

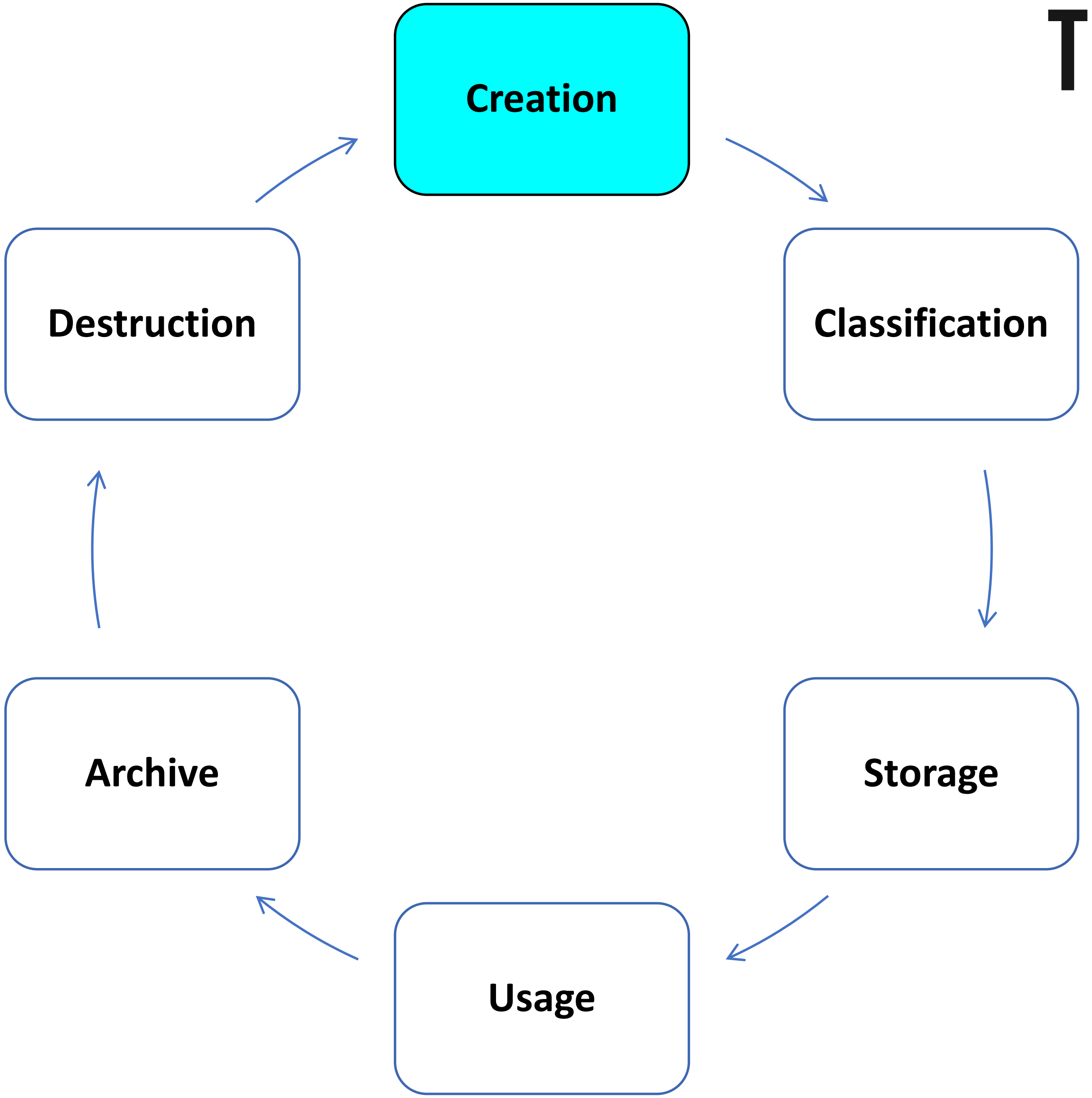
it's important to monitor all assignment of privileges and the use of privileged operations.

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

THE INFORMATION LIFECYCLE



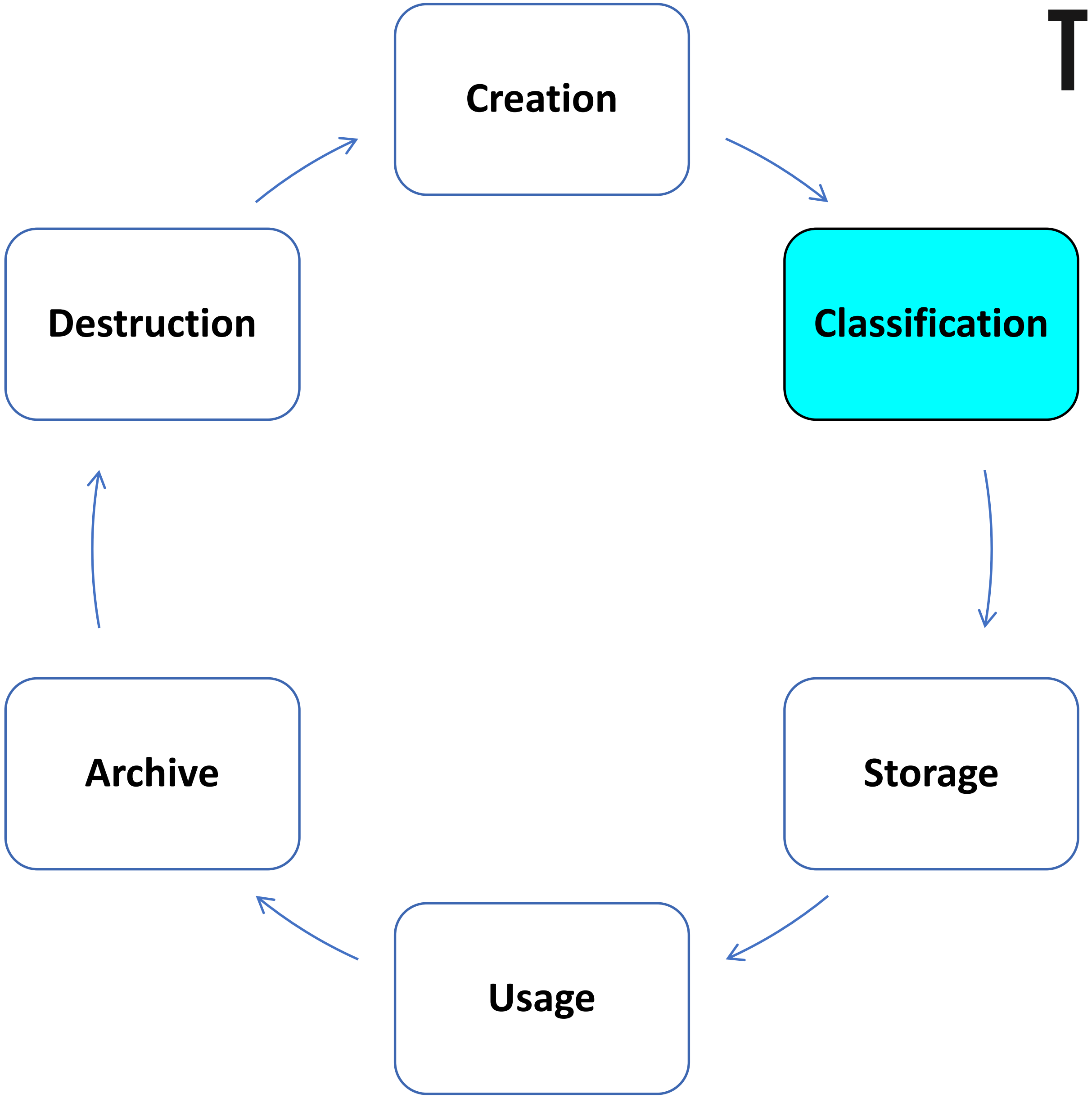
Can be created by **users**

a user creates a file

Can be created by **systems**

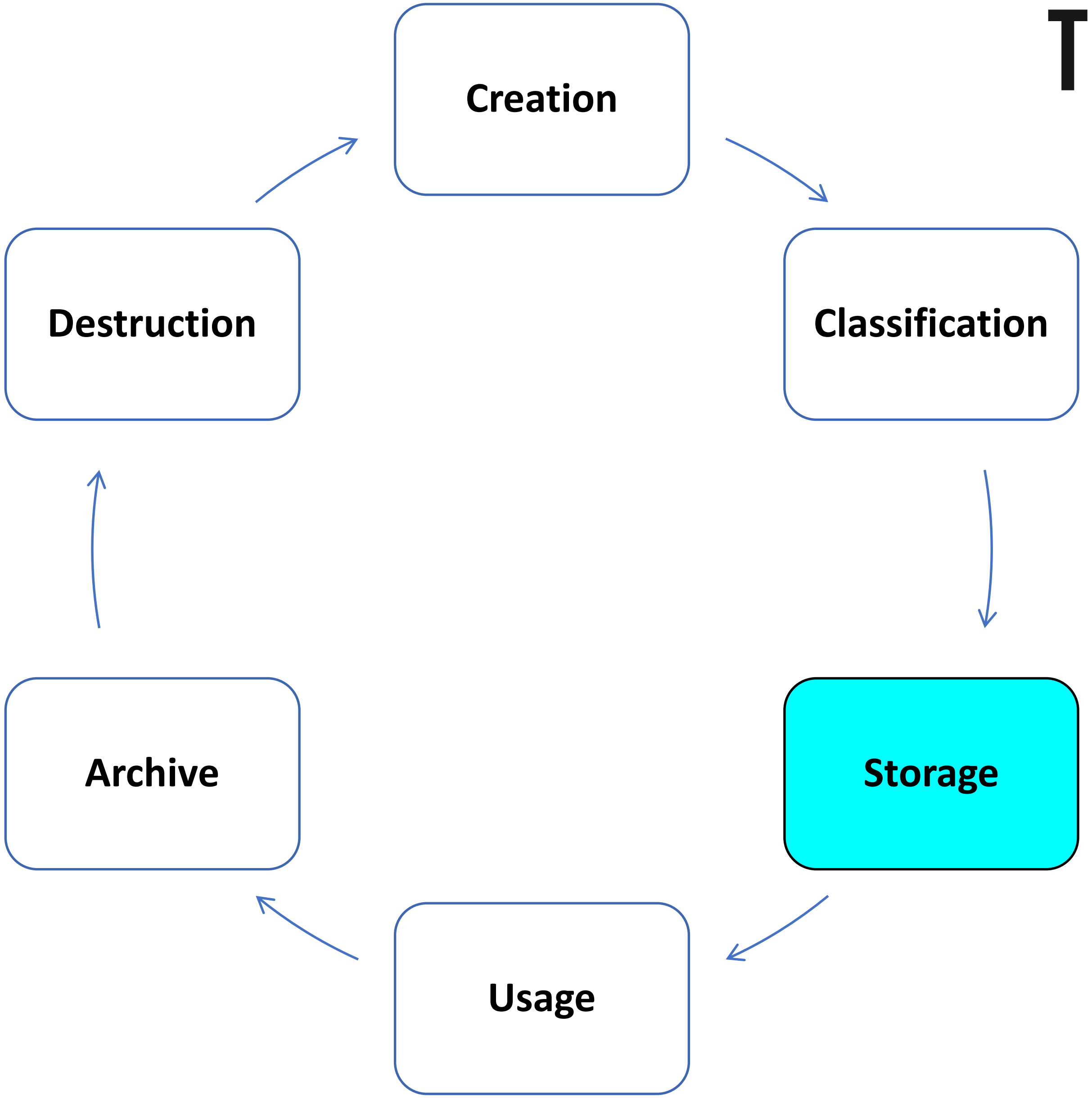
a system logs access

THE INFORMATION LIFECYCLE



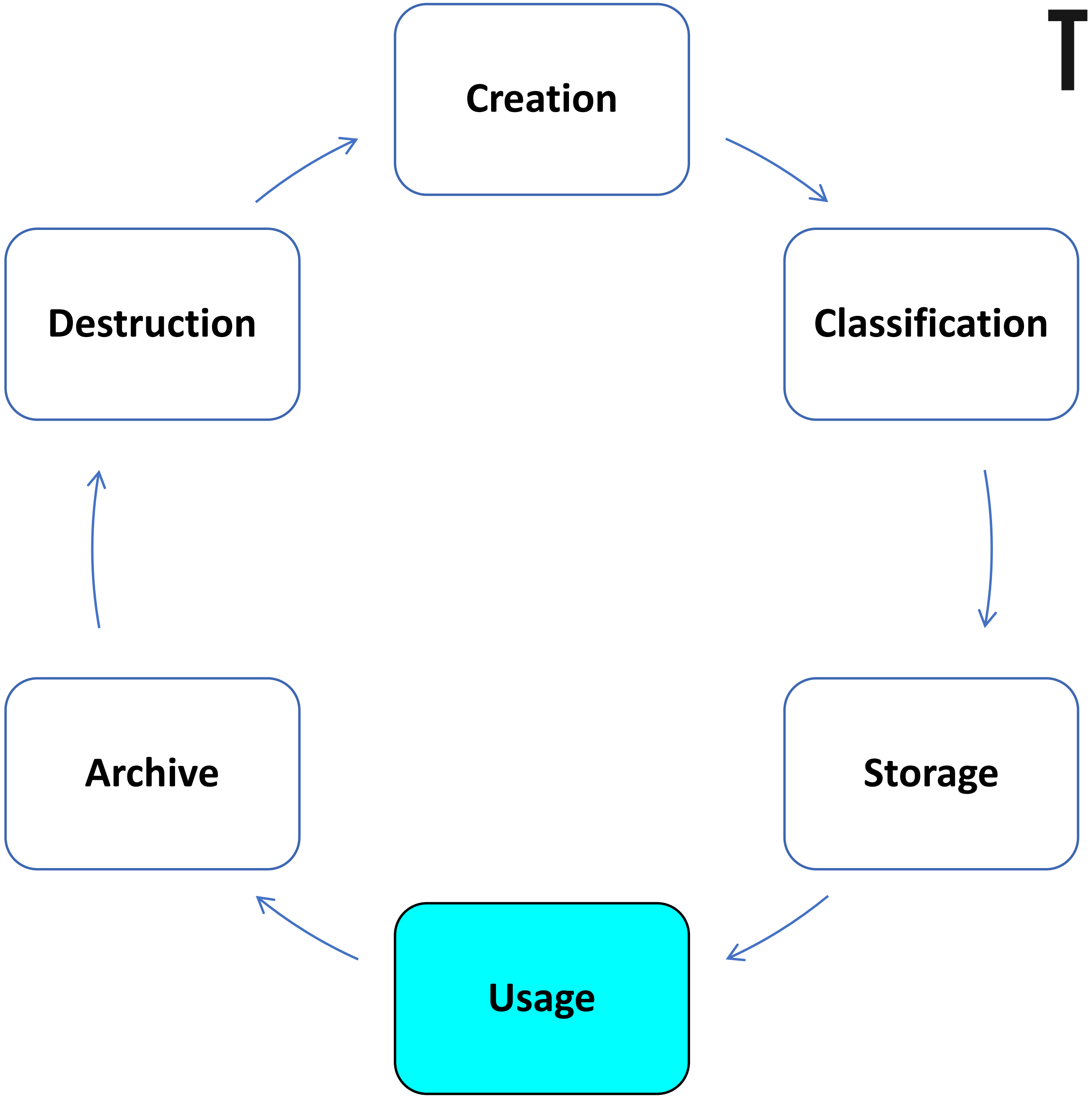
To ensure it’s handled properly, it’s important to ensure data is **classified** as soon as possible.

THE INFORMATION LIFECYCLE



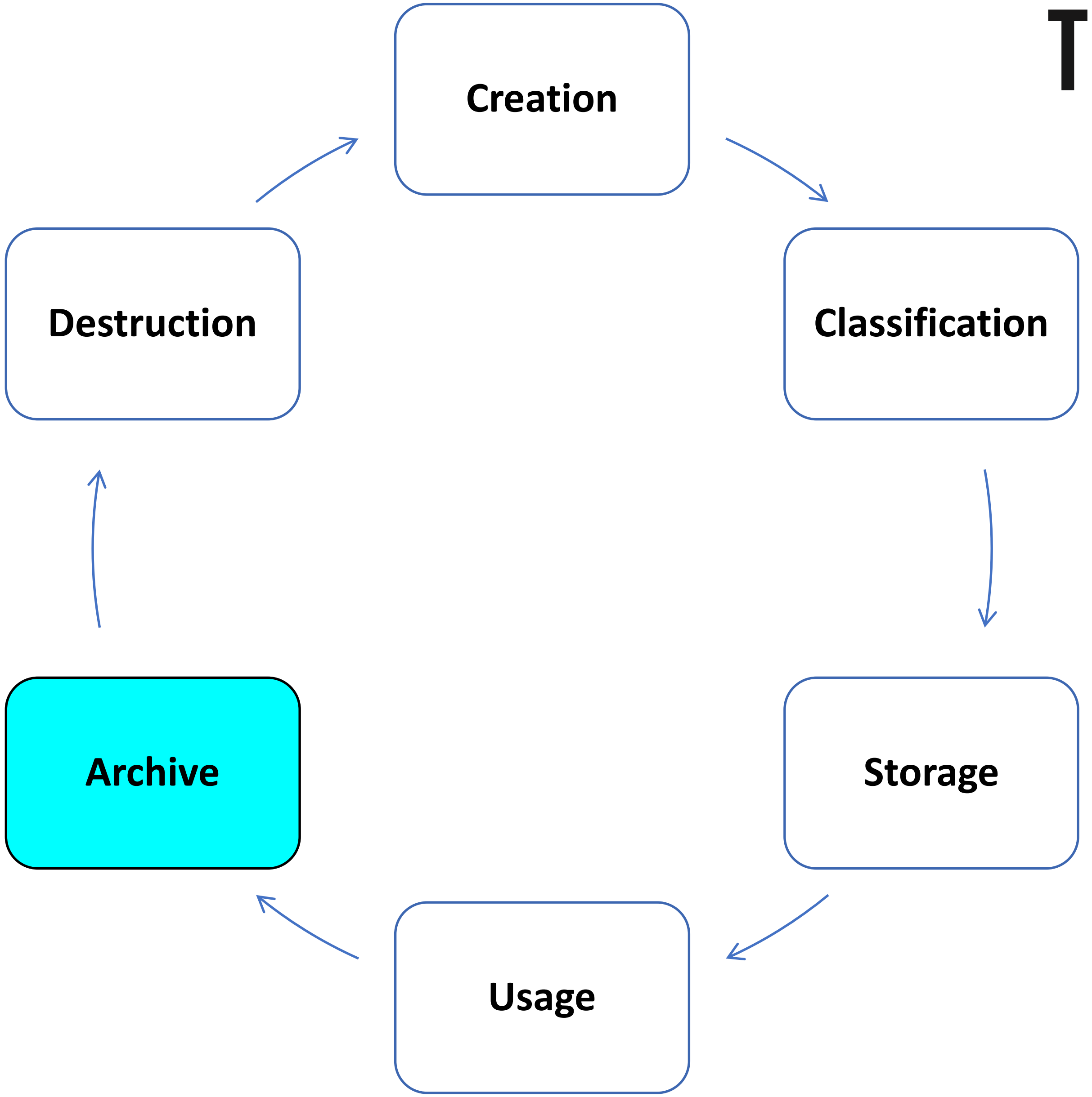
Data should be **protected** by adequate security controls based on its classification.

THE INFORMATION LIFECYCLE



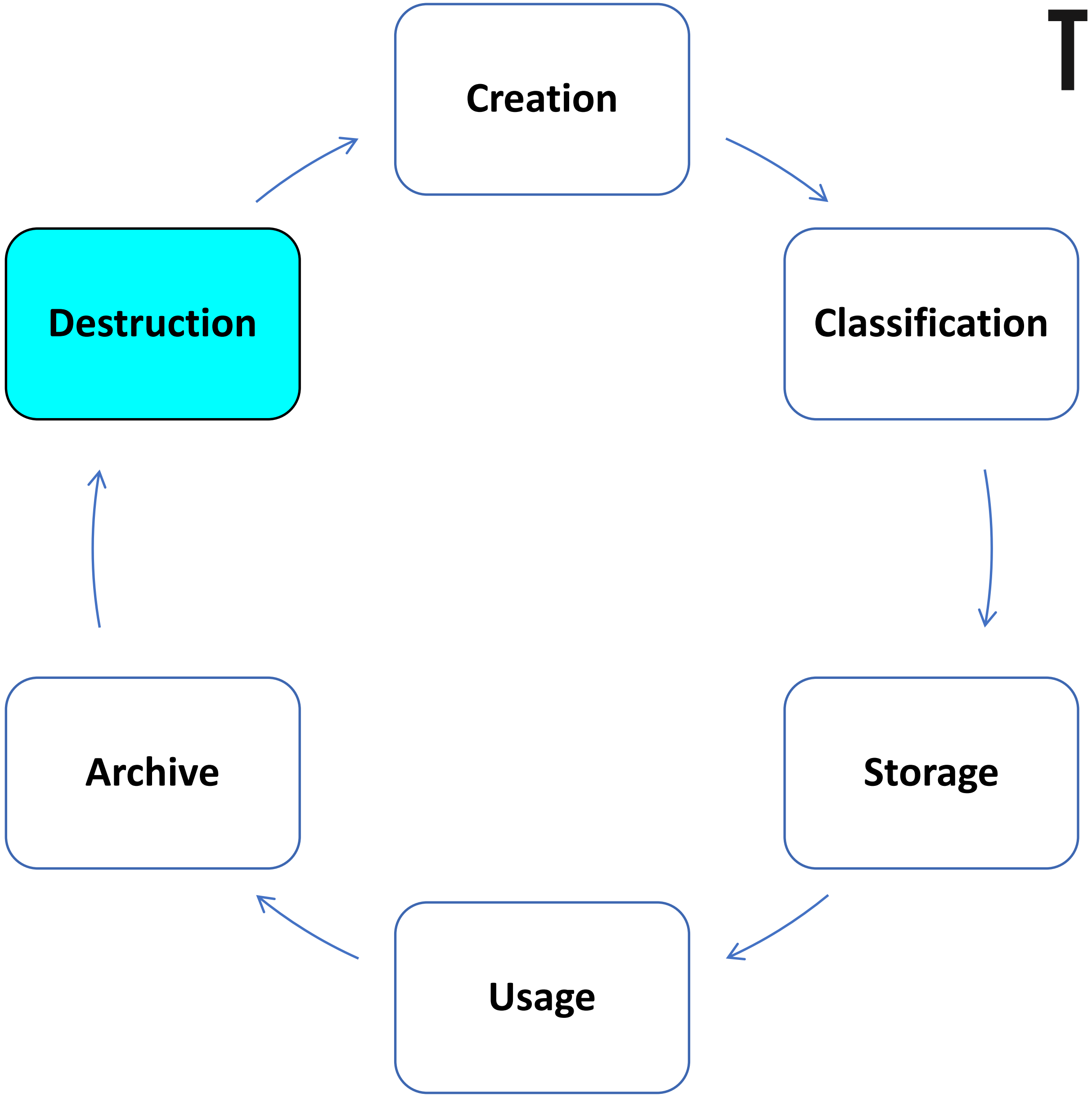
refers to anytime data is in use or in transit over a network

THE INFORMATION LIFECYCLE



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

THE INFORMATION LIFECYCLE



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

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

SECURE PROVISIONING

of resources includes ensuring that resources are deployed in a secure manner and maintained in a secure manner throughout their lifecycles.

example: deploy a PC from a secure image

VIRTUAL ASSETS

Virtual assets include:

- virtual machines (VM)
- virtual desktop infrastructure (VDI)
- software-defined networks (SDN)
- virtual storage area networks (SAN)

compute

network

storage

Hypervisors are the primary component that manages virtual assets, but also provide attackers with an additional target.

Both hypervisors and VMs need to be patched

VIRTUAL ASSETS

Security issues with cloud-based assets

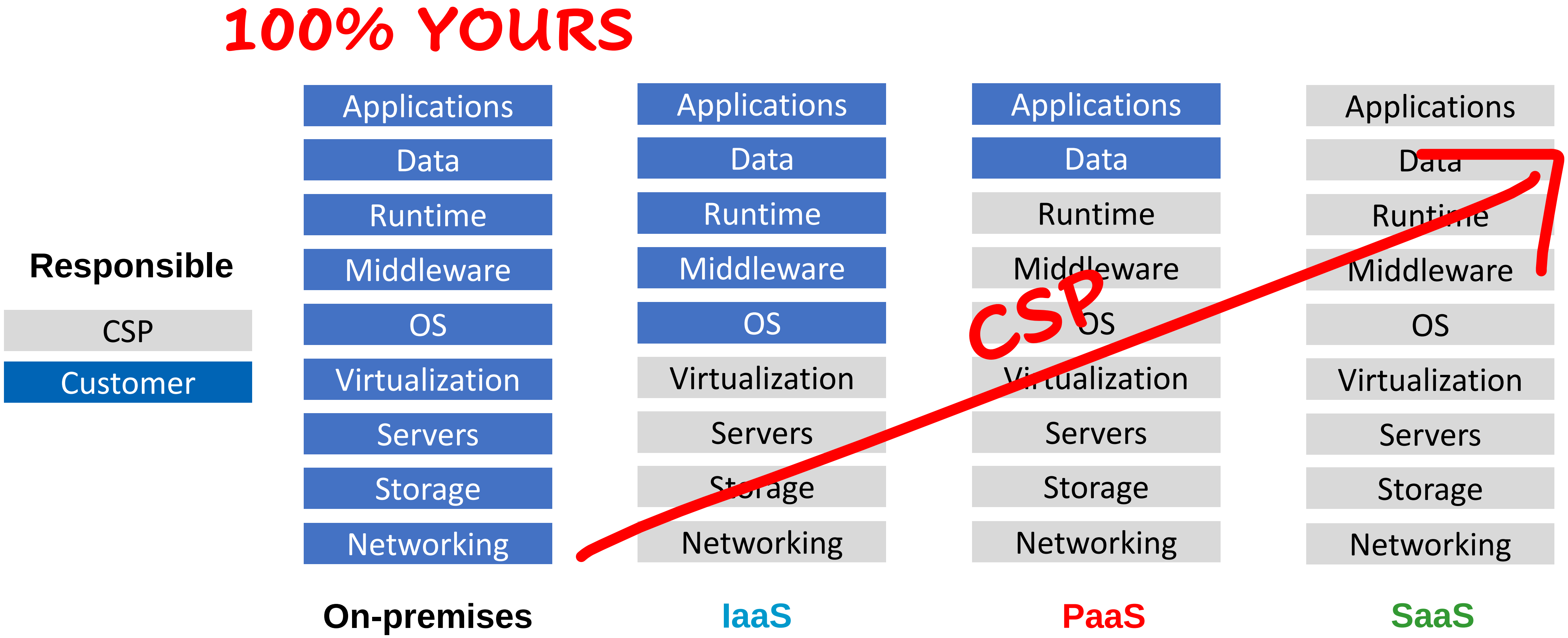
Storing data in the cloud increases the risk, so steps may be necessary to protect the data, depending on its value.

When leasing cloud-based services, you should know who is responsible for maintenance and security.

"shared responsibility model"

The **cloud service provider (CSP)** provides the least amount of maintenance and security in the IaaS model.

SHARED RESPONSIBILITY MODEL



100% YOURS

CSP

Responsible

⬜ CSP

🟦 Customer

On-premises	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	⬜ Applications
🟦 Data	🟦 Data	🟦 Data	⬜ Data
🟦 Runtime	🟦 Runtime	⬜ Runtime	⬜ Runtime
🟦 Middleware	🟦 Middleware	⬜ Middleware	⬜ Middleware
🟦 OS	🟦 OS	⬜ OS	⬜ OS
🟦 Virtualization	⬜ Virtualization	⬜ Virtualization	⬜ Virtualization
🟦 Servers	⬜ Servers	⬜ Servers	⬜ Servers
🟦 Storage	⬜ Storage	⬜ Storage	⬜ Storage
🟦 Networking	⬜ Networking	⬜ Networking	⬜ Networking

Configuration & Change Management

Can prevent 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

helps reduce outages or weakened security from unauthorized changes.

Versioning uses a labeling or numbering system to track changes in updated versions of software.

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

PATCH MANAGEMENT

Patch Management

aka "update management"

ensures that systems are kept up-to-date with current security patches.

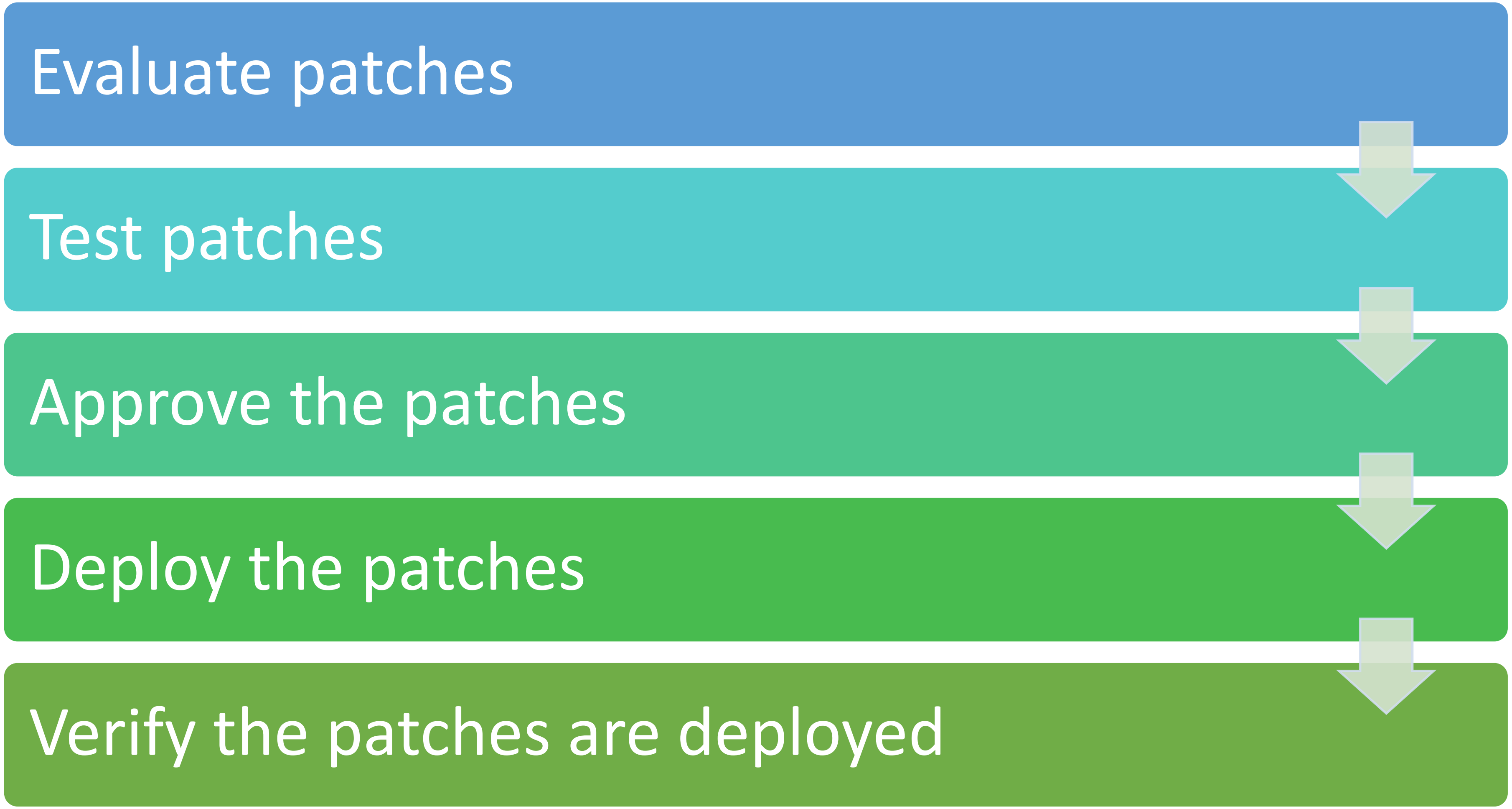
will evaluate, test, approve, and deploy patches.

system audits verify the deployment of approved patches to system.

intertwined with **change and configuration management** to ensure that documentation reflects changes.

Orgs without patch management will experience outages from known issues that could have been prevented

PATCH MANAGEMENT PROGRAM



Evaluate patches

Test patches

Approve the patches

Deploy the patches

Verify the patches are deployed

Vulnerability scans can identify missing patches

VULNERABILITY MANAGEMENT

Vulnerability Management

includes routine vulnerability scans and periodic vulnerability assessments.

Vulnerability Scanners

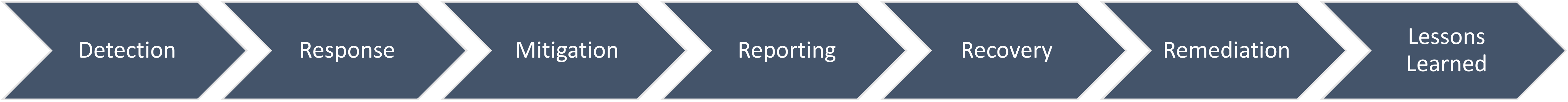
can detect known security vulnerabilities and weaknesses, absence of patches or weak passwords.

Vulnerability Assessments

extend beyond just technical scans and can include reviews and audits to detect vulnerabilities.

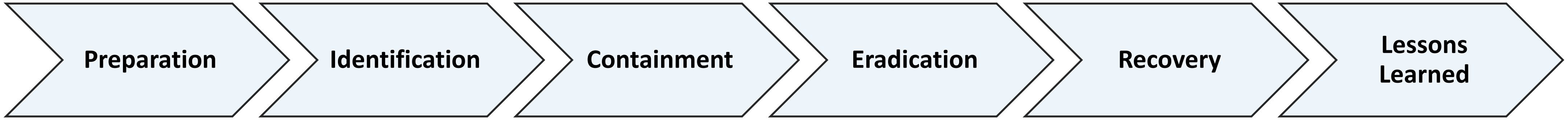
DOMAIN 7: INCIDENT RESPONSE STEPS

Official Study Guide ← on the exam



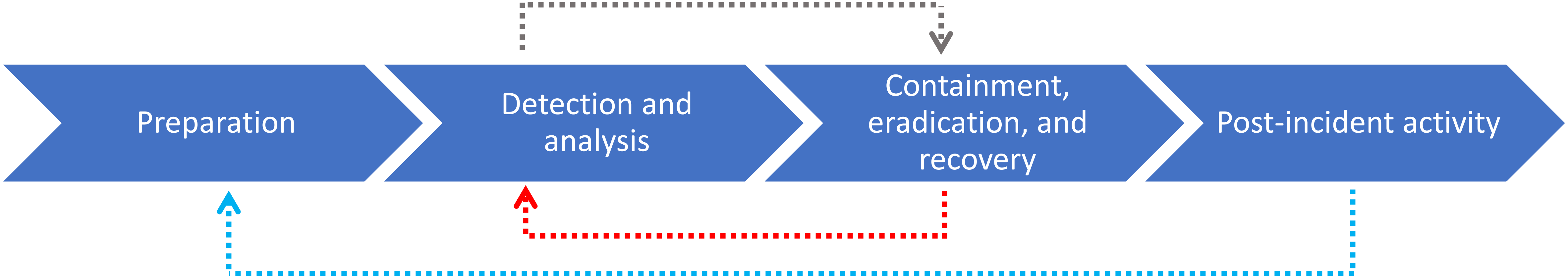
Detection → Response → Mitigation → Reporting → Recovery → Remediation → Lessons Learned

SANS



Preparation → **Identification** → **Containment** → **Eradication** → **Recovery** → **Lessons Learned**

NIST 800-61v2



Preparation → Detection and analysis → Containment, eradication, and recovery → Post-incident activity

DOMAIN 7: INCIDENT RESPONSE STEPS

The CISSP lists incident response steps as

- detection
- response ← limit or contain the scope
- mitigation
- reporting
- recovery
- remediation
- lessons learned

include root cause analysis

DOMAIN 7: DENIAL-OF-SERVICE ATTACKS

prevent a system from responding to legitimate requests for service.

Common DoS attacks

newer attacks are often variations on older methods.

SYN flood attack

which disrupts the TCP three-way handshake.

Smurf attack

employs an amplification network to send numerous response packets to a victim.

Ping-of-death attack

send numerous oversized ping packets to the victim, causing the victim to freeze, crash, or reboot.

DOMAIN 7: BOTNETS, CONTROLLERS, AND BOT HERDERS

represent significant threats due to the massive number of computers that can launch attacks

Botnet

a collection of compromised computing devices (often called bots or zombies).

Bot Herder

criminal who uses a command-and-control server to remotely control the zombies

often use the botnet to launch attacks on other systems, or to send spam or phishing emails

HONEYPOT, PADDED CELL, PSEUDO FLAWS

Honeypot

a system that often has **pseudo flaws** and fake data to lure intruders. lures and distracts attackers

as long as attackers are in the honeypot, they are not in the live network. ...and admins can observe

Some IDSs have the ability to transfer attackers into a **padded cell** after detection

BLOCKING MALICIOUS CODE

multiple approaches, generally used together

Anti-malware software

with up-to-date definitions installed on each system, at the boundary of the network, and on email servers.

Policies

enforce basic security principles, like principle of least privilege, prevent regular users from installing potentially malicious software.

Education

educating users about the risks and the methods attackers commonly use to spread viruses helps users understand and avoid dangerous behaviors.

PENETRATION TESTS

start by discovering vulnerabilities and then mimicking an attack to identify what vulnerabilities can be exploited.

should not be done without express consent and knowledge from management.

can result in damage, so should be done on isolated systems whenever possible.

- black-box testing (zero knowledge)
- white-box testing (full knowledge)
- gray-box testing (partial knowledge)

three varieties

IDS VS IPS RESPONSE

IDS

reactive

can respond passively by logging and sending notifications or actively by changing the environment

IPS

proactive

is placed in line with the traffic and includes the ability to block malicious traffic before it reaches the target

FLAVORS OF INTRUSION DETECTION SYSTEMS

HID

host-based IDS

can monitor activity on a single system only. A drawback is that attackers can discover and disable them.

NID

network-based IDS

can monitor activity on a network, and a NIDS isn't as visible to attackers.

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

ZERO-DAY EXPLOITS

an attack that uses a vulnerability that is either unknown to anyone but the attacker or known only to a limited group of people.

basic security practices can often prevent!

LOG FILES

data is recorded in databases and different types of log files.

common log files include security logs, system logs, application logs, firewall logs, proxy logs.

should be protected by centrally storing them and using permissions to restrict access.

archived logs should be set to read-only to prevent modifications.

MONITORING

a **form of auditing** that focuses on active review of the log file data.

used to hold subjects accountable for their actions

also used to monitor system performance.

tools such as IDSs or SIEMs automate monitoring and provide real-time analysis of events.

THE VALUE OF AUDIT TRAILS

Audit Trails

records created by recording information about events and occurrences into one or more databases or log files.

used to reconstruct an event, to extract information about an incident,

used to prove or disprove culpability,

a passive form of detective security control

Audit trails are essential evidence in the prosecution of criminals.

SAMPLING

Sampling

the process of extracting elements from a large body of data to construct a meaningful representation or summary of the whole.

Statistical sampling

uses precise mathematical functions to extract meaningful information from a large volume of data.

Clipping

is a form of nonstatistical sampling that records only events that exceed a threshold.

MAINTAINING ACCOUNTABILITY

Accountability

is maintained for individual subjects using auditing.

logs record user activities and users can be held accountable for their logged actions.

directly promotes good user behavior and compliance with the organization’s security policy.

SECURITY AUDITS AND REVIEWS

Security audits and reviews

help ensure that management programs are effective and being followed.

commonly associated with account management practices to prevent violations with least privilege or need-to-know principles.

can also be performed to oversee many programs and processes

- patch management
- vulnerability management
- change management
- configuration management

FREQUENCY OF IT SECURITY AUDITS

What is Auditing?

a methodical examination of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes.

serves as a primary type of detective control

frequency is based on risk.

degree of risk also affects how often an audit is performed.

Secure IT environments rely heavily on auditing and many regulations require it.

AUDITING & DUE CARE

Security audits and effectiveness reviews are key elements in displaying due care. without them, senior management will likely be held accountable and liable for any asset losses that occur.

act with common sense, prudent management, responsible action

CONTROLLING ACCESS TO AUDIT REPORTS

Audit reports often contain **sensitive information**

often include purpose and scope of the audit, and results discovered or revealed

can include sensitive information such as problems, standards, causes, and recommendations.

Only people with sufficient privilege should have access

FOR EXAMPLE:
senior security administrators = full detail
senior management = high-level summary

USER ENTITLEMENTS & ACCESS REVIEWS

Access Review

ensures that object access and account management practices support the security policy.

User Entitlement Audit

ensure that the principle of least privilege is followed and often focus on privileged accounts.

AUDIT ACCESS CONTROLS

effectiveness of access controls should be reviewed / audited regularly

can track logon success and failure of any account

can include resource (object) access and action performed on resources

intrusion detection systems can monitor these logs and easily identify attacks and notify administrators

often automated, auto-reporting, and supported by AI

COMPUTER CRIME

a crime (or violation of a law or regulation) that is directed against, or directly involves, a computer.

CATEGORIES OF COMPUTER CRIME

Computer crimes are classified as one of the following 6 types:

- Military and intelligence attacks
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Thrill attacks

six degrees of Kevin Bacon

six categories of computer crime

ELECTRONIC DISCOVERY

Organizations expecting lawsuit have a duty to preserve digital evidence in a process called **eDiscovery**.

eDiscovery process includes:

- information identification and governance
- preservation and collection
- processing, review, analysis
- production, and presentation

often uses tagging, classification, target specific custodian

DOMAIN 7: GATHERING INFO IN INVESTIGATIONS

to gather sufficient information from the equipment, software, and data from equipment requires

Possession

You must have possession of equipment, software, or data to analyze it and use it as evidence.

Modification

You must acquire the evidence without modifying it or allowing anyone else to modify it.

Law enforcement establishes chain of evidence (aka chain of custody) to document all who handle it.

ALTERNATIVES TO CONFISCATING EVIDENCE

Voluntary surrender

the person who owns the evidence could voluntarily surrender it for investigation.

Subpoena

could be used to compel the subject to surrender the evidence

Search Warrant

most useful when you need to confiscate evidence without giving the subject an opportunity to alter it.

DOMAIN 7: RETAINING INVESTIGATORY DATA

Because you will discover some incidents after they have occurred....

You will lose valuable evidence unless you ensure that critical log files are retained for a reasonable period of time.

You can retain log files and system status information either in-place or in archives

data retention should be defined in security policies

EVIDENCE

Best. Original.

Secondary evidence. Copy.

Direct. Proves or disproves an act based on the five senses.

Conclusive. Incontrovertible, overrides all other types.

Circumstantial. Inference from other info.

Corroborative. Supporting evidence but cannot stand on its own.

Opinions. Expert and non-expert.

Hearsay. Not based on first-hand knowledge.

Evidence must be **relevant**, **complete**, **sufficient** and **reliable**

DOMAIN 7: EVIDENCE ADMISSIBILITY

Types of evidence that may be used **in a criminal or civil trial**:

Real evidence

consists of actual objects that can be brought into the courtroom.

Documentary evidence

consists of written documents that provide insight into the facts.

Testimonial evidence

consists of verbal or written statements made by witnesses.

DOMAIN 7: EVIDENCE ADMISSIBILITY

Requirements for evidence to be **admissible in a court of law**:

TO BE ADMISSIBLE:

Evidence must be relevant to a fact at issue in the case

The fact must be material to the case,

The evidence must be competent or legally collected.

Evidence is considered "competent" if it complies with certain traditional notions of reliability.

DOMAIN 7: COLLECTING EVIDENCE

Importance of collecting

EVIDENCE

As soon you discover an incident...

You must begin to collect evidence and as much information about the incident as possible.

Evidence can be used in a subsequent legal action or in finding attacker identity.

Evidence can also assist you in determining the extent of damage.

NATURAL DISASTERS

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

- Earthquakes
- Floods
- Storms
- Tsunamis
- Volcanic eruptions

MAN-MADE DISASTERS

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

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

RECOVERY SITE TYPES

Three primary types of recovery sites:

HOT **WARM** **COLD**

RECOVERY SITE TYPES

COLD

cost = LOW
effort = HIGH

DESCRIPTION

A “recovery” cold site is essentially just data center space, power, and network connectivity that’s ready and waiting for whenever you might need it.

TO RECOVER

If disaster strikes, your engineering and logistical support teams can readily help you move your hardware into the data center and get you back up and running.

RECOVERY SITE TYPES

WARM

cost = MEDIUM
effort = MEDIUM

DESCRIPTION

A “preventative” warm site allows you to pre-install your hardware and pre-configure your bandwidth needs.

TO RECOVER

If disaster strikes, all you have to do is load your software and data to restore your business systems.

RECOVERY SITE TYPES

HOT

cost = HIGH
effort = LOW

DESCRIPTION

A “proactive” hot site allows you to keep servers and a live backup site up and running in the event of a disaster. You replicate your production environment in that data center.

TO RECOVER

This allows for an immediate cutover in case of disaster at your primary site. A hot site is a must for mission critical sites.

RECOVERY SITE TYPES (CONT)

Service Bureau

a company that leases computer time. Service bureaus own large server farms and often fields of workstations. may be onsite or remote

Mobile Site

nonmainstream alternatives to traditional recovery sites. They typically consist of self-contained trailers or other easily relocated units.

Multiple Sites

Just what it sounds like. May mix-and-match some combination of the aforementioned options

RPO AND RTO

Recovery Point Objective (RPO) | is the age of files 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.

MUTUAL ASSISTANCE AGREEMENTS (MAAs)

PROs and CONs of MAAs

Benefits of an MAA

Mutual assistance agreements (MAAs) provide an inexpensive alternative to disaster recovery sites.

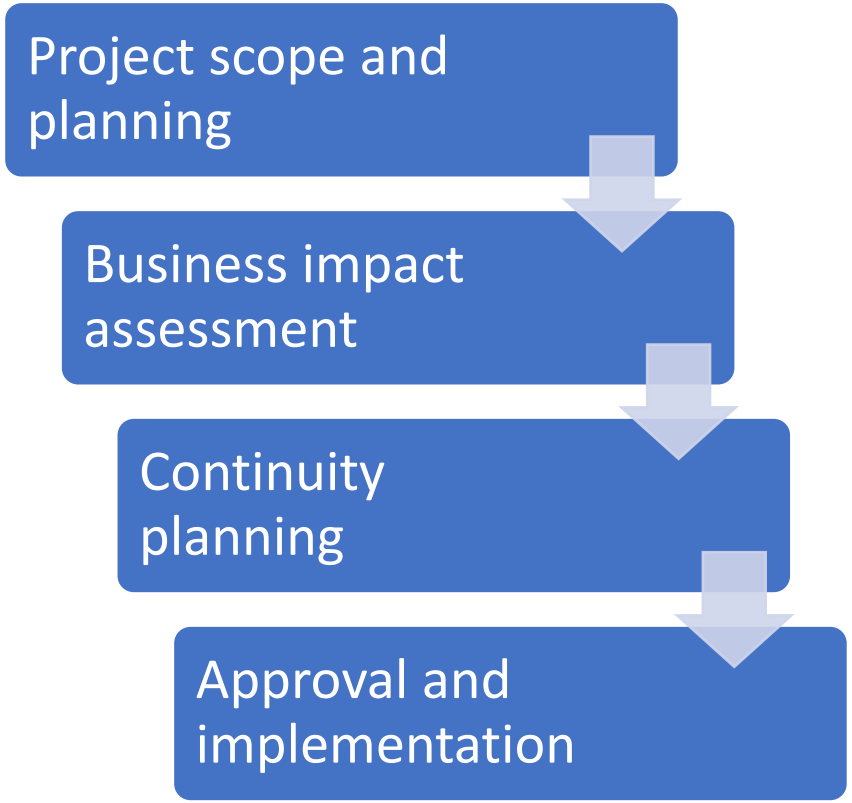
Risk of an MAA

Organizations participating in an MAA may also be shut down by the same disaster, and MAAs raise confidentiality concerns.

Why are MAAs uncommon?

They are not commonly used because they are difficult to enforce.

BUSINESS CONTINUITY PLANNING (BCP)



Project scope and planning

Business impact assessment

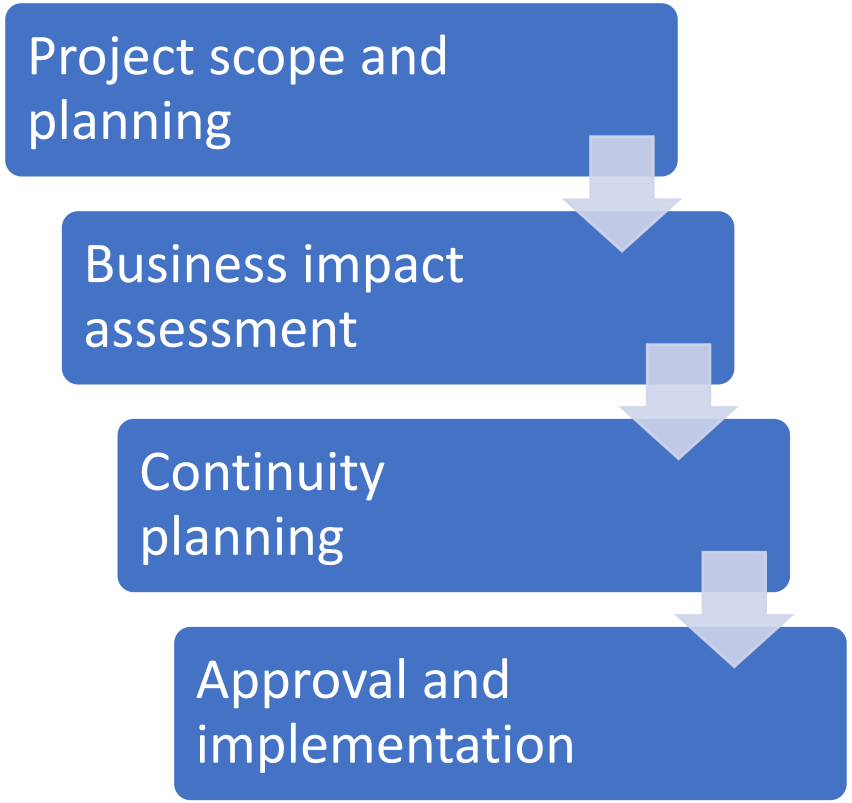
Continuity planning

Approval and implementation

The 4 main steps of Business Continuity Planning

assessment of business impact happens within BCP

BUSINESS CONTINUITY PLANNING (BCP)



Project scope and planning

Business impact assessment

Continuity planning

Approval and implementation

The 4 main steps of Business Continuity Planning

GOAL:
efficient response to enhance a company's ability to recover from a disruptive event promptly

BCP DEFINITIONS

Some BCP-related definitions worth knowing

BCP (Business Continuity Plan)

the overall organizational plan for “how-to” continue business.

COOP (Continuity of Operations Plan)

the plan for continuing to do business until the IT infrastructure can be restored.

DRP (Disaster Recovery Plan)

the plan for recovering from an IT disaster and having the IT infrastructure back in operation.

BCP DEFINITIONS

Some BCP-related definitions worth knowing

BRP (Business Resumption Plan)
the plan to move from the disaster recovery site back to your business environment or back to normal operations.

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.

BCP DEFINITIONS

Some BCP-related definitions worth knowing

MTD (Max tolerable downtime)
The amount of time we can be without the asset that is unavailable BEFORE we must declare a disaster and initiate our disaster recovery plan.

GOALS OF DR AND BCP

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

5 TYPES OF DISASTER RECOVERY PLAN TESTS

Know the 5 types of disaster recovery plan tests:

- Read-through
- Structured walk-through
- Simulation test
- Parallel test
- Full interruption test

5 TYPES OF DISASTER RECOVERY PLAN TESTS

Read-through test

You distribute copies of disaster recovery plans to the members of the disaster recovery team for review.

Structured walk-through aka table-top exercise

Members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.

Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting.

The team members refer to the document and discuss the appropriate responses to that particular type of disaster.

so far, these are all talk

5 TYPES OF DISASTER RECOVERY PLAN TESTS

Simulation test

Similar to structured walk-through, except some of the response measures are then tested (on non-critical functions).

Parallel test

involves relocating personnel to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform their disaster recovery responsibilities just as they would for an actual disaster.

Full interruption test

like parallel tests but involves actually shutting down operations at the primary site and shifting them to the recovery site.

all involve some form of 'doing'

5 TYPES OF DISASTER RECOVERY PLAN TESTS

A couple of related terms

Recovery Team recover
is used to get critical business functions running at the alternate site.

Salvage Team restore
is used to return the primary site to normal processing conditions.

BACKUP STRATEGIES

Electronic Vaulting

is used to transfer database backups to a remote site as part of a bulk transfer.

Remote Journaling

Transmitting only the journal or transaction logs to the off-site facility and not the actual files.

Remote Mirroring

a live database server is maintained at the backup site.

the most advanced database backup solution (and also tends to be the most expensive of these)

CATEGORIES OF DISRUPTION (from CISSP CBK)

There are 3 main categories of disruption:

Non-Disaster
disruption in service from device malfunction or user error.

Disaster
entire facility unusable for a day or longer.

Catastrophe
major disruption that destroys the facility altogether.
Requires a short term and long term solution.

MODERN FIREWALLS

Firewalls
Web Application

protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

typically protects web applications from attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewalls
Next Generation

a "deep-packet inspection firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

INTELLIGENCE IN THREAT MODELING

UEBA

User and Entity Behavioral Analytics

entity behavior is collected and input into a threat model.

model establishes a baseline of "normal" based on historical data

can conduct an analysis to uncover more details around anomalous events

'automated investigation' also exists in some platforms

INTELLIGENCE IN THREAT MODELING

Threat Intelligence

threat feeds

Activities an organization undertakes to educate itself about changes in the threat landscape

often a feed containing malicious entities ingested by cybersecurity tools

A single feed may be comprised of many sources, including open-source intelligence

entity = IP, website, threat actor, file hash, and more

THE ROLE OF AI & ML

Analyzing and improving cybersecurity posture is no longer a human-scale problem. Artificial Intelligence (AI) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.

THE ROLE OF AI & ML

Along with AI, machine learning (ML) has become critical technologies in information security, in quickly analyzing millions of events and identify many different types of threats

THE ROLE OF AI & ML

Histories of behavior build profiles on users, assets, and networks, allowing AI to detect and respond to deviations from established norms.

know that AI and ML factor in anti-malware, SIEM, IPS/IDS, and IDaaS, and more