CISM®

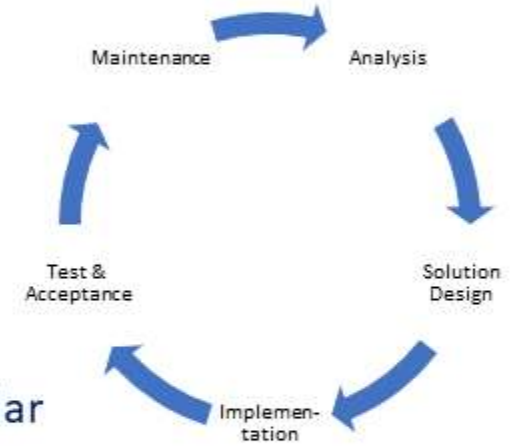
DOMAIN 4

Welcome to the fourth CISM Domain.

- 19% of the exam questions on the certification are from this domain.
- How we plan for incidences and disasters.
- Business Continuity Planning and Disaster Recovery Planning.
- BIA (Business Impact Analysis).
- Supply, personnel and infrastructure redundancy.
- Disaster Recovery sites.
- Other BCP sub plans:
  - COOP (Continuity of Operations Plan), Cyber Incident Response Plan, OEP (Occupant Emergency Plan).
- After a disruption.
- Digital, spinning disk, network and software forensics.
- Memory and data remanence.
- Data remanence and destruction.

- **Domain 4 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.

- **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.



- **BCP and DRP:**
  - **BCP** (Business Continuity Plan):
    - We look at what we would 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.

- **BCP and DRP:**
  - **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, ...

- **BCP and DRP:**
  - **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.

- **BCP and DRP:**
  - **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).

- **BCP and DRP:**
  - **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% 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 name, and have it on hand for potential epidemics.
      - When the H1N1 flu was declared a pandemic the ISP I worked for at the time, had identified critical staff and they were offered some of the very limited vaccines for the H1N1.
    - **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?

- **BCP and DRP:**
  - 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.

- **BCP and DRP:**
  - 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.

Education, Plans, Processes & Training.

Pre-disaster mitigation implementations.

DR/BCP/EOP (emergency Operations plan)

Post-disaster recovery plan.

- **BCP and DRP:**
  - 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.

- **Developing 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.

- **Developing our BCP and DRP:**
  - 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.

- **Developing our BCP and DRP:**
  - **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.

- **Developing our BCP and DRP:**
  - **BIA** (continued):
    - **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.

- **Developing our BCP and DRP:**
  - **BIA** (continued): 
    - **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.

- **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.

- **Recovery Strategies:**
  - **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 vise versa.
    - This can be promised space or some racks with hardware completely segmented off the network there.

- **Recovery Strategies:**
  - **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.

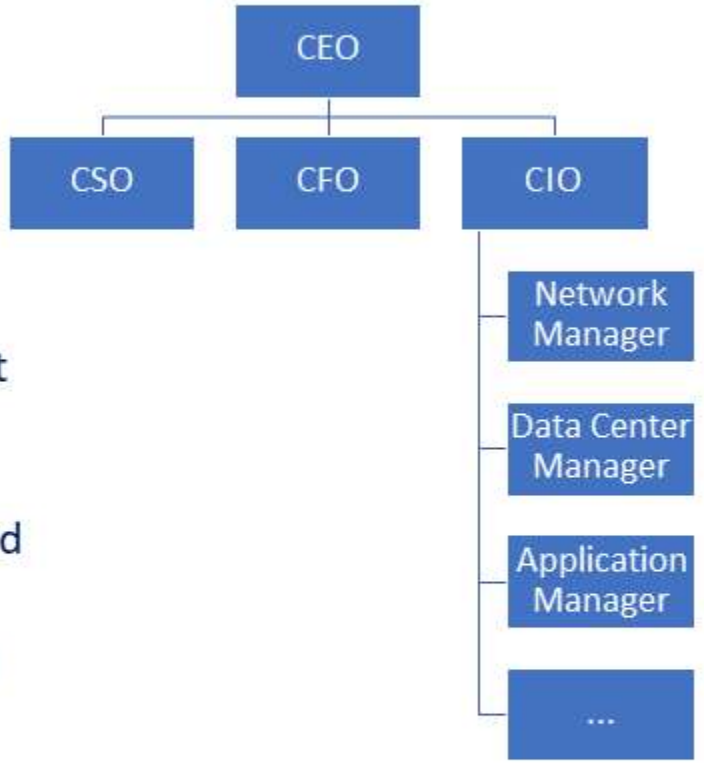
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

- **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.

- **Other BCP plans:**
  - **Related plans:**
    - **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.

- **Other BCP plans:**
  - **Related plans:**
    - **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).

- **Other BCP plans:**
  - **Related plans:**
    - **Call Trees:**
      - 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.



- **Other BCP plans:**
  - **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.

- **Other BCP plans:**
  - **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.

- **Testing the plans:**
  - **Simulated tests:** 
    - **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:**
    - **Parparallel 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 the plans:**
  - **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.

- **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.

- **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.

- **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.

- **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 Tableau write-blocker attached to a hard disk.

- **Administrative Security:**
  - **Digital (computer) forensics:**
    - **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.

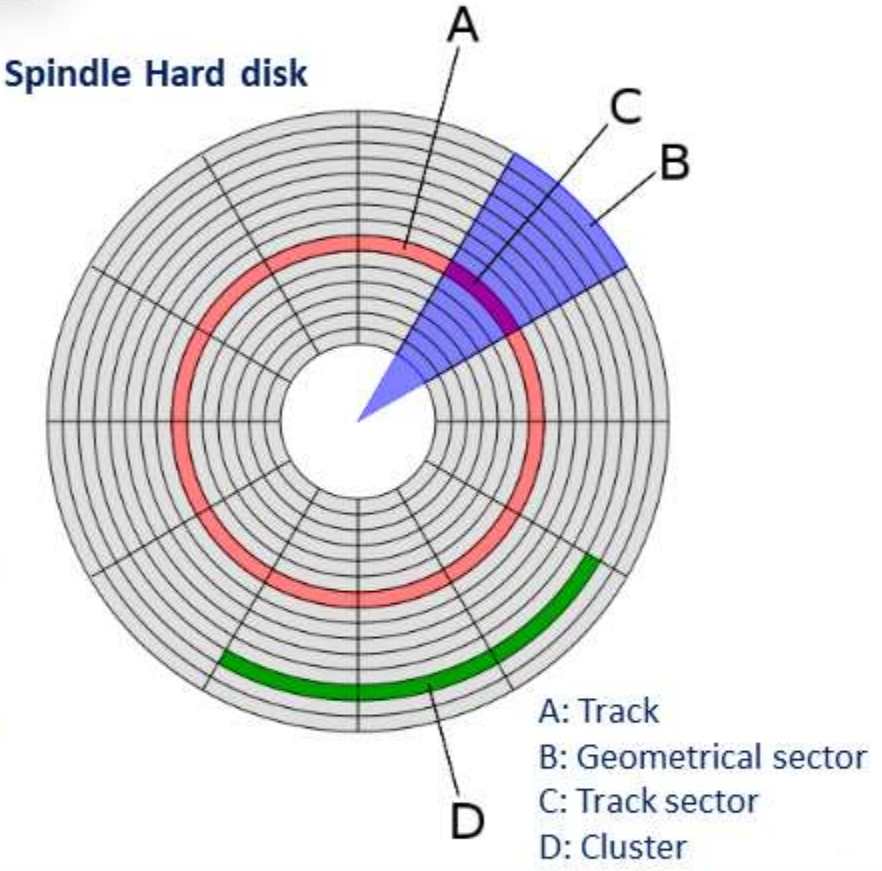
Cell phone in an evidence bag

- **Administrative Security:**
  - **Digital forensics:**
    - 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.

- **Administrative Security:**
  - **Digital forensics:**
    - 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.

- **Administrative Security:**
  - **Digital forensics:**
    - 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?

- **Administrative Security:**
  - **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).



- **Administrative Security:**
  - **Digital forensics:**
    - **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.

Memory and Data Remanence:

SRAM

- **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.

SDRAM

Memory and Data Remanence:

- **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 Destruction:

When we no longer need a certain media, we must dispose of it in a manner that ensures the data can't 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 the 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** is done by writing 0's or random characters over the data.
      - As far as we know there is no tool available that can recover even single pass overwriting (not possible on damaged media).

Data Destruction:

- **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).
- While it may not be necessary, it is a lot cheaper than a potential $1,000,000 fine or loss of proprietary technology or state secrets.

Crushed/shredded hard disk fragments.

- **Administrative Security:**
  - **Digital forensics:**
    - **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 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, 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.

- **Administrative Security:**
  - **Digital forensics:**
    - **Network forensics:**
      - 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.

- **Administrative Security:**
  - **Digital forensics:**
    - **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.

- **Administrative Security:**
  - **Digital forensics:**
    - **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', 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.

What we covered in Domain 4

- How we plan for incidences and disasters.
- Business Continuity Planning and Disaster Recovery Planning.
- BIA (Business Impact Analysis).
- Supply, personnel and infrastructure redundancy.
- Disaster Recovery sites.
- Other BCP sub plans:
  - COOP (Continuity of Operations Plan), Cyber Incident Response Plan, OEP (Occupant Emergency Plan).
- After a disruption.
- Digital, spinning disk, network and software forensics.
- Memory and data remanence.
- Data remanence and destruction.

- Thank you for staying here with me!