



## Welcome to the Seventh CBK Domain:

► In this domain we cover:

- Investigations support and requirements, Logging and monitoring activities.
- Provisioning of resources, Foundational security operations concepts, Resource protection techniques.
- Preventative measures, Patch and vulnerability management, Change management processes.
- Incident management, Recovery strategies, Disaster recovery processes and plans, Business continuity planning and exercises.
- Personnel safety concerns.

*This chapter is how we secure our day-to-day operations, how we continue to function in a disaster event and how we recover after an event. The domain also has some areas that just didn't fit in elsewhere.*

*CBK 7 makes up 13% of the exam questions.*

► CBK 7 Key Terms:

- **BCP (Business Continuity Plan):** Long-term plan to ensure the continuity of business operations in a disaster event.
- **DR (Disaster Recovery):** Policies, procedures and tools to recover from a natural, environmental or man made disaster.
- **Collusion:** An agreement between two or more individuals to subvert the security of a system.
- **COOP (Continuity of Operations Plan):** A plan to maintain operations during a disaster.
- **Disaster:** Any disruptive event that interrupts normal system operations.
- **DRP (Disaster Recovery Plan):** Short-term plan to recover from a disruptive event, part of our BCP.
- **MTBF (Mean Time Between Failures):** How long a new or repaired system or component will function on average before failing.
- **MTTR (Mean Time to Repair):** How long it will take to recover a failed system.
- **RAID (Redundant Array of Independent/Inexpensive Disks):** Using multiple disk drives to achieve greater data reliability, speed, and fault tolerance.
- **Mirroring:** Complete duplication of data to another disk, used by some levels of RAID.
- **Striping:** Spreading data writes across multiple disks to achieve performance gains, used by some levels of RAID.

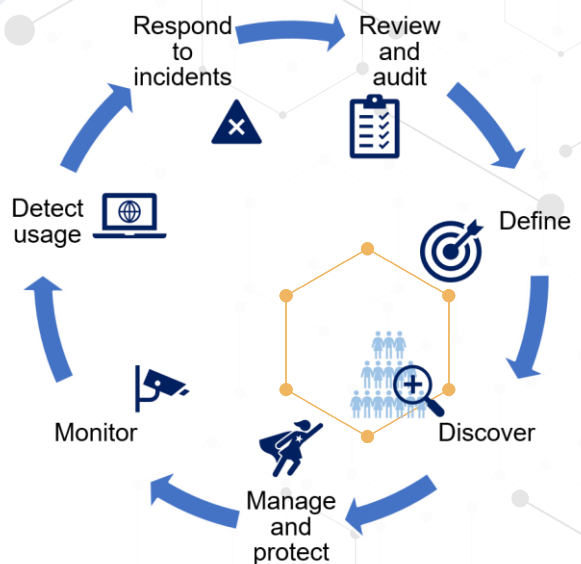


### ▶ Administrative Personnel Security Controls:

- **Administrative Security:**
  - Provides the means to control people's operational access to data.
  - **Least Privilege:**
    - ♦ We give employees the minimum necessary access they need, no more, no less.
  - **Need to Know:**
    - ♦ Even if you have access, if you do not need to know, then you should not access the data.  
(Kaiser employees).
  - **Separation of Duties:**
    - ♦ More than one individual in one single task is an internal control intended to prevent fraud and error.
    - ♦ We do not allow the same person to enter the purchase order and issue the check.
    - ♦ For the exam assume the organization is large enough to use separation of duties, in smaller organizations where that is not practical, compensating controls should be in place.
  - **Job Rotation:**
    - ♦ For the exam think of it to detect errors and frauds. It is easier to detect fraud and there is less chance of collusion between individuals if they rotate jobs.
    - ♦ It also helps with employees burnout and it helps employees understand the entire business.
    - ♦ This can be too cost prohibitive for the exam/real life, make sure on the exam the cost justifies the benefit.
  - **Mandatory Vacations:**
    - ♦ Done to ensure one person is not always performing the same task, someone else has to cover and it can keep fraud from happening or help us detect it.
    - ♦ Their accounts are locked and an audit is performed on the accounts.
    - ♦ If the employee has been conducting fraud and covering it up, the audit will discover it.
    - ♦ The best way to do this is to not give too much advance notice of vacations.
- With the combination of all 5 we minimize some of the insider threats we may have.



- **NDA (Non-Disclosure Agreement):**
  - We covered NDA's between our and other organizations, it is also normal to have them for internal employees.
  - Some employment agreements will include a clause restricting employees' use and dissemination of company-owned confidential information.
- **Background Checks:**
  - References, Degrees, Employment, Criminal, Credit history (less common, more costly).
  - For sensitive positions the background check is an ongoing process.
- **Privilege Monitoring:**
  - The more access and privilege an employee has the more we keep an eye on their activity.
  - They are already screened more in depth and consistently, but they also have access to many business critical systems, we need to audit their use of that access.
  - With more access comes more responsibility and scrutiny.
- **Privileged Account/Access Management (PAM):**
  - Account (account safeguarded) vs. Access (Account + what can the account access/do).
  - We want to identify and monitor anyone with more access than the normal user. The higher privileges they have the closer they should be monitored.
  - We monitor the what/when/how/why/where of what is accessed.
  - Full monitoring, limit privileges, MFA, monitor remote connections, logs/records are immutable, anomaly detection, continuous monitoring, full visibility of all admins, and no group accounts.
  - **Users:**
    - ♦ **Regular users:** Analyze performance, improve efficiency.
    - ♦ **Privileged users:** Access matrix, what was changed?
    - ♦ **All users:** Sensitive data, critical systems, insider/outsider threats, and meeting compliance/regulatory requirements.
  - **Systems:**
    - ♦ All servers (including jump servers), all endpoints, and remote workstations.



**The Privileged Access Management lifecycle**



- **Conduct Logging and Monitoring Activities:**
  - Logging = Managing all the logs from our applications and infrastructure, the raw data.
  - Monitoring = Making sure that our applications and infrastructure is available and responds to user requests within an acceptable time frame, alerts us of issues, the data being used.
- **Threat Intelligence:**
  - **Threat Feeds:** A stream of raw current and potential threats.
    - ♦ We can use a threat intelligence feed to get actual usable data, such as suspicious domains, malware hashes, potential malicious code, flagged IPs.
    - ♦ We can then use that feed to compare to our ingress/egress traffic.
  - **Threat Hunting:** Actively looking for threats on our network.
    - ♦ We assume attackers are able to access our network and have not been detected, we aggressively search our systems for any threat indicator.
- **User and Entity Behavior Analytics (UEBA):**
  - We use machine/deep learning to model typical and atypical user behavior, setting a baseline.
  - With the baseline, we can identify anomalies and threats sooner.
  - For that we look at:
    - ♦ Use cases – How do normal users use our network and data?
    - ♦ Data sources – Data sources, normally a data lake/warehouse or SIEM, should not be deployed directly.
    - ♦ Analytics – To build the baseline and detect anomalies.

### ▶ Administrative Security:

- **Digital (Computer) Forensics:**
  - Focuses on the recovery and investigation of material found in digital devices, often in relation to computer crime.
  - Closely related to incident response, forensics is based on gathering and protecting the evidence, where incidents responses are how we react in an event breach.
  - We preserve the crime scene and the evidence, we can prove the integrity of it at a later needed time, often court.



A portable write-blocker attached to a hard disk.





### ▪ The Forensic Process:

- ♦ Identify the potential evidence, acquire the evidence, analyze the evidence, make a report.
- ♦ We need to be more aware of how we gather our forensic evidence, attackers are covering their tracks, deleting the evidence and logs.
- ♦ This can be through malware that is only in volatile memory, if power is shut off (to preserve the crime scene), the malware is gone and the evidence is lost.
- ♦ Rather than shutting the system down, we can if considered safe disconnect it from the network and take bit by bit copies of the memory, drives, running processes and network connection data.



Cell phone in an evidence bag.

- The evidence we collect must be accurate, complete, authentic, convincing, admissible.

- **Identification:** Identify the evidence, what is left behind

### ▪ Preservation:

- ♦ Everything is documented, chain of custody: Who had it when? What was done? When did they do it?
- ♦ Pull the original, put it in write protected machine, we make a hash.
- ♦ We only do examinations and analysis on bit level copies, we confirm they have the same hash as the original before and after examination

### ▪ Collection:

- ♦ We examine and analyze the data, again document everything.
- ♦ We handle the evidence as little as possible.
- ♦ Work from most volatile to least volatile, starting with the RAM and ending with the hard disks.

- We use our incident response plan:

- This can include getting our HR and Legal departments involved.

- We ensure our evidence is acquired in a legal manner. Remember the US Constitution 4th amendment.

- ♦ *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.*

- Anything subpoenaed, search warranted, turned over voluntarily and in exigent circumstances (immediate danger of being destroyed), can allow law enforcement to bypass the 4th amendment.

- **Examination:** Find the facts and document them, collecting the data.

- **Analysis:** Look at the data and look for meaning or reason.



- **Presentation in Court:** We present our findings and any other evidence.
- **Decision:** The court rules on the case.
- Forensic data is normally obtained from binary images of secondary storage and portable storage devices like hard drives, flash drives, CDs, DVDs, and cell phones, ...
- We use a binary or bit stream image copy to ensure we get an exact copy of the device, and not just a copy of certain sectors.
- **Real Evidence:** Tangible and Physical objects, in IT Security: Hard Disks, USB Drives – NOT the data on them.
- **Evidence Integrity** – It is vital the evidence's integrity cannot be questioned, we do this with hashes. Any forensics is done on copies and never the originals, we check hash on both original and copy before and after the forensics.
- **Chain of Custody** – Chain of custody form, this is done to prove the integrity of the data. No tampering was done.
  - ♦ Who handled it?
  - ♦ When did they handle it?
  - ♦ What did they do with it?
  - ♦ Where did they handle it?



- **Artifacts (e.g., computer, network, mobile device):**

- Can be digital traces left behind by attackers (logs and data generated by those devices) but it can also be physical devices (computers, mobile devices, network devices) and other forms of evidence.
- We need to preserve the artifacts both to ensure they are useful in our forensics and even more importantly, if we ever go to court.

- **Continuous monitoring:**

- Exactly what it sounds like.
- All events are recorded for later potential analysis.
- Helps us detect compliance and risk issues.

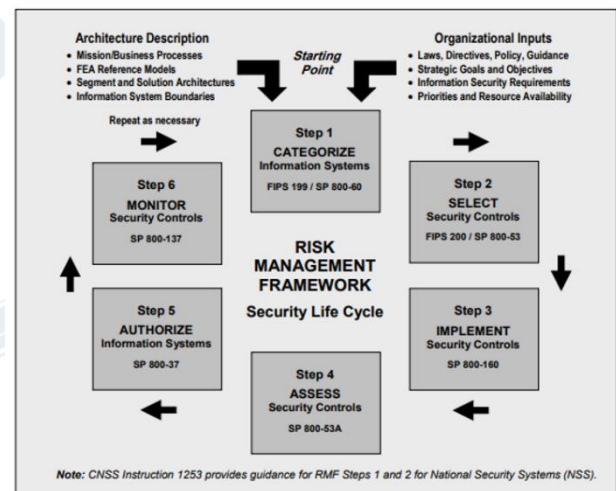


FIGURE 2: RISK MANAGEMENT FRAMEWORK

From NIST 800-53



- **Digital Forensics:**

- Here are the four basic types of disk-based forensic data:

- ♦ **Allocated Space:**

- The portions of the disk that are marked as actively containing data.

- ♦ **Unallocated Space:**

- The portions of the disk that does not contain active data.
- This is parts that have never been allocated and previously allocated parts that have been marked unallocated.
- When a file is deleted, the parts of the disk that held the deleted file are marked as unallocated and made available for use. (This is also why deleting a file does nothing, the data is still there until overwritten).

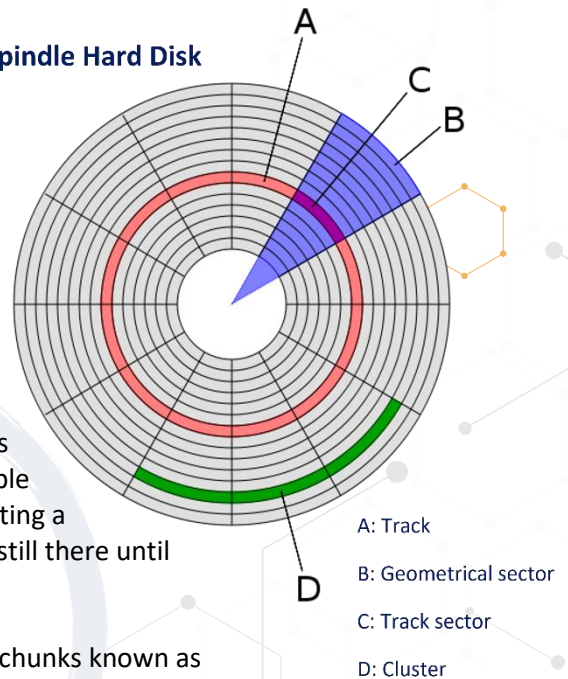
- ♦ **Slack Space:**

- Data is stored in specific size chunks known as clusters (clusters = sectors or blocks).
- A cluster is the minimum size that can be allocated by a file system.
- If a particular file, or final portion of a file, does not require the use of the entire cluster then some extra space will exist within the cluster.
- This leftover space is known as slack space: it may contain old data, or can be used intentionally by attackers to hide information.

- ♦ **Bad Blocks/Clusters/Sectors:**

- Hard disks end up with sectors that cannot be read due to some physical defect.
- The sectors marked as bad will be ignored by the operating system since no data could be read in those defective portions.
- Attackers can mark sectors or clusters as being bad in order to hide data within this portion of the disk.

**Spindle Hard Disk**





### ▪ Network Forensics:

- ♦ A sub-branch of digital forensics where we look at the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.
- ♦ Network investigations deal with volatile and dynamic information.
- ♦ Network traffic is transmitted and then lost, so network forensics is often a proactive investigation.
- ♦ **Network Forensics generally has two uses.**
  - **The first type** is monitoring a network for anomalous traffic and identifying intrusions (IDS/IPS).
    - An attacker might be able to erase all log files on a compromised host, a network-based evidence might be the only evidence available for forensic analysis.
  - **The second type** relates to law enforcement.
    - In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.
- ♦ Systems used to collect network data for forensics use usually come in two forms:
  - **Catch-it-as-you-can:**
    - All packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode.
    - This approach requires large amounts of storage.
  - **Stop, look and listen:**
    - Each packet is analyzed in a basic way in memory and only certain information is saved for future analysis.
    - This approach requires a faster processor to keep up with incoming traffic.

### ▪ Embedded Device Forensics:



- ♦ We have for decades analyzed and investigated standard systems, traffic and hardware, but embedded devices is a new player.
  - ♦ They include SSD's, GPS's, cell phones, PDA and much more.
  - ♦ They can contain a lot of information, but how do we safely retrieve it while keeping the integrity of the data?
  - ♦ We talked about how the IoT (Internet Of Things) can be a security concern, but all the devices can also hold a wealth of information.
    - Where does the GPS say the car, phone or person was at a certain time?
    - When did the AC turn on? Can we assume someone was home at that time?
- Forensic examiners may have to be able to access, interpret and analyze embedded devices in their investigation.





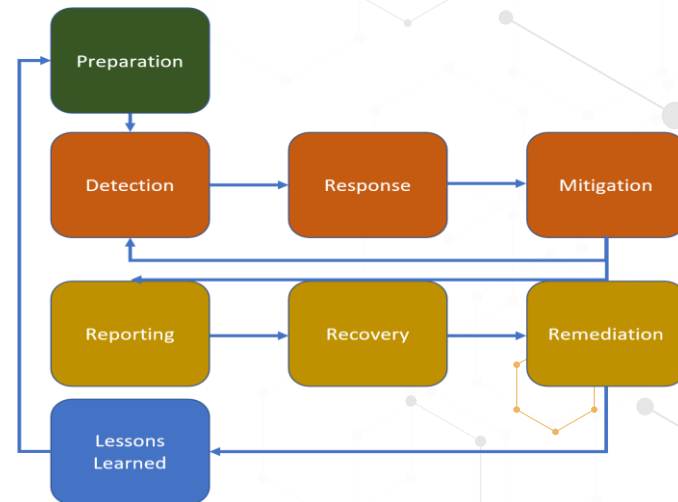
- **Forensic Software Analysis:**
  - ♦ Comparing and/or reverse engineering software.
  - ♦ Reverse engineering malware is one of the most common examples.
  - ♦ Investigators often have a binary copy of a malware program and try to deduce what it does.
  - ♦ Common tools are disassemblers and debuggers.
- Software forensics can also refer to intellectual property infringement. For the exam this is not the type we talk about.
- **Egress Monitoring:**
  - ♦ Done to prevent data exfiltration both logically and physically.
  - ♦ For logical egress monitoring, we can use DLP systems.
    - This can be both network-based and endpoint DLP systems.
    - Even if the data is encrypted and we can't decrypt it, we can still prevent the egress from our network.
  - ♦ For physical egress monitoring, we could use guards, make sure the trash and any other way things can be physically removed from our organization are monitored and secured.
- **Electronic Discovery (E-discovery):**
  - ♦ The discovery in legal proceedings, litigation, government investigations, or Freedom of Information Act requests, where the information is in electronic format.
  - ♦ Considered different from paper information because of its intangible form, volume, transience and persistence.
  - ♦ Usually accompanied by metadata that is not found in paper documents and that can play an important part as evidence.
  - ♦ The preservation of metadata from electronic documents creates special challenges to prevent spoliation.
  - ♦ Can be very costly and take a lot of time with the amounts of data we store. Proper retention for backups can reduce this as well as what we back up.
  - ♦ The Electronic Discovery Reference Model (EDRM):
    - Information governance, identification, preservation, collection, processing, review, analysis, production, and presentation.
- **Incident Management:**
  - Involves the monitoring and detection of security events on our systems, and how we react in those events.
  - It is an administrative function of managing and protecting computer assets, networks and information systems.
  - The primary purpose is to have a well understood and predictable response to events and computer intrusions.



- We have very clear processes and responses, and our teams are trained in them and know what to do when an event occurs.
- Incidents are very stressful situations, it is important staff knows exactly what to do, that they have received ongoing training and understand the procedures.
- **Incidences and events can generally be categorized in 3 classes:** 
  - ♦ **Natural:** Hurricanes, floods, earthquakes, blizzards, anything that is caused by nature.
  - ♦ **Human:** Done intentionally or unintentionally by humans, these are by far the most common.
  - ♦ **Environmental:** This is not nature, but the environments we work in, the power grid, the internet connections, hardware failures, software flaws,...
- **Event:** 
  - ♦ An observable change in state, this is neither negative nor positive, it is just something has changed.
  - ♦ A system powered on, traffic from one segment to another, an application started.
- **Alert:**
  - ♦ Triggers warnings if certain event happens.
  - ♦ This can be traffic utilization above 75% or memory usage at 90% or more for more than 2 minutes.
- **Incident:**
  - ♦ Multiple adverse events happening on our systems or network, often caused by people.
- **Problem:**
  - ♦ Incidence with an unknown cause, we would follow similar steps to incidence response.
  - ♦ More time would be spent on root cause analysis, we need to know what happened so we can prevent it from happening again, this could be a total internet outage or server crash.
- **Inconvenience (Non-disasters):**
  - ♦ Non-disruptive failures, hard disk failure, 1 server in a cluster is down,...
- **Emergency (Crisis):**
  - ♦ Urgent, event with the potential for loss of life or property.
- **Disaster:**
  - ♦ Our entire facility is unusable for 24 hours or longer.
  - ♦ If we are geographically diverse and redundant we can mitigate this a lot.
  - ♦ Yes, a snowstorm can be a disaster.
- **Catastrophe:**
  - ♦ Our facility is destroyed.



- We most common use a 8-step lifecycle.
- 1. **Preparation.**
- 2. **Detection** (Identification).
- 3. **Response** (Containment).
- 4. **Mitigation** (Eradication).
- 5. **Reporting.**
- 6. **Recovery.**
- 7. **Remediation.**
- 8. **Lessons Learned** (Post-incident Activity, Post Mortem, or Reporting).




- **Preparation:**
  - ♦ This is all the steps we take to prepare for incidences.
  - ♦ We write the policies, procedures, we train our staff, we procure the detection soft/hardware, we give our incidence response team the tools they need to respond to an incident.
  - ♦ The more we train our team, the better they will handle the response, the faster we recover, the better we preserve the crime scene (if there is one), the less impactful an incident will be.
- **Detection:**
  - ♦ Events are analyzed to determine if they might be a security incident.
  - ♦ If we do not have strong detective capabilities in and around our systems, we will most likely not realize we have a problem until long after it has happened.
  - ♦ The earlier we detect the events, the earlier we can respond, IDS's can help us detect, where IPS's can help us detect and prevent further compromise.
  - ♦ The IDS's and IPS's can help us detect and prevent on a single network segment, we also need something that can correlate all the information from the entire network.
- **Response:**
  - ♦ The response phase is when the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.
  - ♦ This can be taking a system off the network, isolating traffic, powering off the system, or however our plan dictates to isolate the system to minimize both the scope and severity of the incident.
  - ♦ Knowing how to respond, when to follow the policies and procedures to the letter and when not to, is why we have senior staff handle the responses.
  - ♦ We make bit level copies of the systems, as close as possible to the time of incidence to ensure they are a true representation of the incident.



- ♦ IT Security is there to help the business, it may not be the choice of senior management to disrupt business to contain or analyze, it is ultimately a decision that is made by them.
- ♦ We stop it from spreading, but that is it, we contain the event.
- **Mitigation:**
  - ♦ We understand the cause of the incident so that the system can be reliably cleaned and restored to operational status later in the recovery phase.
  - ♦ Organizations often remove the most obvious sign of intrusion on a system or systems, but miss backdoors and other malware installed in the attack.
  - ♦ The obvious sign is often left to be found, where the actual payload is hidden. If that is detected or assumed, we often just rebuild the system from scratch and restore application files from a known good backup, but not system files.
  - ♦ To ensure the backup is good, we need to do root cause analysis, we need a timeline for the intrusion, when did it start?
  - ♦ If it is from a known vulnerability we patch. If it's a newly discovered vulnerability we mitigate it before exposing the newly built system to the outside again.
  - ♦ If anything else can be learned about the attack, we can add that to our posture.
  - ♦ Once eradication is complete, we start the recovery phase.
- **Reporting:**
  - ♦ We report throughout the process beginning with the detection, and we start reporting immediately when we detect malicious activity.
  - ♦ The reporting has 2 focus areas: technical and non-technical.
  - ♦ The incident handling teams report the technical details of the incident as they start the incident handling process, but they also notify management of serious incidents.
  - ♦ The procedures and policies will outline when which level of management needs to be informed and involved, it is commonly forgotten until later and can be a RPE (Resume Producing Event).
  - ♦ Management will also involve other departments if needed, this could be legal, PR or whomever has been identified in the policies or procedures.
- **Recovery:**
  - ♦ We carefully restore the system or systems to operational status.
  - ♦ When the system is ready for reinsertion is determined by the business unit responsible for the system.
  - ♦ We closely monitor the rebuilt or cleaned system carefully, it is possible the attackers left backdoors or we did not remove all the infected sectors.





- ♦ Often the system(s) are reinserted off peak hours to minimize the effect of the system(s) still being infected, or they can be introduced in a controlled sandbox environment to see if the infection persists.
- **Remediation:**
  - ♦ The remediation happens during the mitigation phase, where vulnerabilities on the impacted system or systems are mitigated.
  - ♦ Remediation continues after mitigation and becomes broader, this can be patching all systems with the same vulnerability or change how the organization authenticates.
- **Lessons Learned:** 
  - ♦ This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
  - ♦ We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.
  - ♦ How can we as an organization grow and become better next time we have another incidence? While we may have fixed this one vulnerability there are potentially 100's of new ones we know nothing about yet.
  - ♦ At the end of lessons learned we produce a report to senior management, with our findings, we can only make suggestions, they are ultimately in charge (and liable).
  - ♦ Often after major incidents organizations shift to a top-down approach and will listen more to IT Security.
  - ♦ The outcome and changes of the Lessons Learned will then feed into our preparation.
- **Root-Cause Analysis:**
  - ♦ We attempt to determine the underlying weakness or vulnerability that allowed the incident to happen.
  - ♦ If we do not do the root-cause analysis we will most likely face the same problem again.
  - ♦ We need to fix the vulnerability on the system(s) that were effected, but also on any system in the organization that has that particular vulnerability or set of vulnerabilities.
  - ♦ We could have a weak password policy and weak encryption, that could be the root cause of a system compromise, we then would implement countermeasures to remove the vulnerability.
  - ♦ If we do nothing and just fix the problem, the root of the issue still persists, that is what we need to fix.



### ▶ Preventive and Detective Controls:

- **IDS's and IPS's:**

- We use both IDS's (Intrusion Detection Systems) and IPS's (Intrusion Prevention Systems) on our network to capture and alert or block traffic seen as malicious.
- They can be categorized into 2 types and with 2 different approaches toward identifying malicious traffic.



- ♦ **Network-Based**, placed on a network segment (a switch port in promiscuous mode).
  - ♦ **Host-Based**, on a client, normally a server or workstation.
  - ♦ **Signature (Pattern) Matching**, similar to anti virus, it matches traffic against a long list of known malicious traffic patterns.
  - ♦ **Heuristic-Based (Behavioral)**, uses a normal traffic pattern baseline to monitor for abnormal traffic.
- Just like firewalls, routers, servers, switches and everything else in our environment they just see part of the larger picture, for full picture views and data correlation we use a **SIEM** (Security Information and Event Management) system or even better a **SOAR** (Security Orchestration, Automation, and Response) system.

- **IDS (Intrusion Detection System):**

- They are passive, they monitor, but they take no action other than sending out alerts.
- Events trigger alerts: Emails/text message to administrators or an alert on a monitoring tool, but if not monitored right this can take hours before noticed.

- **IPS (Intrusion Prevention System):**

- Similar to IDS, but they also take action to malicious traffic, what they do with the traffic is determined by configuration.
- Events trigger an action, drop/redirect traffic, often combined with the trigger monitoring/administrator warnings, emails or text messages.

- **IDS/IPS:**

- Part of our layered defense.
- Basically they are packet sniffers with analysis engines.

- **Network-Based**, placed on a network segment (a switch port in promiscuous mode).

- Looks at a segment of our network, normally a switch, but can aggregate multiple switches.
- Inspects Host/destination ports, IP's, protocols, content of traffic, but can obviously not look in encrypted traffic.
- Can protect against DDOS, Port scans, brute force attacks, policy violations,...
- Deployed on one switch, port and NIC must be promiscuous and port must be a span port.

- **Host-Based**, on a client, normally a server or workstation.

- We only look at a single system.
- Who is using the system, the resource usage, traffic,...
- It can be application specific, it doesn't have to be the entire system we monitor.
- If we do chose to do traffic analysis it will impact the host by slowing it down.



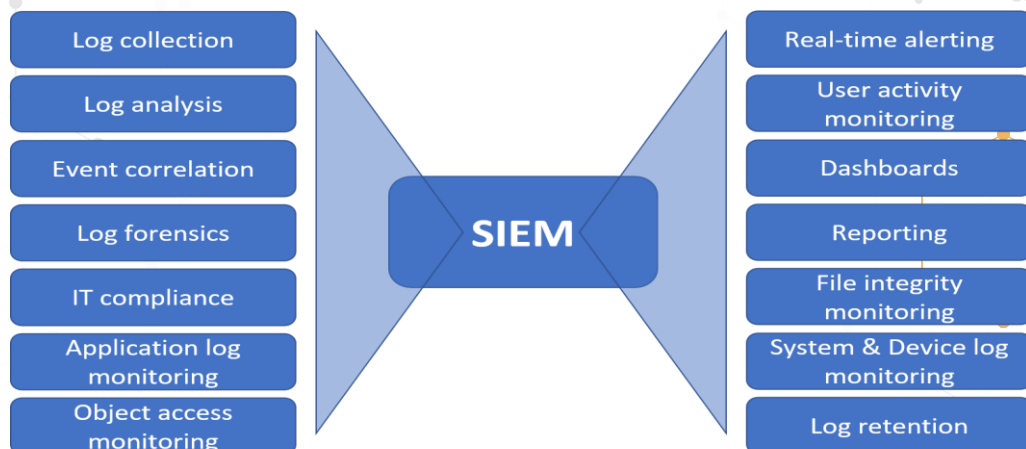
- Certain attacks can turn off HIDS/HIPS.
- Can look at the actual data (it is decrypted at the end device), NIDS/NIPS can't look at encrypted packets.
- **Signature-Based:**
  - Looks for known malware signatures.
  - Faster since they just check traffic against malicious signatures.
  - Easier to set up and manage, someone else does the signatures for us.
  - They are completely vulnerable to 0 day attacks, and have to be updated constantly to keep up with new vulnerability patterns.
- **Heuristic-Based (Behavioral):**
  - Looks for abnormal behavior - can produce a lot of false positives.
  - We build a baseline of what normal network traffic looks like and all traffic is matched to that baseline.
  - Traffic not matching the baseline is handled depending on settings, they can take a lot of tweaking.
  - Can detect 'out of the ordinary' activity, not just attacks.
  - Takes much more work and skills.
- **Hybrid-Based** systems combining both are more used now and check for both signatures and abnormalities.
- **Intrusion Events and Masking:**
  - IDS/IPS obviously then prompt attackers to develop attacks that try to avoid detection.
    - ♦ **Fragmentation:** Sending fragmented packets, the attack can avoid the detection system's ability to detect the attack signature.
    - ♦ **Avoiding Defaults:** The TCP port utilized by a protocol does not always provide an indication to the protocol which is being transported. Attackers can send malware over an unexpected port.
    - ♦ **Low-Bandwidth Coordinated Attacks:** A number of attackers (or agents) allocate different ports or hosts to different attackers making it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.
    - ♦ **Address spoofing/proxying:** attackers can use poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server then it makes it very difficult for IDS to detect the origin of the attack.
    - ♦ **Pattern Change Evasion:** The attacker changes the data used slightly, which may avoid detection.



- Alerts on IDS's/IPS's can, like biometrics, be one of 4 categories:
  - ♦ **True Positive:** An attack is happening and the system detects it and acts.
  - ♦ **True Negative:** Normal traffic on the network and the system detects it and does nothing.
  - ♦ **False Positive:** Normal traffic and the system detects it and acts.
  - ♦ **False Negative:** An attack is happening the system does not detect it and does nothing.
- We rarely talk about the "true" states since things are happening like they are supposed to, we are interested in when it doesn't and we prevent authorized traffic or allow malicious traffic.

	TRUE	FALSE
POSITIVE	True-Positive Rule matched Attack	False-Positive Rule matched No attack
NEGATIVE	True-Negative No rule matched No attack	False-Negative No rule matched Attack

- **SIEM (Security information and event management):**
  - Often pronounced SEM or SIM.
  - Provides a holistic view of our organization's events and incidents.
  - Gathers from all our systems and looks at everything
  - Centralizes the storage and interpretation of logs, traffic and allows near real-time automated identification, analysis and recovery of security events.







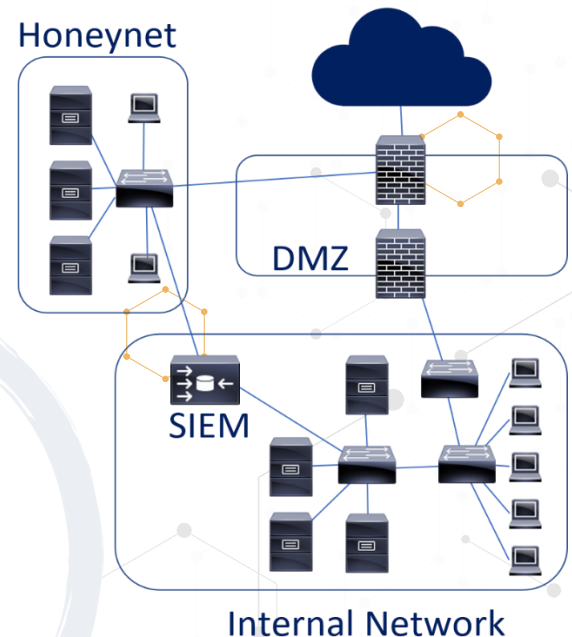
- **SOAR (Security Orchestration, Automation, and Response):**
  - A software solution that uses AI to allow us to respond to some security incidents automatically.
  - SOAR vs. SIEM: Very similar, both detect/alert on security events, but using AI, SOAR will also react to some events.
    - ♦ SIEMs often generate more alerts than a SOC team can handle, SOAR can reduce that.
  - SOAR combines all the comprehensive data we gather, has case management, standardization, workflows, and analytics, and it can integrate with many of our other solutions (Vulnerability Management (VM), IT Service Management (ITSM), Threat Intelligence, ...).
  - All this can help our organization implement a detailed defense-in-depth solution.
- **Application Positive-listing:**
  - We can positive-list the applications we want to allow to run on our environments, but it can also be compromised.
  - We would positive-list against a trusted digital certificate, a known hash or path and name, the latter is the least secure, an attacker can replace the file at the path with a malicious copy.
  - Building the trusted application positive-list takes a good deal of time, but is far superior to negative-listing, there are 10,000's of application and we can never keep up with them.
- **Removable Media Controls:**
  - Good security policies would also have us lock down USB ports, CD drives, memory card ports and anything else where you can load malicious code onto our systems from external devices.
  - For servers we may rarely have to enable USB ports for firmware or other updates, we would enable the ports while we use them and lock them right away after, it is safer to be done centrally via group policies or similar.
- **Honeypots and Honeynets:**
  - **Honeypots:**
    - ♦ System looking like a real system, but with the sole purpose of attracting attackers.
    - ♦ They are used to learn about our vulnerabilities and how attackers would circumvent our security measures.
    - ♦ Used both internally and externally, internal honeypots can alert us to attackers and malware that made it past our security perimeter and external honeypots teach us about the attack vectors attackers use.
    - ♦ External honeypots will get compromised on a regular basis, we analyze the attack and ensure our internal systems are protected against that type of attack.



- ♦ Honeypots are rarely hardened completely, our actual data servers are always hardened completely.
- ♦ Always talk to your legal department before deploying honeypots.
  - Remember the thin line between entrapment and enticement.
  - What are the legal/liability ramifications if an attacker launches a 3rd party attack from your honeypot/net.
  - Get very clear legal guidelines issued before deploying, and get senior management's approval in writing.

- **Honeynets:**

- ♦ A network (real or simulated) of honeypots, can be a full server farm simulated with applications, OS's and fake data.
- ♦ Best practice segments the honeynet from our actual network by a DMZ/firewall.
- ♦ The SIEM/SOAR systems collect the data from our internal systems as well as the honeynet.



- **Configuration Management:**

- When we receive or build new systems they often are completely open, before we introduce them to our environment we harden them.
- We develop a long list of ports to close, services to disable, accounts to delete, missing patches and many other things.
- Often it is easier to have OS images that are completely hardened and use the image for the new system, we then update the image when new vulnerabilities are found or patches need to be applied, often though we use a standard image and just apply the missing patches.
- We do this for any device on our network, servers, workstations, phones, routers, switches,...
- Pre-introduction into our production environment we run vulnerability scans against the system to ensure we didn't miss anything (Rarely done on workstations, should be done on servers/network equipment).
- Having a standard hardening baseline for each OS ensures all servers are similarly hardened and there should be no weak links, we also have the standardized hardening making troubleshooting much easier.
- Once a system is introduced to our production environment we monitor changes away from our security baseline, most changes are administrators troubleshooting or making workarounds, which may or may not be allowed, but it could also be an attacker punching a path out of our network.



### ▶ Asset Management:

#### • Patch Management:

- In order to keep our network secure we need to apply patches on a regular basis.
- Whenever a vulnerability is discovered the software producer should release a patch to fix it.
- Microsoft for instance have "Patch Tuesday" (2nd Tuesday of the month).
  - ♦ They release all their patches for that month.
  - ♦ If critical vulnerabilities are discovered they push those patches outside of Patch Tuesday.
  - ♦ Most organizations give the patches a few weeks to be reviewed and then implement them in their environment.
- We normally remember the OS patches, but can often forget about network equipment updates, array updates, IoT updates and so on, if they are not patched we are not fully using defense in depth and we can expose ourselves to risk.
- I have seen places where full rack disk arrays were not encrypted and had not been patched since installation over 10 years prior, the reasoning was poorly designed data storage and updating would take the disks offline for up to an hour, which for the organization was unacceptable.
- We use software to push our patches to all appropriate systems, this is easier, we ensure all systems gets patched and they all get the same parts of the patch, we may exclude some parts that have an adverse effect on our network.
- Common tools could be SCCM or WSUS, they do not only push patches, but any software we want to distribute to our organization.
- We do the pushes after hours to not impact the availability during working hours, normally done Friday or Saturday night somewhere between 01:00 am and 04:00 am.
- Most places avoid midnight as a lot of backups and jobs run at that time, and end no later than 04:00 am or 05:00 am to ensure systems are online by the start of business the following day.

#### • Change Management:

- Our formalized process on how we handle changes to our environments.
- If done right we will have full documentation, understanding and we communicate changes to appropriate parties.
- The change review board should be comprised of both IT and other operational units from the organization, we may consider impacts on IT, but we are there to serve the organization, they need to understand how it will impact them and raise concerns if they have any.
- A change is proposed to the change board, they research in order to understand the full impact of the change.
- The person or group submitting the change should clearly explain the reasons for the change, the pro's and con's of implementing and not implementing, any



changes to systems and processes they know about and in general aide and support the board with as much information as needed.

- The board can have senior leadership on it or they can have a predefined range of changes they can approve and anything above that threshold they would make recommendations but changes require senior leadership approval.
- There are many different models and process flows for change management, some are dependent on organization structure, maturity, field of business and many other factors.

- ♦ A generalized flow would look like this:

1. Identifying the change.
2. Propose the change.
3. Assessing risks, impacts and benefits of implementing and not implementing.
4. Provisional change approval, if testing is what we expect this is the final approval.
5. Testing the change, if what we expected we proceed, if not we go back.
6. Scheduling the change.
7. Change notification for impacted parties.
8. Implementing the change.
9. Post implementation reporting of the actual change impact.

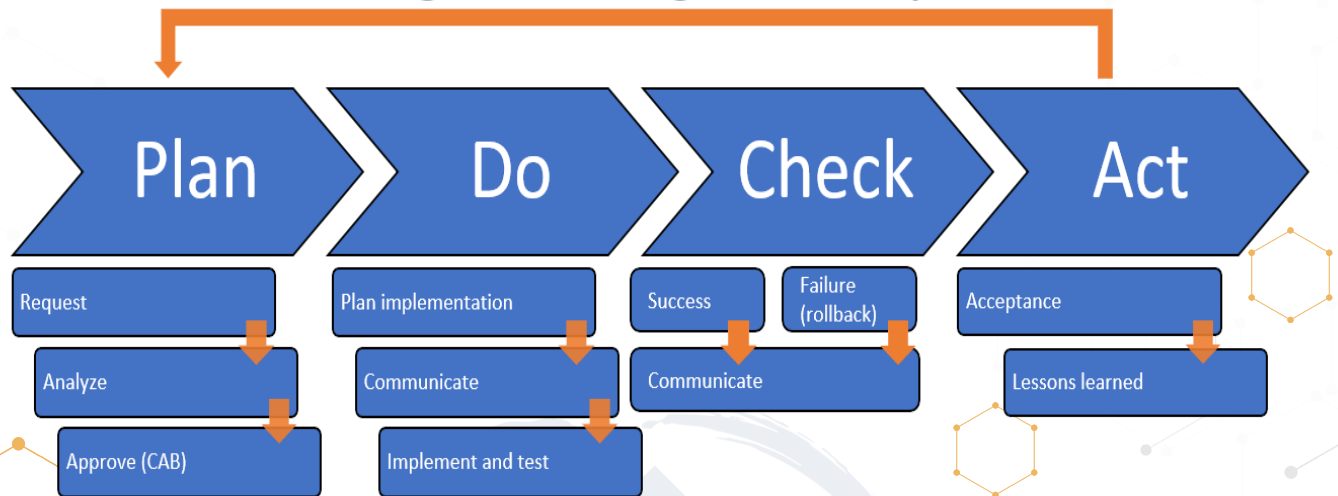
- We closely monitor and audit changes, remember changes can hold residual risk which we would then have to mitigate.
- Everything in the change control process should be documented and kept, often auditors want to see that we have implemented proper change controls, and that we actually follow the paper process we have presented them with.







# The Change management process



- **0-day Vulnerabilities:**

- Vulnerabilities not generally known or discovered, the first time an attack is seen is considered day 0, hence the name.
- From when a vulnerability is discovered it is now only a short timespan before patches or signatures are released on major software.
- With millions of lines of code in a lot of software and the 1% errors we talked about there will always be new attack surfaces and vulnerabilities to discover. The only real defense against the 0 day exploits is defense in depth and when discovered immediate patching as soon as it is available and we have tested it in our test environments. Most signatures in IDS/IPS and anti virus auto update as soon as new signatures are available.
- **0-day Vulnerability:** The vulnerability that has not been widely discovered and published.
- **0-day Exploit:** Code that uses the 0-day vulnerability.
- **0-day Attack:** The actual attack using the code.
- The Stuxnet worm that targeted Iran's nuclear centrifuges used 4 unique 0-day exploits (previously unheard of).
- It was developed over 5+ years and estimated to have cost 100's of millions of dollars.
- **Stuxnet has three modules:**
  - ♦ A **worm** that executes all routines related to the main payload of the attack;
  - ♦ A **link** file that automatically executes the propagated copies of the worm.
  - ♦ A **rootkit** responsible for hiding all malicious files and processes, preventing detection of Stuxnet.
- It is introduced to the target environment by an infected USB flash drive.



- The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC, If both are not present, Stuxnet becomes dormant inside the computer, it will still replicate the worm.
- If both are present, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

### ► Continuity of Operations:

#### • Fault Tolerance:

- To ensure our internal SLAs and provide as high availability as possible we use as high degree of redundancy and resiliency as makes sense to that particular system and data set.

#### ▪ Backups:

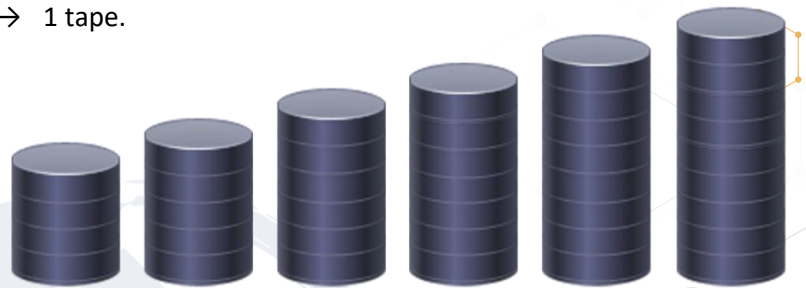
- ♦ One of the first things that comes to mind when talking about fault tolerance is backups of our data, while it is very important it is often like log reviews an afterthought and treated with "Set it and forget it" mentality.
- ♦ For backups we use Full, Incremental, Differential and Copy backups, and how we use them is determined on what we need from our backups.
- ♦ How much data we can stand to lose and how fast we want the backup and restore process to be.
- ♦ In our backup solution we make backup policies of what to back up, what to exclude, how long to keep the data of the Full, Incremental and Differential backups.
- ♦ All these values are assigned dependent on what we back up, and normal organizations would have different backup policies and apply those to the appropriate data.
- ♦ This could be Full 3, 6, 12, 36, 84 months and infinity, the retention is often mandated by our policies and the regulations in our field of business.
- ♦ It is preferable to run backups outside of business hours, but if the backup solution is a little older it can be required to run around the clock, in that case we put the smaller and less important backups in the daytime and the important larger ones after hours.
- ♦ We often want to exclude parts of the system we are backing up, this could be the OS, the trashcan, certain program folders, ... we just backup what is important and rarely everything.
- ♦ If a system is compromised and the issue is a rootkit, the rootkit would persist on the backup if we did a full mirror restore, by eliminating some of the system data we not only backup a lot less data, we also may avoid the infection we are trying to remedy.
- ♦ For very important data we may do hourly incremental or use another form of data loss prevention (covered later in this chapter).



### ♦ Full Backup:



- This backs everything up, the entire database (most often), or the system.
- A full backup clears all archive bits.
- Dependent on the size of the data we may do infrequent full backups, with large datasets it can take many hours for a full backup.
- **IF we need to restore on Thursday:**
  - Restore with a single Wednesday full backup tape.
  - 1 tape.



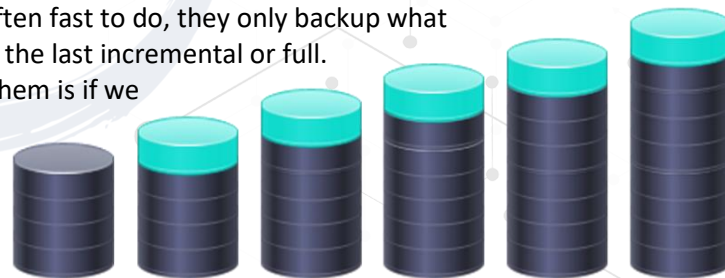
### Full Backup:

Everything in the backup policy is backed up.

### ♦ Incremental Backup:



- Backs up everything that has changed since the last backup.
- Clears the archive bits.
- Incremental are often fast to do, they only backup what has changed since the last incremental or full.
- The downside to them is if we do a monthly full backup and daily incremental, we have to get a full restore and could have to use up to 30 tapes, this would take a lot longer than with 1 Full and 1 Differential.




### Incremental Backup:

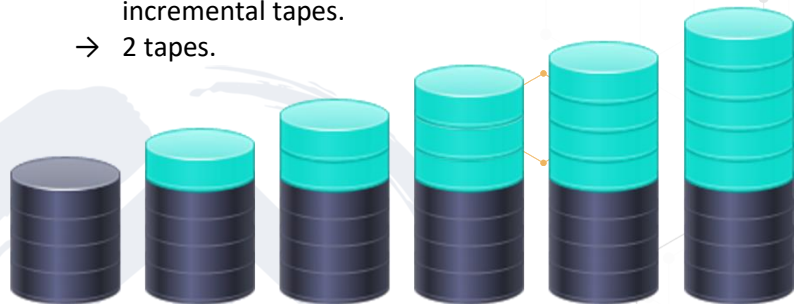
- Anything changed since the last backup is backed up.
- The archive bit is cleared.

### ▫ IF we need to restore on Thursday:

- Restore with the full Sunday backup and Monday, Tuesday, and Wednesday's incremental tapes.
- 4 tapes.



- ♦ **Differential Backup:** 
  - Backs up everything since the last Full backup.
  - Does not clear the archive bit.
  - Faster to restore since we just need 2 tapes for a full restore, the full and the differential.
  - Backups take longer than the incremental, we are backing everything since the last full.
  - Never use both incremental and differential on the same data, it is fine on the same backup solution, different data has different needs.
  - **IF we need to restore on Thursday:**
    - Restore with the Sunday full backup and Wednesday's incremental tapes.
    - 2 tapes.



### Differential Backup:

- Anything changed since the last Full backup is backed up.
  - The archive bit is not cleared.
- ♦ **Copy Backup:**
    - This is a full backup with one important difference, it does not clear the archive bit.
    - Often used before we do system updates, patches and similar upgrades.
    - We do not want to mess up the backup cycle, but we want to be able to revert to a previous good copy if something goes wrong.
  - ♦ **Archive Bit:**
    - For Windows the NTFS has an archive bit on file, it is a flag that indicates if the file was changed since the last Full or Incremental backup.





- On our systems we build in fault tolerance to give them as high as possible uptime, we do this with redundant hardware and systems, one of the practices we use is RAID.

- RAID (Redundant Array of Independent/Inexpensive Disks):**



- Comes in 2 basic forms, disk mirroring and disk striping.

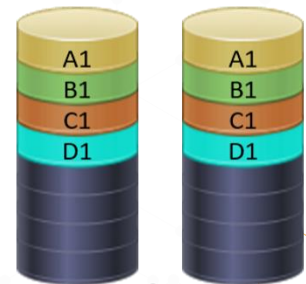
- Disk Mirroring:**

- Writing the same data across multiple hard disks, this is slower, the RAID controller has to write all data twice.
- Uses at least 2 times as many disks for the same data storage, needs at least 2 disks.

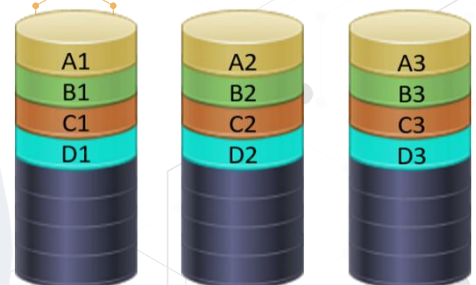
- Disk Striping:**

- Writing the data simultaneously across multiple disks providing higher write speed.
- Uses at least 2 disks, and in it self does not provide redundancy.
- We use parity with striping for the redundancy, often by XOR, if we use parity for redundancy we need at least 3 disks.

### Disk Mirroring: Disk A      Disk B



### Disk Striping, no parity: Disk A      Disk B      Disk C



- There are many different types of RAID, for the exam I would know the above terms and how RAID 0, 1 and 5 works.

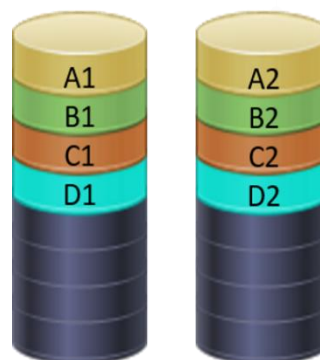
- RAID 0:**

- Striping with no mirroring or parity, no fault tolerance, only provides faster read write speed, requires at least 2 disks

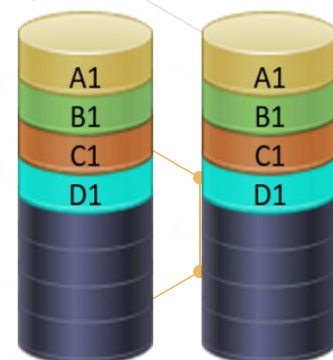
- RAID 1:**

- Mirror set, 2 disks with identical data, and write function is written to both disks simultaneously.

### RAID 0



### RAID 1





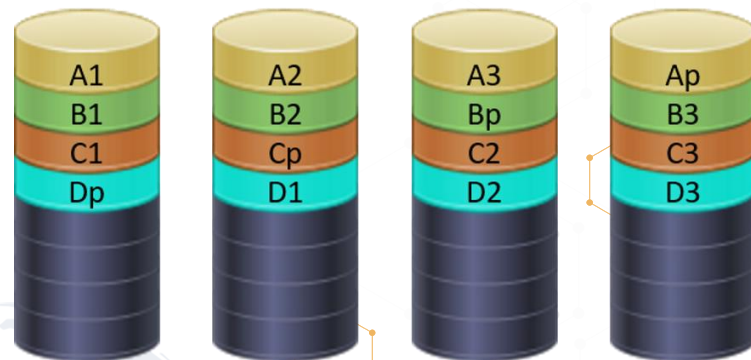
### ▪ RAID 5:



- ♦ Block level striping with distributed parity, requires at least 3 disks.
- ♦ Combined speed with redundancy.

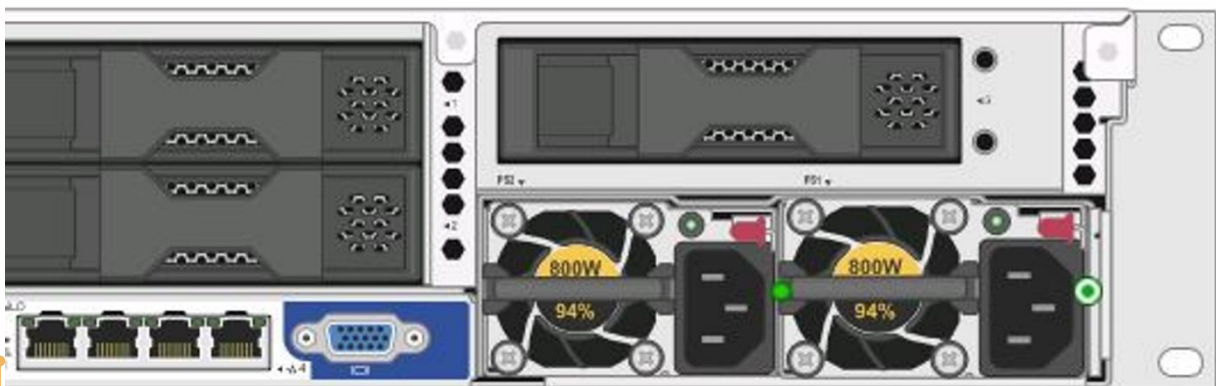
- RAID will help with data loss when we have a single disk failure if we use a fault tolerant RAID type, if more than one disk fails before the first is replaced and rebuilt, we would need to restore from our tapes.
- Most servers have the same disks with the same manufacturer date, they will hit their MTBF (Mean time between failures) around the same time.
- Larger data centers often have SLA's with the hard disk/server vendor, which also includes MTTR (Mean time to repair).
- This could be within 4 or 8 hours the vendor has to be onsite with a replacement disk.

### RAID 5



### • System Redundancy:

- On top of the RAID and the backups we also try to provide system redundancy as well as redundant parts on the systems.
- The most common system failures are from pieces with moving parts, this could be disks, fans or PSU (power supplies).
- Most servers have redundant power supplies, extra fans, redundant NIC's.
- The NIC and PSU serve a dual purpose, both for internal redundancy and external. If a UPS fails, the server is still operational with just the 1 PSU getting power.
- Redundant disk controllers are also reasonably common, we design and buy the system to match the redundancy we need for that application.



Redundant PSU's in s server



- Often we have spare hardware on hand in the event of a failure, this could include hard disks, PSU's, fans, memory, NICs.
- Many systems are built for some hardware to be hot-swappable, most commonly HDD's, PSU's and fans.
- If the application or system is important we often also have multiple systems in a cluster.
- Multiple servers often with a virtual IP, seen as a single server to users.
- Clustering is designed for fault tolerance, often combined with load balancing, but not innately.
- Clustering can be active/active, this is load balancing, with 2 servers both servers would actively process traffic.
- Active/passive: There is a designated primary active server and a secondary passive server, they are connected and the passive sends a keep-alive or heartbeat every 1-3 seconds, are you alive, are you alive,... AS long as the active server responds the passive does nothing, if the active does not respond for (normally) 3 keepalives the passive assumes the primary is dead and assumes the primary role.
- In well designed environments the servers are geographically dispersed.
- We can also use other complementary backup strategies to give ourselves more real time resilience, and faster recovery.
- **Database Shadowing:**
  - ♦ Exact real time copy of the database or files to another location.
  - ♦ It can be another disk in the same server, but best practice dictates another geographical location, often on a different media.
- **Electronic Vaulting (E-vaulting):**
  - ♦ Using a remote backup service, backups are sent off-site electronically at a certain interval or when files change.
- **Remote Journaling:**
  - ♦ Sends transaction log files to a remote location, not the files themselves. The transactions can be rebuilt from the logs if we lose the original files.



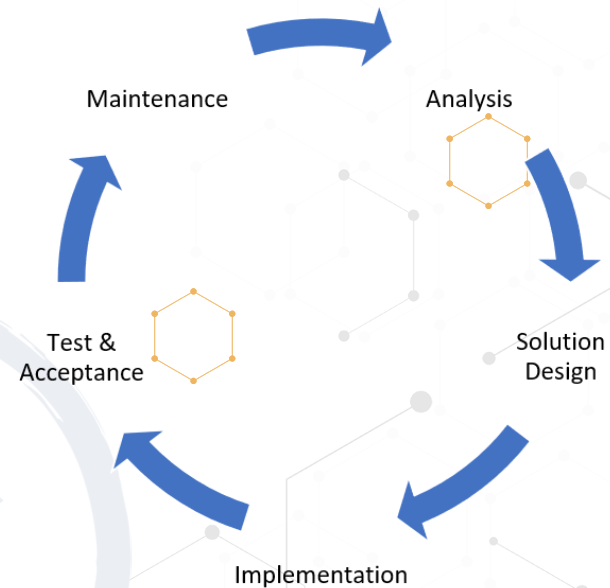
### ► BCP and DRP:

- Any organization will encounter disasters every so often, how we try to avoid them, how we mitigate them and how we recover when they happen is very important.
- If we do a poor job the organization may be severely impacted or have to close.
- Companies that had a major loss of data, 43% never reopen and 29% close within two years.

#### • BCP (Business Continuity Plan):



- This is the process of creating the long-term strategic business plans, policies and procedures for continued operation after a disruptive event.
- It is for the entire organization, everything that could be impacted, not just IT.
- Lists a range of disaster scenarios and the steps the organization must take in any particular scenario to return to regular operations.
- BCP's often contain COOP (Continuity of Operations Plan), Crisis Communications Plan, Critical Infrastructure Protection Plan, Cyber Incident Response Plan, DRP (Disaster Recovery Plan), ISCP (Information System Contingency Plan), Occupant Emergency Plan.
- What would we do if a critical supplier closed, the facility was hit by an earthquake, what if we were snowed in and staff couldn't get to work,...
  - ♦ They are written ahead of time, and continually improved upon, it is an iterative process.
  - ♦ We write the BCP with input from key staff and at times outside BCP consultants.



#### • DRP (Disaster Recovery Plan):

- This is the process of creating the short-term plans, policies, procedures and tools to enable the recovery or continuation of vital IT systems in a disaster.
- It focuses on the IT systems supporting critical business functions, and how we get those back up after a disaster.
- DRP is a subset of our BCP.
- We look at what we would do if we get hit with a DDOS attack (can be in the DRP or in our Cyber Incident Response Plan), a server gets compromised, we experience a power outage, ...
- Often the how and system specific, where the BCP is more what and non-system specific.





- We categorize disasters in 3 categories: **Natural, Human, or Environmental.**
  - **Natural:**
    - ♦ Anything caused by nature, this could be earthquakes, floods, snow, tornados, ...
    - ♦ They can be very devastating, but are less common than the other types of threats.
    - ♦ The natural disaster threats are different in different areas, we do the risk analysis on our area.
    - ♦ For one site we could build our buildings and data center earthquake resilient and another flood resilient.
  - **Human:**
    - ♦ Anything caused by humans, they can be intentional or unintentional disasters.
    - ♦ Unintentional could be an employee uses a personal USB stick on a PC at work and spreads malware, just as bad as if an attacker had done it, but the employee were just ignorant, lazy or didn't think it would matter.
    - ♦ Intentional could be malware, terrorism, DOS attacks, hacktivism, phishing, ...
  - **Environmental (Not to be confused with natural disasters):**
    - ♦ Anything in our environment, could be power outage/spikes, hardware failures, provider issues, ...
- **Errors and Omissions (Human):**
  - The most common reason for disruptive events are internal employees, often called errors and omissions.
  - They are not intending to harm our organization, but they can inadvertently do so by making mistakes or not following proper security protocols.
  - This could be a mistype, leaving a door unlocked to go outside to smoke or leaving a box of backup tapes somewhere not secure.
  - They often have a minor impact, but if we have issues where they are deemed very common or potentially damaging we can build in controls to mitigate them.
  - We could put a double check in place for the mistype, an alarm on the unlocked door that sounds after being open for 10 seconds, or very clear procedures and controls for the transport of backup tapes.
- **Electrical or Power Problems (Environmental):**
  - Are power outages common in our area?
  - Do we have proper battery and generator backup to sustain our sites for an extended period of time?
  - We want the redundancy of UPS's and generators, they both supply constant and clean power.
  - These should always be in place in data centers, but what about our other buildings?
  - Power fluctuations can damage hardware.





- **Heat (Environmental):**
  - Many data centers are kept too cold, the last decades research has shown it is not needed.
  - Common temperature levels range from 68–77 °F (20–25 °C) - with an allowable range 59–90 °F (15–32 °C).
  - Keeping a Data Center too cold wastes money and raises humidity.
- **Pressure (Environmental):** Keeping positive pressure keeps outside contaminants out.
- **Humidity (Environmental):** Humidity should be kept between 40 and 60% rH (Relative Humidity).
  - Low humidity will cause static electricity and high humidity will corrode metals (electronics).
- **Warfare, Terrorism and Sabotage (Human):**
  - We still see plenty of conventional conflicts and wars, but there is much more happening behind the veil of the internet, hacking for causes, countries, religion and many more reasons.
  - It makes sense to cripple a country's or region's infrastructure if you want to invade or just destabilize that area.
  - This could be for war, trade, influence or many other reasons, everything is so interconnected we can shut down water, electricity or power from across the world.
  - The targets are not always the obvious targets, hospitals, air travel, shipping, production,... are potential targets.
  - **State, Cause or Religious Hacking (Human):**
    - ♦ Common, we often see the attacks happening 9-5 in that time zone, this is a day job.
    - ♦ Approximate 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
    - ♦ Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China),...



- **Financially Motivated Attackers (Human):**

- We are seeing more and more financially motivated attacks, they can be both highly skilled or not.
- The lower skilled ones could be normal phishing attacks, social engineering or vishing, these are often a numbers game, but only a very small percentage needs to pay to make it worth the attack.
- The ones requiring more skills could be stealing cardholder data, identity theft, fake anti-malware tools, or corporate espionage,...
- Ransomware is a subtype of financially motivated attacks, it will encrypt a system until a ransom is paid, if not paid the system is unusable, if paid the attacker may send instructions on how to recover the system.
- Attackers just want the payday, they don't really care from whom.




WannaCry ransomware screenshot from an infected system.

- **Personnel Shortages(Human/Nature/Environmental):**

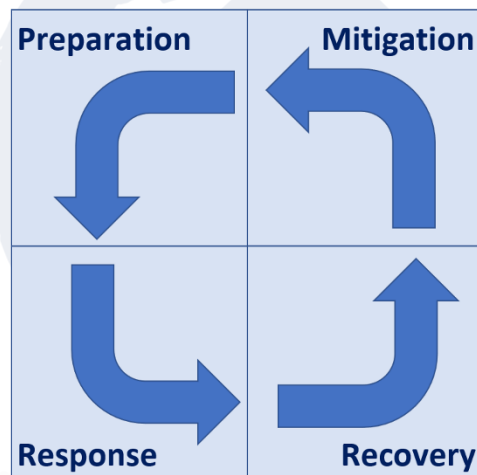
- In our BCP, we also have to ensure that we have redundancy for our personnel and how we handle cases where we have staff shortages.
- If we have 10% of our staff, how impacted is our organization?
- This can be caused by natural events (snow, hurricane) but is more commonly caused by the flu or other viruses.
- **Pandemics:**
  - ♦ Organizations should identify critical staff by position not by name, and have it on hand for potential epidemics. <Insert your own COVID-19 work experiences here.>
- **Strikes:**
  - ♦ A work stoppage caused by the mass refusal of employees to work.
  - ♦ Usually takes place in response to employee grievances.
  - ♦ How diminished of a workforce can we have to continue to function?
- **Travel:**
  - ♦ When our employees travel, we need to ensure both they and our data is safe.
  - ♦ That may mean avoiding certain locations, limiting what they bring of hardware and what they can access from the remote location.
  - ♦ If they need laptops/smartphones, we use encryption, device monitoring, VPNs, and all other appropriate measures.



- Our **DRP (Disaster Recovery Plan)** should answer at least three basic questions:
  - What is the objective and purpose?
  - Who will be the people or teams who will be responsible in case any disruptions happen?
  - What will these people do (our procedures) when the disaster hits?
- Normal plans are a lot more in depth and outline many different scenarios, they have a clear definition of what a disaster is, who can declare it, who should be informed, how often we send updates to whom, who does what,...
- It is easy to just focus on getting back up and running when we are in the middle of a disaster, staff often forget about communication, preserving the crime scene (if any) and in general our written procedures.
-  **DRP has a lifecycle of Mitigation, Preparation, Response and Recovery.**
  - **Mitigation:** Reduce the impact, and likelihood of a disaster.
  - **Preparation:** Build programs, procedures and tools for our response.
  - **Response:** How we react in a disaster, following the procedures.
  - **Recovery:** Reestablish basic functionality and get back to full production.

Education,  
Plans,  
Processes &  
Training.

DR/BCP/EOP  
(emergency  
Operations  
plan)



Pre-disaster  
mitigation  
implementations.

Post-disaster  
recovery plan.

- We have looked at the first 2 before, for now we will focus on Response and Recovery.
  - **Response:** How we react in a disaster, following the procedures.
    - ♦ How we respond and how quickly we respond is essential in Disaster Recovery.
    - ♦ We assess if the incident we were alerted to or discovered is serious and could be a disaster, the assessment is an iterative process.
      - The more we learn and as the team gets involved we can assess the disaster better.
    - ♦ We notify appropriate staff to help with the incident (often a call tree or automated calls), inform the senior management identified in our plans and if indicated by the plan communicate with any other appropriate staff.



- **Recovery:** Reestablish basic functionality and get back to full production.
  - ♦ We act on our assessment using the plan.
  - ♦ At this point all key stakeholders should be involved, we have a clearer picture of the disaster and take the appropriate steps to recover. This could be DR site, system rebuilds, traffic redirects,...

### ► Developing our BCP and DRP:

- Older versions of NIST 800-34 had these steps as a framework for building our BCP/DRP, they are still very applicable.
- **Project Initiation:** We start the project, identify stakeholders, get C-level approval and formalize the project structure.
- **Scope the Project:** We identify exactly what we are trying to do and what we are not.
- **Business Impact Analysis:** We identify and prioritize critical systems and components.
- **Identify Preventive Controls:** We identify the current and possible preventative controls we can deploy.
- **Recovery Strategy:** How do we recover efficiently? What are our options? DR site, system restore, cloud,...
- **Plan Design and Development:** We build a specific plan for recovery from a disaster, procedures, guidelines and tools.
- **Implementation, Training, and Testing:** We test the plan to find gaps and we train staff to be able to act on the plan.
- **BCP/DRP Maintenance:** It is an iterative process. Our organization develops, adds systems, facilities or technologies and the threat landscape constantly changes, we have to keep improving and tweaking our BCP and DRP.




- Senior management needs to be involved and committed to the BCP/DRP process, without that it is just lip service.
  - They need to be part of at least the initiation and the final approval of the plans.
  - They are responsible for the plan, they own the plan and since they are ultimately liable, they must show due-care and due-diligence.
  - We need top-down IT security in our organization (the exam assumed we have that).
  - In serious disasters, it will be Senior Management or someone from our legal department that will talk to the press.
  - Most business areas often feel they are the most important area and because of that their systems and facilities should receive the priority, senior management being ultimately liable and the leaders of our organization, obviously have the final say in priorities, implementations and the plans themselves.



- BCP/DRP's are often built using the waterfall project management methodology, we will cover it in the next domain.
- The BCP team has sub-teams responsible for rescue, recovery and salvage in the event of a disaster or disruption.

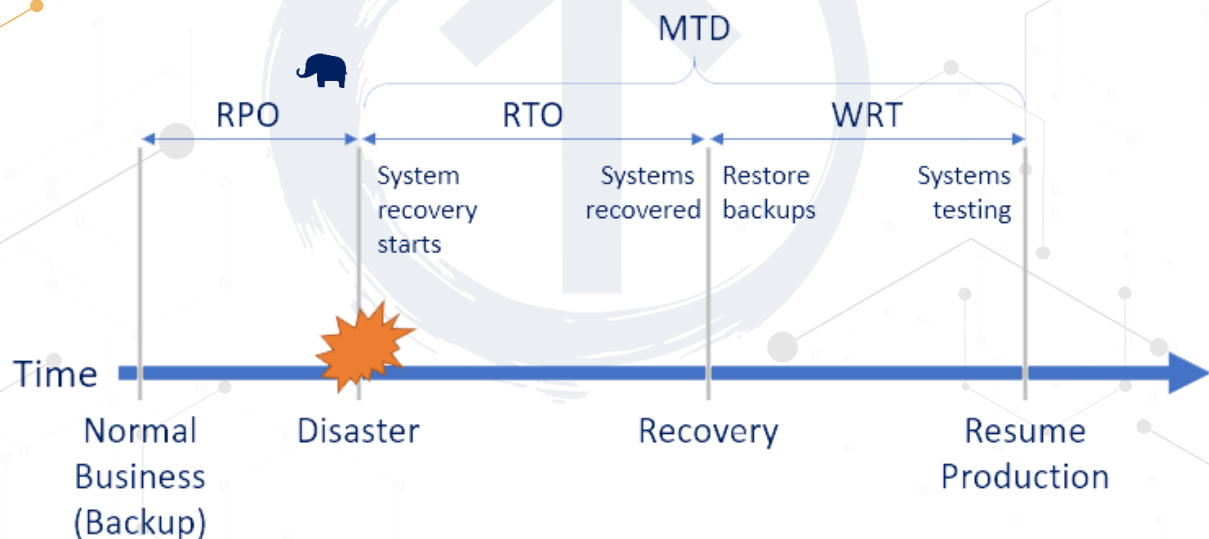


- **Rescue Team (Activation/Notification):**
  - ♦ Responsible for dealing with the disaster as it happens. Evacuates employees, notifies the appropriate personnel (call trees) pulls the network from the infected server or shuts down systems, and initial damage assessment.
- **Recovery Team (Failover):**
  - ♦ Responsible for getting the alternate site up and running as fast as possible or for getting the systems rebuilt.
  - ♦ We get the most critical systems up first.
- **Salvage Team (Failback):**
  - ♦ Responsible for returning our full infrastructure, staff and operations to our primary site or a new facility if the old site was destroyed.
  - ♦ We get the least critical systems up first, we want to ensure the new sites is ready and stable before moving the critical systems back.
- **BIA (Business Impact Analysis):** 
  - Identifies critical and non-critical organization systems, functions and activities.
  - Critical is where disruption is considered unacceptable, the acceptability is also based on the cost of recovery.
  - A function may also be considered critical if dictated by law.
  - For each critical (in scope) system, function or activity, two values are then assigned:
  - **RPO (Recovery Point Objective):** The acceptable amount of data that can not be recovered.
    - ♦ The recovery point objective must ensure that the maximum tolerable data loss for each system, function or activity is not exceeded.
    - ♦ If we only back up once a week, we accept up to a week of data loss.
  - **MTD (Maximum Tolerable Downtime)  $MTD \geq RTO + WRT$ :**
    - ♦ The time to rebuild the system and configure it for reinsertion into production must be less than or equal to our MTD.
    - ♦ The total time a system can be inoperable before our organization is severely impacted.
    - ♦ Remember companies that had a major loss of data, 43% never reopen and 29% close within two years.
    - ♦ Other frameworks may use other terms for MTD, but for the exam know and use MTD.
    - ♦ MAD (Maximum Allowable Downtime), MTO (Maximum Tolerable Outage), MAO (Maximum Acceptable Outage), MTPoD (Maximum Tolerable Period of Disruption).








- **RTO (Recovery Time Objective):** The amount of time to restore the system (hardware).
  - ♦ The recovery time objective must ensure that the MTD for each system, function or activity is not exceeded.
- **WRT (Work Recovery Time)** (software):
  - ♦ How much time is required to configure a recovered system.
- **MTBF (Mean Time Between Failures):**
  - ♦ How long a new or repaired system or component will function on average before failing, this can help us plan for spares and give us an idea of how often we can expect hardware to fail.
- **MTTR (Mean Time to Repair):**
  - ♦ How long it will take to recover a failed system.
- **MOR (Minimum Operating Requirements):**
  - ♦ The minimum environmental and connectivity requirements for our critical systems to function, can also at times have minimum system requirements for DR sites.
  - ♦ We may not need a fully spec'd system to resume the business functionality.



- **MTBF (Mean Time Between Failures):** How long a system or component will function on average before failing.
- **MTTR (Mean Time to Repair):** How long it will take to recover a failed system.
- **MOR (Minimum Operating Requirements):** The minimum environmental and connectivity requirements for our critical systems to function, can also at times have minimum system requirements for DR sites.



### ► Recovery Strategies:

- In our recovery process we have to consider the many factors that can impact us, we need look at our options if our suppliers, contractors or the infrastructure are impacted as well.
- We may be able to get our data center up and running in 12 hours, but if we have no outside connectivity that may not matter.
- **Supply chain:**
  - If an earthquake hits, do our local suppliers function, can we get supplies from farther away, is the infrastructure intact?
- **Infrastructure:** How long can we be without water, sewage, power,...?
  - We can use generators for power, but how long do we have fuel for?
  - In prolonged power outages, we have pre-determined critical systems we leave up and everything else is shut down to preserve power (fuel) and lessen HVAC requirements.
- **Recovery Strategies:**
  - From our MTD we can determine our approach to how we handle disasters and the safeguards we put in place to mitigate or recover from them.
  - **Redundant Site:**
    - ♦ Complete identical site to our production, receives a real time copy of our data.
    - ♦ Power, HVAC, Raised floors, generators,...
    - ♦ If our main site is down the redundant site will automatically have all traffic fail over to the redundant site.
    - ♦ The redundant site should be geographically distant, and have staff at it.
    - ♦ By far the most expensive recovery option, end users will never notice the fail over.
  - **Hot Site:**
    - ♦ Similar to the redundant site, but only houses critical applications and systems, often on lower spec'd systems.
    - ♦ Still often a smaller but a full data center, with redundant UPS's, HVAC's, ISP's, generators,...
    - ♦ We may have to manually fail traffic over, but a full switch can take an hour or less.
    - ♦ Near or real-time copies of data.
  - **Warm Site:**
    - ♦ Similar to the hot site, but not with real or near-real time data, often restored with backups.
    - ♦ A smaller but full data center, with redundant UPS's, HVAC's, ISP's, generators,...
    - ♦ We manually fail traffic over, a full switch and restore can take 4-24+ hrs.



### ▪ Cold Site:



- ♦ A smaller but full data center, with redundant UPSs', HVAC's, ISP's, generators,...
- ♦ No hardware or backups are at the cold site, they require systems to be acquired, configured and applications loaded and configured.
- ♦ This is by far the cheapest, but also longest recovery option, can be weeks+.

### ▪ Reciprocal Agreement Site:

- ♦ Your organization has a contract with another organization that they will give you space in their data center in a disaster event and vice versa.
- ♦ This can be promised space or some racks with hardware completely segmented off the network there.

### ▪ Mobile Site:

- ♦ Basically a data center on wheels, often a container or trailer that can be moved wherever by a truck.
- ♦ Has HVAC, fire suppression, physical security, (generator),... everything you need in a full data center.
- ♦ Some are independent with generator and satellite internet, others need power and internet hookups.

### ▪ Subscription/Cloud Site:

- ♦ We pay someone else to have a minimal or full replica of our production environment up and running within a certain number of hours (SLA).
- ♦ They have fully built systems with our applications and receive backups of our data, if we are completely down we contact them and they spin the systems up and apply the latest backups.
- ♦ How fast and how much is determined by our plans and how much we want to pay for this type of insurance.

Site	Cost	Hardware/Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

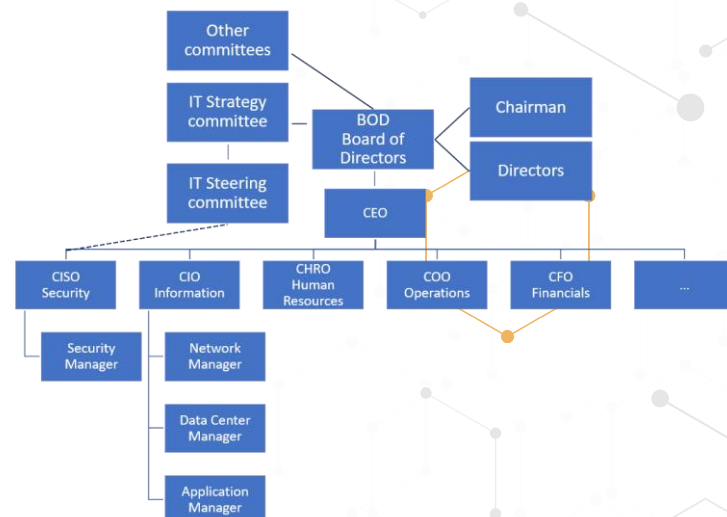


### ► Other BCP Plans:

#### • Related Plans:



- Our BCP being the overarching plan also contains our other plans, including but not limited to:
- **COOP (Continuity of Operations Plan):**
  - ♦ How we keep operating in a disaster, how do we get staff to alternate sites, what are all the operational things we need to ensure we function even if at reduced capacity for up to 30 days.
- **Cyber Incident Response Plan:**
  - ♦ How we respond in cyber events, can be part of the DRP or not. This could be DDOS, worms, viruses,...
- **OEP (Occupant Emergency Plan):**
  - ♦ How do we protect our facilities, our staff and the environment in a disaster event.
  - ♦ This could be fires, hurricanes, floods, criminal attacks, terrorism,...
  - ♦ Focuses on safety and evacuation, details how we evacuate, how often we do the drills and the training staff should get.
- **BRP (Business Recovery Plan):**
  - ♦ Lists the steps we need to take to restore normal business operations after recovering from a disruptive event.
  - ♦ This could be switching operations from an alternate site back to a (repaired) primary site.
- **Continuity of Support Plan:**
  - ♦ Focuses narrowly on support of specific IT systems and applications.
  - ♦ Also called the IT Contingency Plan, emphasizing IT over general business support.
- **CMP (The Crisis Management Plan):**
  - ♦ Gives us effective coordination among the management of the organization in the event of an emergency or disruptive event.
  - ♦ Details what steps management must take to ensure that life and safety of personnel and property are immediately protected in case of a disaster.
- **Crisis Communications Plan:**
  - ♦ A subplan of the CMP.
  - ♦ How we communicate internally and externally during a disaster.
  - ♦ Who is permitted to talk to the press? Who is allowed to communicate what to whom internally?






- **Call Trees:**
  - ♦ Each user in the tree calls a small number of people.
  - ♦ The calling tree is detailed in the communications plan and should be printed out and at the home of staff, assume we have no network or system access.
  - ♦ Starts from the bottom up and then top down.
  - ♦ The staff that discovers the incident calls their manager or director, they then contact someone at a senior level (often the CEO).
  - ♦ The CEO calls the rest of the C-level leadership, they call their directors and managers and the managers call their staff.
  - ♦ Obviously only where it is appropriate and needed for the recovery effort or if staff is directly impacted by the disaster.
  - ♦ Should be done with 2 way confirmation, managers/directors should confirm to their C-level executive that they did get a hold of the identified staff.
  - ♦ Automated call trees are often a better idea than manual ones, notifying people of the disaster is one of those things that tends to get forgotten.
  - ♦ They are hosted at a remote location, often on SaaS, and key personnel that are allowed to declare a disaster can activate them.
- **Off Site Copies and Plans:**
  - We keep both digital and physical copies of all our plans at offsite locations, assume we can't access our data or our facilities. Relying on memory is a bad idea.
  - We also keep critical business records in the same manner.
- **EOC (Emergency Operations Center):**
  - A central temporary command and control facility responsible for our emergency management, or disaster management functions at a strategic level during an emergency.
  - It ensures the continuity of operation of our organization.
  - We place the EOC in a secure location if the disaster is impacting a larger area.
- **MOU/MOA (Memorandum of Understanding/Agreement):**
  - Staff signs a legal document acknowledging they are responsible for a certain activity.
  - If the test asks "A critical staff member didn't show, and they were supposed to be there. What could have fixed that problem?" it would be the MOU/MOA. While slightly different they are used interchangeably on the test.
- **Executive Succession Planning:**
  - Senior leadership often are the only ones who can declare a disaster.
  - We need to plan for if they are not available to do so.
  - Their unavailability may be from the disaster or they may just be somewhere without phone coverage.
  - Organizations must ensure that there is always an executive available to make decisions





- Our plans should clearly outline who should declare a disaster, if they are not available, who is next in line and the list should be relatively long.
- Organizations often have the entire executive team at remote sessions or conferences (it is not very smart).
- **Employee Redundancy:**
  - We should have a high degree of skilled employee redundancy, just like we have on our critical hardware.
  - It is natural for key employees to move on, find a new job, retire or win the lottery.
  - If we do not prepare for it we can cripple our organization.
  - Can be mitigated with training and job rotation.

### ▶ Testing the Plans:

- We have built our plans, now we need to see how complete and accurate they are, they are living documents we continually improve them.
- **Simulated Tests:** 
  - **DRP Review:**
    - ♦ Team members who are part of the DRP team review the plan quickly looking for glaring omissions, gaps or missing sections in the plan.
  - **Read-Through (Checklist):**
    - ♦ Managers and functional areas go through the plan and check a list of components needed for in the recovery process.
  - **Walk/Talk-through (Tabletop or Structured Walkthrough):**
    - ♦ A group of managers and critical personnel sit down and talk through the recovery process.
    - ♦ Can often expose gaps, omissions or just technical inaccuracies that would prevent the recovery.
  - **Simulation Test (Walkthrough Drill):**
    - ♦ Similar to the walkthrough (but different, do not confuse them).
    - ♦ The team simulates a disaster and the teams respond with their pieces from the DRP.
- **Physical Tests:**
  - **Parallel Processing:**
    - ♦ We bring critical components up at a secondary site using backups, while the same systems are up at the primary site, after the last daily backup is loaded we compare the two systems.
  - **Partial Interruption:**
    - ♦ We interrupt a single application and fail it over to our secondary facilities, often done off hours.
  - **Full Interruption:**
    - ♦ We interrupt all applications and fail it over to our secondary facilities, always done off hours.
  - Both partial and full are mostly done by fully redundant organizations, build your plans for your environment.



- **Testing:**
  - To ensure the plan is accurate, complete and effective, happens before we implement the plan.
- **Drills (Exercises):**
  - Walkthroughs of the plan, main focus is to train staff, and improve employee response (think fire drills).
- **Auditing:**
  - A 3<sup>rd</sup> party ensures that the plan is being followed, understood and the measures in the plan are effective.

### ▶ Training for the Plans:

- For most of our plans we need to provide training for our staff on how they react and handle their piece of the plan.
  - We train evacuations, fire safety, CPR, first aid, and for the DRP the teams with responsibilities needs to feel comfortable performing their tasks.
  - If an employee is expected to restore a system from tape and they have never done it is time to train them.
    - ♦ Do they know how to get the restore tapes (they are of course not kept on premises).
  - Does the UPS fail over automatically or does someone have to flip the switch, does every data center employee know how to do that?
  - It is each functional unit's responsibility they are ready for a disaster, they need to provide the training (they are taught it), in the end what we need is awareness (they actively use it).
  - This is also where we would do as much as possible for the people redundancy.
    - ♦ New staff is trained on our systems as well as the emergency protocols and how to perform their tasks.
    - ♦ If we only have one server administrator we better hope he is not on vacation when our incident happens.

### ▶ Improving the Plans:

- The plans needs to be continually updated, it is an iterative process.
  - Plans should be reviewed and updated at least every 12 months.
  - If our organization has had a major change we also update the plans.
    - ♦ This could be:
      - We acquired another company or we split off into several companies.
      - We changed major components of our systems (new backup solution, new IP scheme,...).
      - We had a disaster and we had a lot of gaps in our plans.
      - A significant part of senior leadership has changed.
  - When we update the plans older copies are retrieved and destroyed, and current versions are distributed.





### ► After a Disruption or Test:

- Once we have had and recovered from a disruption or we have done our failover test we do a lessons learned.
- **Lessons Learned:**
  - This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
  - We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.
  - What happened and didn't happen is less important than how we improve for next time.
  - We do not place blame, the purpose is improving.
  - How can we as an organization grow and become better next time we have another incidence? While we may have fixed this one vulnerability there are potentially 100's of new ones we know nothing about yet.
  - The outcome and changes of the Lessons Learned will then feed into our preparation and improvement of our BCP and DRP.



### ► After a Disruption:

- We only use our BCP/DRP's when our other countermeasures have failed.
- This makes the plans even more important. (Remember 2/3 of business with major data loss close).
- When we make and maintain the plans there are some common pitfalls we want to avoid:
  - Lack of senior leadership support
  - Lack of involvement from the business units
  - Lack of critical staff prioritization
  - Too narrow scope
  - Inadequate telecommunications and supply chain management
  - Lack of testing
  - Lack of training and awareness
  - Not keeping the BCP/DRP plans up to date, or no proper versioning controls

### ► BCP/DRP Frameworks:

- When building or updating our BCP/DRP plans, we can get a lot of guidance from these frameworks, and just like the other standards and frameworks we use we often tailor and tweak them to fit the needs of our organization.
- **NIST 800-34:** 
  - Provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption.
- **ISO 22301:** 
  - Societal security, Business continuity management systems, specifies a management system to manage an organization's business continuity plans, supported by ISO 27031.



- **ISO/IEC-27031:** 
  - Societal security, Business continuity management systems – Guidance, which provides more pragmatic advice concerning business continuity management
- **BCI (Business Continuity Institute):** 
  - 6 step process of "Good Practice Guidelines (GPG)" the independent body of knowledge for Business Continuity.

► **What we covered in the Seventh CBK Domain:**

- How we through **Administrative Personnel Security** can mitigate some inside threats.
- Who is allowed to do **Digital Forensics** and how we do it right.
- Events, Alerts, Incidents and Problems. What we react to and how we react.
- Incident management and responses.
- SIEM's, IDS's and IPS's: both host and network based ones and what each of them can and can't do.
- Configuration management, patch management, change management.
- Oday vulnerabilities and how our only defense is defense in depth and at times abnormality detection.
- Fault tolerance, backups, RAID, e-vaulting, remote journaling, database shadowing, hardware and system redundancy.
- BCP and DRP's:
  - What we need to consider and how we prioritize our systems and facilities for the plans.
  - How we build, test, train and maintain the plans.
  - How we react in a disaster scenario and recover from it.