Thor's Study Guide - CISM® Domain 4

Contents

Thor's Study Guide - CISM® Domain 4

Thor's Study Guide – CISM® Domain 4

Introduction to Domain 4: Incident Management

- In Domain 4, we look at how we prepare, mitigate, and react when we have an incident.
- 30% of the exam questions on the certification are from this domain.

- We talk about incidences management; how we plan, test, and prepare for incidences and disasters.
- The plans we make; our BCP, DRP and many other BCP sub plans (COOP, OEP, CIRP, …).
- How we build those plans from our BIA (Business Impact Analysis).
- We look at supply, personnel, and infrastructure redundancy.
- The different types of disaster Recovery sites.
- What we do after a disruption.
- Forensics: Digital, spinning disk, network, and software forensics.
- Data remanence and destruction.
- Then we finish Domain 4 by looking at malware, programming concepts, and personnel security.

- This should be what you are tested on for Domain 4 until the next planned CISM curriculum change in 2027.

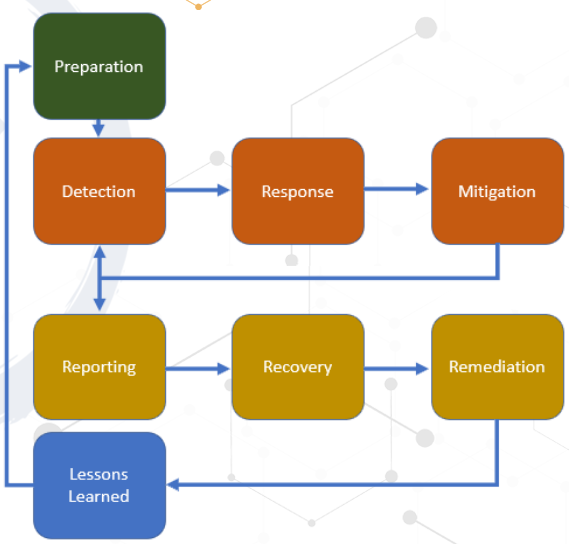
Administrative Security

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 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 an 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, Postmortem, 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.

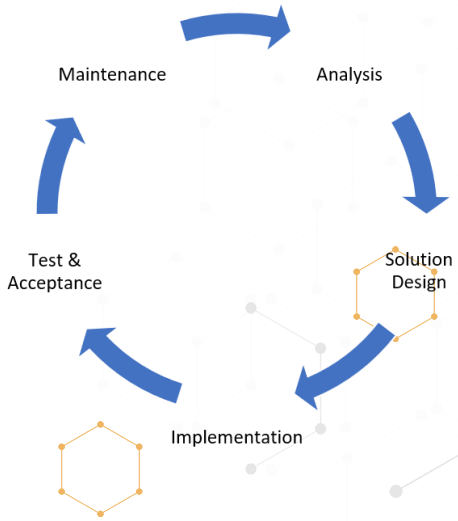
- **Lessons Learned:**
  - This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
  - We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.
  - How can we as an organization 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 affected, 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.

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.



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.

- **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.

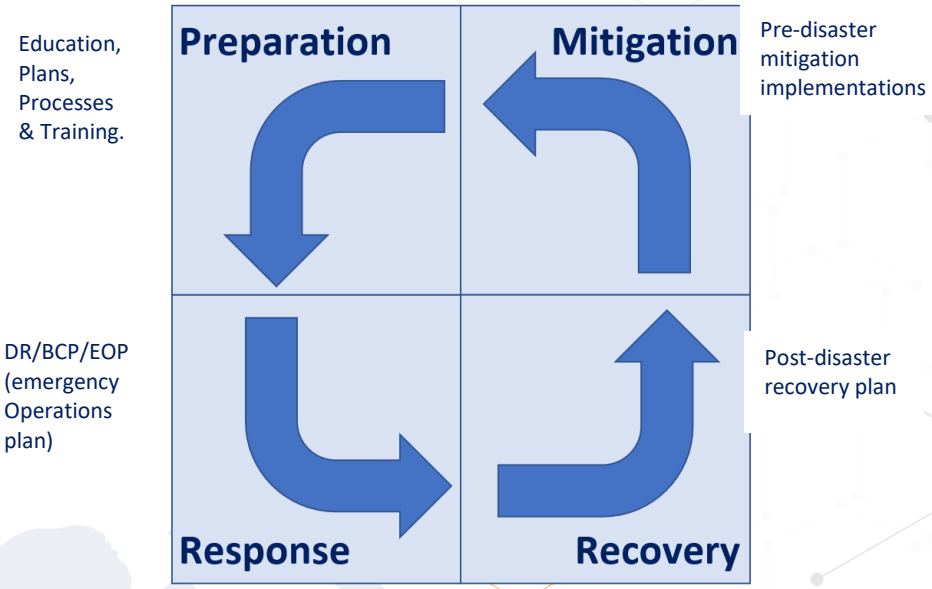
Personnel

- **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.

DRP (Disaster Recovery Plan) Basics

- 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 likeliness 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.

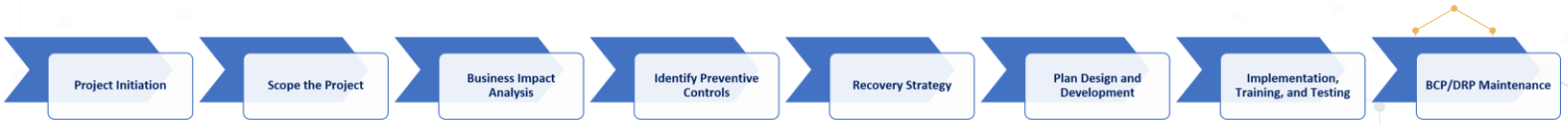


- We have looked at the first 2 before, for now we will focus on Response and Recovery.
  - **Response**: How we react in a disaster, following the procedures.
    - How we respond and how quickly we respond is essential in Disaster Recovery.
    - We assess if the incident we were alerted to or discovered 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.

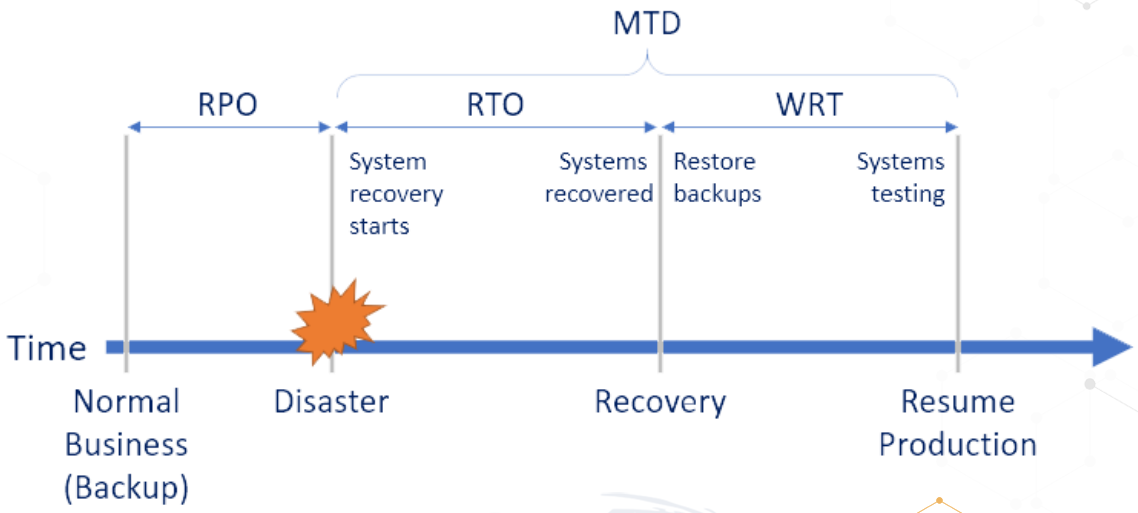


- Senior management needs to be involved and committed to the BCP/DRP process; without that it is just lip service.
  - They need to be part of at least the initiation and the final approval of the plans.
  - They are responsible for the plan, they own the plan and since they are ultimately liable, they 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 cannot 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 ≥ 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 have minimum system requirements for DR sites.



Supply and Infrastructure Redundancy

- 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 supplier's 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.

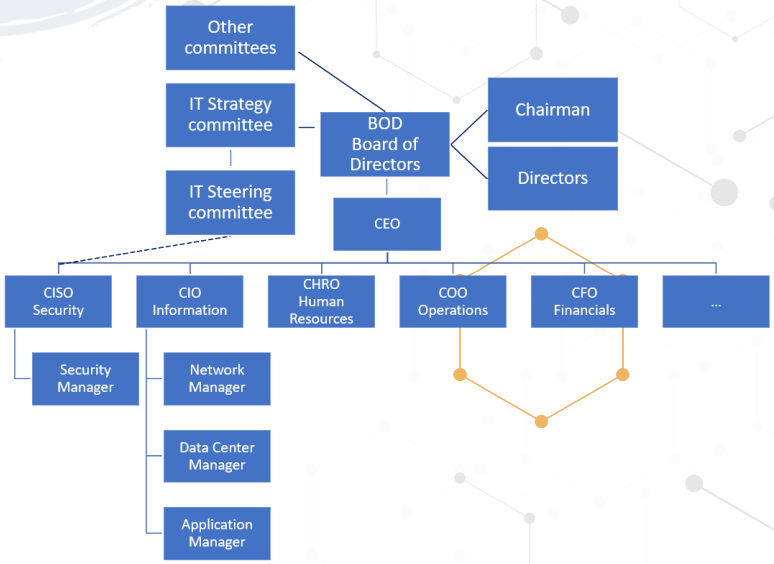
- Still often a smaller but a full data center, with redundant UPS's, HVAC's, ISP's, generators, …
- We may have to manually fail traffic over, but a full switch can take an hour or less.
- Near or real-time copies of data.

- **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 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.

- **Offsite 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, Training, and Improving 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 3rd party ensures that the plan is being followed, understood and the measures in the plan are effective.
- 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.

- The plans need 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

- 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 Lessons Learned will then feed into our preparation and improvement of our BCP and DRP.
- We only use our BCP/DRP's when our other countermeasures have failed.
- This makes the plans even more important. (Remember 72% of business with major data loss closed).
- 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.

Digital Forensics

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.
- **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.
- 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 incidence 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 and mp3 players.
- 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.

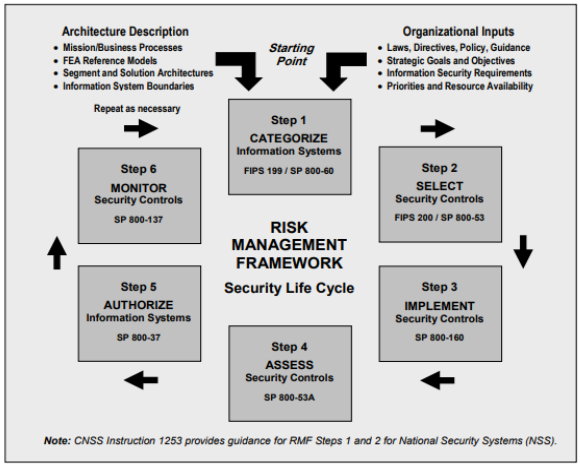


FIGURE 2: RISK MANAGEMENT FRAMEWORK

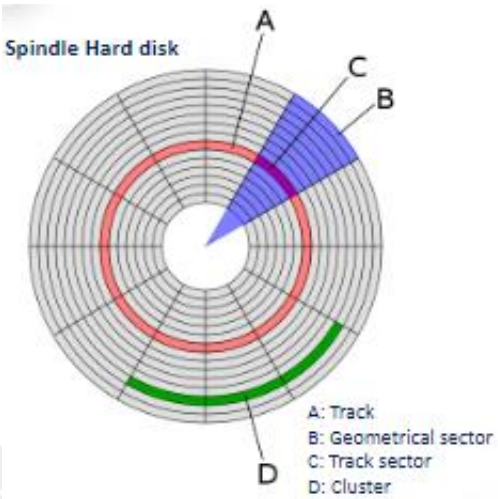
From NIST 800-53

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

https://thorteaches.com/study/

Spinning Disk 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).



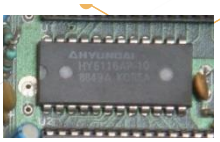
  - **Slack Space:**
    - Data is stored in specific size chunks known as clusters (clusters = sectors or blocks).
    - A cluster is the minimum size that can be allocated by a file system.
    - If a particular file, or final portion of a file, does not require the use of the entire cluster then some 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.

Memory and Data Remanence

- **Data Remanence:** Data left over after normal removal and deletion of data.
- **Memory:** Is just 0's (off) and 1's (on); switches representing bits.
  - **ROM:**
    - **ROM (Read Only Memory)** is nonvolatile (retains memory after power loss); most common use is the BIOS.
      - **PROM (Programmable read only memory)** – Can only be written once, normally at the factory.

- **EPROM (Erasable programmable read only memory)** – Can be erased (flashed) and written many times, by shining an ultraviolet light (flash) on a small window on the chip (normally covered by foil).
- **EEPROM (Electrically erasable programmable read only memory)** – These are electrically erasable; you can use a flashing program. This is still called read only.
- The ability to write to the BIOS makes it vulnerable to attackers.
  - **PLD (Programmable logic devices)** are programmable after they leave the factory (EPROM, EEPROM and flash memory). Not PROM.
    - **Cache Memory:** L1 cache is on the CPU (fastest), L2 cache is connected to the CPU, but is outside it.
    - **RAM (Random Access Memory)** is volatile memory. It loses the memory content after a power loss (or within a few minutes). This can be memory sticks or embedded memory.
      - **SRAM and DRAM:**
        - **SRAM (Static RAM):** Fast and expensive. Uses latches to store bits (Flip-Flops).
          - Does not need refreshing to keep data, keeps data until power is lost. This can be embedded on the CPU.
        - **DRAM (Dynamic RAM)** Slower and cheaper. Uses small capacitors.
          - Must be refreshed to keep data integrity (100-1000ms).
          - This can be embedded on graphics cards.
          - **SDRAM: (Synchronous DRAM):**
            - What we normally put in the motherboard slots for the memory sticks.
            - DDR (Double Data Rate) 1, 2, 3, 4 SDRAM.

SRAM



SD RAM

Firmware and SSD's (Solid State Drives)

- **Firmware:**
  - This is the BIOS on a computer, router or switch, the low-level operating system and configuration.
  - The firmware is stored on an embedded device.
  - PROM, EPROM, EEPROM are common firmware chips.
- **Flash memory:**
  - Small portable drives (USB sticks are an example); they are a type of EEPROM.
- **SSD drives** are a combination of EEPROM and DRAM, can't be degaussed.
  - To ensure no data is readable we must use must ATA Secure Erase or/and destruction of SSD drives.

Data Remanence and Destruction

When we no longer need a certain media, we must dispose of it in a manner that ensures the data cannot be retrieved. This pertains to both electronic media and paper copies of data.

- **Paper disposal** – It is highly encouraged to dispose of ANY paper with any data on it in a secure manner. This also has standards and cross shredding is recommended. It is easy to scan and have a program re-assemble documents from normal shreds like this one.
- **Digital disposal** – The digital disposal procedures are determined by the type of media.
    - **Deleting, formatting, and overwriting (Soft destruction):**
        - **Deleting** a file just removes it from the table; everything is still recoverable.
        - **Formatting** does the same, but it also puts a new file structure over the old one. Still recoverable in most cases.
        - **Overwriting** (Clear) is done by writing 0s or random characters over the data.
        - **Sanitization** is a process of rendering target data on the media infeasible for a given level of recovery effort.
        - **Purge** is removing sensitive data from a system or device to a point where data recovery is no longer feasible even in a laboratory environment.
        - **Degaussing** destroys magnetic media by exposing it to a very strong magnetic field. This will also most likely destroy the media integrity.
    - **Full physical destruction is safer than soft destruction:**
        - **Disk crushers** do exactly what their name implies: they crush disks (often used on spinning disks).
        - **Shredders** do the same thing as paper shredders do; they just work on metal. These are rare to have at normal organizations, but you can buy the service.
        - **Incineration, pulverizing, melting, and acid** are also (very rarely) used to ensure full data destruction.

It is common to do multiple types of data destruction on sensitive data (both degaussing and disk crushing/shredding).

Network and Software 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 pro-active 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, 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 are a new player.
    - They include SSDs, GPSs, 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.

0-day Attacks

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.

Warfare, Terrorism, Sabotage, and Ransomware

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.

Programming Concepts

- **Machine Code:**
  - Software executed directly by the CPU, 0's and 1's understood by the CPU.
- **Source Code:**
  - Computer programming language, written in text and is human understandable, translated into machine code.
- **Assembler Languages:**
  - Short mnemonics like ADD/SUB/JMP, which are matched with the full-length binary machine code; assemblers convert assembly language into machine language. A disassembler does the reverse.
- **Compiler Languages:**
  - Translates the higher-level language into machine code and saves, often as executables, compiled once and run multiple times.
- **Interpreted Languages:**
  - Similar to compiler languages but interprets the code each time it is run into machine code.
- **Bytecode:**
  - An interpreted code, in intermediary form, converted from source code to interpreted, but still needs to be converted into machine code before it can run on the CPU.
- **Procedural Languages (Procedure-oriented):**
  - Uses subroutines, procedures, and functions.
- **Object-oriented Programming (OOP):**
  - Based on the concept of objects, which may contain data, in the form of fields, often known as attributes, and code, in the form of procedures, often known as methods.
  - An object's procedures can access and often modify the data fields of the objects with which they are associated.
  - In OOP, computer programs are designed by making them out of objects that interact with one another.
- **4th Generation languages (4GL):**
  - Fourth-generation languages are designed to reduce programming effort and the time it takes to develop software, resulting in a reduction in the cost of software development.
  - Increases the efficiency by automating the creation of machine code.
  - Often uses a GUI, drag, and drop, and then generating the code, often used for websites, databases, and reports.
- **Programming Languages and Generations:**
  - **1st generation:** Machine Code
  - **2nd Generation:** Assembler languages
  - **3rd Generation:** C, C++, Java, Python, PHP, Perl, C#, BASIC, Pascal, Fortran, ALGOL, COBOL,
  - **4th Generation:** ABAP, Unix Shell, SQL, PL/SQL, Oracle Reports, R, …
  - **5th Generation:** Prolog, OPS5, Mercury, …
- **CASE (Computer-Aided Software Engineering):**
  - Similar to and were partly inspired by computer-aided design (CAD) tools used for designing hardware products.
  - Used for developing high-quality, defect-free, and maintainable software.

- Often associated with methods for the development of information systems together with automated tools that can be used in the software development process.
- **CASE software** is classified into 3 categories:
  - **Tools** support specific tasks in the software life cycle.
  - **Workbenches** combine two or more tools focused on a specific part of the software life cycle.
  - **Environments** combine two or more tools or workbenches and support the complete software life cycle.

- **Top-Down Programming:**
  - Starts with the big picture, then breaks it down into smaller segments.
  - An overview of the system is formulated, specifying, but not detailing, any first-level subsystems.
  - Each subsystem is then refined in yet greater detail, sometimes in many additional subsystem levels, until the entire specification is reduced to base elements.
  - Procedural programming leans toward Top-Down, you start with one function and add to it.
- **Bottom-Up Programming:**
  - Piecing together of systems to build more complex systems, making the original systems a sub-system of the overarching system.
  - The individual base elements of the system are first specified in great detail, they are then linked together to form larger subsystems, which then in turn are linked, sometimes in many levels, until a complete top-level system is formed.
  - OOP leans tends toward Bottom-Up, you start by developing your objects and build up.
- **Software Release:**
  - **Open source:**
    - We release the code publicly, where it can be tested, improved, and corrected, but it also allows attackers to find the flaws in the code.
  - **Closed Source:**
    - We release the software, but keep the source code a secret, may be sound business practice, but can also be security through obscurity.
  - **Proprietary Software:**
    - Software protected by intellectual property and/or patents, often used interchangeably with Closed Source software, but it really is not. It can be both Open and Closed Source software.
    - Any software not released into the public domain is protected by copyright.
  - **Free Software:**
    - **Freeware:**
      - Actually, free software, it is free of charge to use.
    - **Shareware:**
      - Fully functional proprietary software that is initially free to use.
      - Often for trials to test the software, after 30 days you have to pay to continue to use.
    - **Crippleware:**
      - Partially functioning proprietary software, often with key features disabled.

        - The user is required to make a payment to unlock the full functionality.
    - **EULAs (End-User License Agreements):**
        - Electronic form where the user clicks "I agree" to the software terms and conditions while installing the software.

- **Software Licenses:**
    - Open-source software can be protected by a variety of licensing agreement.
        - **GNU (General Public License) also called GPL:**
            - Guarantees end users the freedom to run, study, share and modify the software.
            - A copyleft license, which means that derivative work can only be distributed under the same license terms.
        - **BSD (Berkeley Software Distribution):**
            - A family of permissive free software licenses, imposing minimal restrictions on the use and redistribution of covered software.
            - This is different than copyleft licenses, which have reciprocity share-alike requirements.
        - **Apache:**
            - Software must be free, distribute, modify, and distribute the modified software.
            - Requires preservation of the copyright notice and disclaimer.

Database Security

- **Polyinstantiation** (Alternative Facts) – Two (or more) instances of the same file depending on who accesses it.
    - The real information may be available to subjects with Top Secret clearance, but different information will be available to staff with Secret or lower clearance.
- **Aggregation** is a collection or gathering of data together for the purpose of statistical analysis. (You see the bigger picture rather than the individual pieces of data).
- **Inference** requires deducing from evidence and reasoning rather than from explicit statements.
- **Data mining** is the computing process of discovering patterns in large data sets.
    - It uses methods combining machine learning, statistics, and database systems.
- **Data Analytics** is looking at what normal operations look like, then allowing us to identify abuse more proactively from insider threats or compromised accounts.

We mitigate the attacks with **Defense in Depth** (again) – We secure the building, the entrances, the doors, the network, the servers, the OS, the DB, screen the employees, … We have solid policies, procedures, standards, and guidelines.

Malware

Malware

- **Malware (Malicious Code)** - This is the catch-all name for any malicious software used to compromise systems or data.
    - **Viruses** - require some sort of human interaction and are often transmitted by USB sticks or other portable devices.
    - When the program is executed, it replicates itself by inserting its own code into other programs.
        - **Macro** (document) Viruses: Written in Macro Languages, embedded in other documents (Word, Outlook).
        - **Boot Sector** Viruses: Infect the boot sector or the Master Boot Record, ensuring they run every time the PC boots.
        - **Stealth Viruses:** Try to **hide themselves** from the OS and antivirus software.
        - **Polymorphic Viruses**: Change their signature to avoid the antivirus signature definitions.
        - **Multipart** (Multipartite) Viruses: Spread across **multiple vectors**. They are often hard to get rid of because even if you clean the file infections, the virus may still be in the boot sector and vice-versa.
- **Worms** - spread through **self-propagation** - they need no human interaction; they do both the payload damage and replicate through aggressive network use (also makes them easier to spot).
- **Trojans** - malicious code **embedded** in a program that is normal. This can be games, attachments, website clicks, etc.
- **Rootkits** - Replace some of the OS/Kernel with a malicious payload. User rootkits work on Ring 3 and Kernel rootkits on Ring 0.
- **Logic Bombs** - Malicious code that executes at a certain time or event - they are dormant until the event (IF/THEN).
    - IF Bob is not getting an annual bonus over $10,000, THEN execute malicious code.
    - IF date and time is 5/15/2022 00:02:12, THEN execute malicious code.
- **Packers** – Programs to compress *.exe files, which can be used to hide malware in an executable, neutral technology.
- **Antivirus Software** - tries to protect us against malware.
    - **Signature based** - looks for known malware signatures - MUST be updated constantly.
    - **Heuristic (Behavioral) based** - looks for abnormal behavior - can result in a lot of false positives.
- **Server (Service) Side Attacks:**
    - Attacks directly from an attacker to a target.
    - Defense in Depth can mitigate some of these.
    - The term "Server" does not mean only servers, just that the attack is directly aimed at the end target. (They come to you).
- **Client-Side Attacks:**
    - The client initiates, then gets infected with malicious content usually from web browsers or instant messaging applications. (**You go to them**).
    - Since most firewalls protect inbound mostly, client-side attacks are often more successful.

Web Architecture and Attacks

- The internet is a very complex place. Security is often added on as an afterthought and not designed in as it should be.
- On top of that the internet was never intended to be what it is today; it was originally designed to be a secure closed network.
    - **Applets:** Small applications often embedded into other software (web browsers).
        - They are executable, downloaded from a server and installed locally on the client.
        - Applets are commonly written in Java or ActiveX (control).
            - **Java** applets run in a sandbox environment - segmenting the java from the OS (limiting some threats), OS agnostic.
            - **ActiveX** runs with certificates (not sandbox) - since ActiveX is an MS product it interacts more with the OS (Windows only).

OWASP

- **OWASP (Open Web Application Security Project)** 2021 - has a Top 10 of the most common web security issues.
    - A01:2021-Broken Access Control
    - A02:2021-Cryptographic Failures
    - A03:2021-Injection
    - A04:2021-Insecure Design
    - A05:2021-Security Misconfiguration
    - A06:2021-Vulnerable and Outdated Components
    - A07:2021-Identification and Authentication Failures
    - A08:2021-Software and Data Integrity Failures
    - A09:2021-Security Logging and Monitoring Failures
    - A10:2021-Server-Side Request Forgery

- **XML (Extensible Markup Language**) is a markup language designed as a standard way to encode documents and data.
    - It is similar to HTML, but more universal.
    - It is mainly used for Web but does not have to be, it can be used to store application configuration, output from auditing tools, and many other things.
- **SOA (Service-Oriented Architecture)** is a style of software design where services are provided to the other components by application components, through a communication protocol over a network.
    - The basic principles of service-oriented architecture are independent of vendors, products, and technologies.
    - SOA is intended to allow multiple different applications to be consumers of services.

Personnel Safety

Personnel Safety is **always** most important

- You may like your servers more but save the co-worker first. (This is very testable).
- Organizations should have clear policies, procedures, and standards for evacuations.
- Evacuation routes should be clearly marked and known by all staff.
- Meeting points should be established (can also stop staff from reentering the building looking for a coworker who is already somewhere else outside).
- Evacuation roles are established; a pre-appointed person ensures all staff is out of the building and another is the meeting point leader.
- Plans are in place for disabled employees (elevators are not working at this time).
- Fire/evacuation drills are held quarterly or annually.
- All exit doors (or special emergency-only doors) have the "panic bar" (crash bar).
- Just like in the data center, we have warning sirens and lights throughout the building to alert staff to exit.

- **Early Warning Systems** (Duress Warning Systems):
  - Warning systems are used to provide immediate alerts to personnel/people in the event of emergencies, severe weather, threat of violence, chemical contamination, ...
  - Duress systems are mostly local and can use overhead speakers, sirens or automated communications like email, pagers, text messages or automated phone calls.

What we covered in Domain 4

Congratulations on finishing Domain 4: Incident Management.

30% of the exam questions on the certification are from this domain.

- In Domain 4 we talked about incidences management; how we plan, test, and prepare for incidences and disasters.
- The plans we make; our BCP, DRP and many other BCP sub plans (COOP, OEP, CIRP, …).
- How we build those plans from our BIA (Business Impact Analysis).
- We looked at supply, personnel and infrastructure redundancy.
- The different types of disaster Recovery sites.
- What we do after a disruption.
- Forensics: Digital, spinning disk, network and software forensics.
- Data remanence and destruction.
- Then we finished Domain 4 by looking at malware, programming concepts, and personnel security.

- This should be what you are tested on for Domain 4 until the next planned CISM curriculum change in 2027.