Thor's Study Guide - CISSP® Domain 1

Contents

Thor's Study Guide – CISSP® Domain 1

Introduction to Domain 1

In this domain we cover:

- **Confidentiality, Integrity, and Availability concepts.**
  We want the right balance; our data needs to be secure, while keeping its integrity intact and availability high.
- **Security Governance Principles.**
  What and how we grant data access to people, the frameworks we use for it, and defense in depth.
- **Legal and Regulatory Issues.**
  The laws and regulations we must adhere to, types of evidence, how we handle it, intellectual property
- **Professional Ethics**
  The ISC2 Code of Ethics and corporate code of ethics.
- **Security Policies, Standards, Procedures and Guidelines**
  How we use policies, standards, guidelines, procedures, baselines what each does.
- **Risk Identification, Assessment, Response, Monitoring and Reporting**
  How we determine the quantitative and qualitative risks to our assets and types of attackers.
- **BCP and BIA**
  The considerations for our BCP (Business Continuity Plan) and our BIA (Business impact analysis).

This domain is highly weighted on the exam (15%) and is the foundation of everything. Every other knowledge domain builds on top of this chapter.

Confidentiality, Integrity and Availability

- **The CIA Triad (*sometimes referred to as AIC*)**
  - **Confidentiality**
    - This is what most people think IT Security is.
    - We keep our data and secrets secret.
    - We ensure no one unauthorized can access the data.
  - **Integrity**
    - How we protect against modifications of the data and the systems.
    - We ensure the data has not been altered.
  - **Availability**
    - We ensure authorized people can access the data they need, when they need to.

- **Confidentiality**, Integrity and Availability.
  - **We use:**
    - Encryption for **data at rest** (for instance AES256), full disk encryption.
    - Secure transport protocols for **data in motion**. (SSL, TLS or IPSEC).
    - Best practices for **data in use** - clean desk, no shoulder surfing, screen view angle protector, PC locking (automatic and when leaving).
    - Strong passwords, multi-factor authentication, masking, access control, need-to-know, least privilege.
  - **Threats:**
    - Attacks on your encryption (cryptanalysis).
    - Social engineering.
    - Key loggers (software/hardware), cameras, Steganography.
    - IoT (Internet of Things) – The growing number of connected devices we have pose a new threat, they can be a backdoor to other systems.

- Confidentiality, **Integrity** and Availability.
  - **We use:**
    - Cryptography (again).
    - Check sums (This could be CRC).
    - Message Digests also known as a hash (This could be MD5, SHA1 or SHA2).
    - Digital Signatures – non-repudiation.
    - Access control.
  - **Threats:**
    - Alterations of our data.
    - Code injections.
    - Attacks on your encryption (cryptanalysis).

- Confidentiality, Integrity and **Availability.**
  - **We use:**
    - IPS/IDS.
    - Patch Management.
    - Redundancy on hardware power (Multiple power supplies/UPS's/generators), Disks (RAID), Traffic paths (Network design), HVAC, staff, HA (high availability) and much more.
    - SLA's – How much uptime do we want (99.9%?) – (ROI)

  - **Threats:**
    - Malicious attacks (DDOS, physical, system compromise, staff).
    - Application failures (errors in the code).
    - Component failure (Hardware).

- **Disclosure, Alteration, and Destruction**
  - The opposite of the CIA Triad is DAD.
    - **Disclosure** – Someone not authorized getting access to your information.
    - **Alteration** – Your data has been changed.
    - **Destruction** – Your data or systems have been destroyed or rendered inaccessible.

IAAA (Identification and Authentication, Authorization and Accountability)

- **Identification**
  - Your name, username, ID number, employee number, SSN etc.
  - "I am Thor".
- **Authentication**
  - "Prove you are Thor". – Should **always** be done with multi-factor authentication!
    - **Something you know - Type 1** Authentication (passwords, pass phrase, PIN, etc.).
    - **Something you have - Type 2** Authentication (ID, passport, smart card, token, cookie on PC, etc.).
    - **Something you are - Type 3** Authentication (and Biometrics) (Fingerprint, iris scan, facial geometry, etc.).
- **Authorization**
  - What are you allowed to access?
  - We use Access Control models. What and how we implement depends on the organization and what our security goals are.
  - More on this in later when we cover DAC, MAC, RBAC, ABAC, and RUBAC.

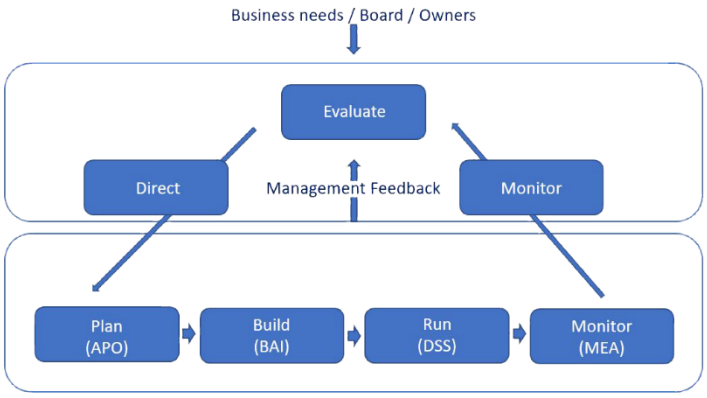
- **Accountability** (also often referred to as Auditing)
  - Trace an Action to a Subject's Identity:
    - Prove who/what a given action was performed by (non-repudiation).

Security Governance Principles

- **Least Privilege and Need to Know.**
  - **Least Privilege** – (Minimum necessary access) Give users/systems exactly the access they need, no more, no less.
  - **Need to Know** – Even if you have access, if you do not need to know, then you should not access the data.

- **Non-repudiation.**
  - A user cannot deny having performed a certain action. This uses both Authentication and Integrity.
- **Subject and Object.**
  - **Subject** – (Active) Most often users, but can also be programs – Subject manipulates Object.
  - **Object** – (Passive) Any passive data (both physical paper and data) – Object is manipulated by Subject.
  - Some can be both at different times, an active program is a subject; when closed, the data in program can be object.

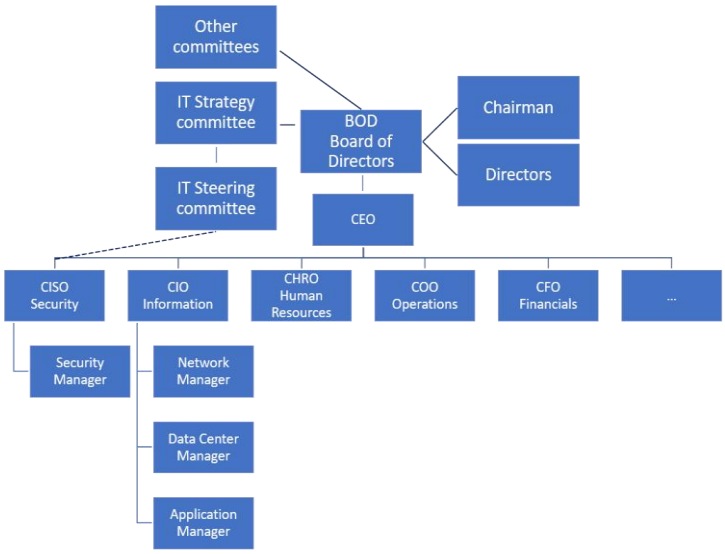
- **Governance vs. Management**
  - **Governance** – This is C-level Executives (Not you).
    - Stakeholder's needs, conditions and options are evaluated to define:
      - ☐ Balanced agreed-upon enterprise objectives to be achieved.
      - ☐ Setting direction through prioritization and decision making.
      - ☐ Monitoring performance and compliance against agreed-upon direction and objectives.
      - ☐ Risk appetite – Aggressive, neutral, adverse.



  - **Management** – How do we get to the destination (This is you).
    - Plans, builds, runs, and monitors activities in alignment with the direction set by the governance to achieve the objectives.
    - Risk tolerance – How are we going to practically work with our risk appetite and our environment.

- **Top-Down vs. Bottom-Up Security Management and Organization structure.**
  - **Bottom-Up:** IT Security is seen as a nuisance and not a helper, often changes when breaches happen.
  - **Top-Down:** IT leadership is on board with IT Security, they lead and set the direction. (The exam).

- **C-Level Executives (Senior Leadership) – *Ultimately Liable.***
  - **CEO:** Chief Executive Officer.
  - **CIO:** Chief Information Officer.
  - **CTO:** Chief Technology Officer.
  - **CSO:** Chief Security Officer.
  - **CISO:** Chief Information Security Officer.
  - **CFO:** Chief Financial Officer.
  - Normal organizations obviously have more C-Level executives, the ones listed here you need to know.



- **Governance standards and control frameworks.**
  - **PCI-DSS** - Payment Card Industry Data Security Standard
    - It is a standard but required if we want to handle or issue credit and debit cards.
  - **OCTAVE®** - Operationally Critical Threat, Asset, and Vulnerability Evaluation.
    - **Self Directed** Risk Management.
  - **COBIT** - Control Objectives for Information and related Technology.
    - **Goals** for IT – Stakeholder needs are mapped down to IT related goals.
  - **COSO** – Committee of Sponsoring Organizations.
    - **Goals** for the entire organization.
  - **ITIL** - Information Technology Infrastructure Library.
    - IT Service Management **(ITSM).**
  - **FRAP** - Facilitated Risk Analysis Process.
    - Analyzes one business unit, application or system at a time in a roundtable brainstorm with **internal** employees. Impact analyzed, threats and risks prioritized.
  - **ISO 27000 series**:
    - **ISO 27001:** Establish, implement, control and improvement of the ISMS. Uses PDCA (Plan, Do, Check, Act)
    - **ISO 27002:** (From BS 7799, 1/2, ISO 17799) Provides practical advice on how to implement security controls. It has 10 domains it uses for **ISMS** (Information Security Management Systems).
    - **ISO 27004:** Provides metrics for measuring the success of your ISMS.

- **ISO 27005:** Standards based approach to risk management.
- **ISO 27799:** Directives on how to protect PHI (Protected Health Information).

Links on all these as well as ones from previous slides in the "Extras" lecture.

- **Defense in Depth** – Also called Layered Defense or Onion Defense.
  - We implement multiple overlapping security controls to protect an asset.
  - This applies both to physical and logical controls.
    - To get to a server, you may have to go through multiple locked doors, security guards, man traps.
    - To get to the data, you may need to get past firewalls, routers, switches, the server, and the applications security.
    - Each step may have multiple security controls.
  - No single security control secures an asset.
  - By implementing Defense in Depth, you improve your organization's Confidentiality, Integrity, and Availability.

Legal and Regulatory Issues

- *There are a handful types of laws covered on the exam and important to your job as an IT Security Professional.*
  - **Criminal Law:**
    - "Society" is the victim and proof must be "Beyond a reasonable doubt".
    - Incarceration, death, and financial fines to "Punish and deter".
  - **Civil Law** (Tort Law):
    - Individuals, groups or organizations are the victims and proof must be "the majority of proof".
    - Financial fines to "Compensate the victim(s)".
  - **Administrative Law** (Regulatory Law):
    - Laws enacted by government agencies (FDA Laws, HIPAA, FAA Laws, etc.)
  - **Private Regulations**:
    - Compliance is required by contract (For instance PCI-DSS).
  - **Customary Law:**
    - Mostly handles personal conduct and patterns of behavior and it is founded in traditions and customs of the area or region.
  - **Religious Law:**
    - Based on the religious beliefs in that area or country, they often include a code of ethics and moralities which are required to be upheld.

- **Liability:**
  - If the question is who is ULTIMATELY liable, the answer is Senior Leadership. This does not mean you are not liable; you may be, that depends on Due Care. Who is held accountable? Who is to blame? Who should pay?

- **Due Diligence and Due Care:**
  - Due Diligence – The research to build the IT Security architecture of your organization, best practices and common protection mechanisms, research of new systems before implementing.
  - Due Care – Prudent person rule – What would a prudent person do in this situation?
    - *Implementing the IT Security architecture, keep systems patched. If compromised: fix the issue, notify affected users (Follow the Security Policies to the letter).*
  - **Negligence** (and gross negligence) is the opposite of Due Care.
    - If a system under your control is compromised and you can prove you did your Due Care, you are most likely not liable.
    - If a system under your control is compromised and you did NOT perform Due Care, you are most likely liable.

- **Evidence:**

  How you obtain and handle evidence is VERY important.
  - **Types of evidence:**
    - **Real Evidence:** Tangible and physical objects in IT Security: Hard disks, USB drives – NOT the data on them.
    - **Direct Evidence:** Testimony from a firsthand witness, what they experienced with their 5 senses.
    - **Circumstantial Evidence:** Evidence to support circumstances for a point or other evidence.
    - **Collaborative Evidence:** Supports facts or elements of the case: not a fact on its own, but support other facts.
    - **Hearsay:** Not first-hand knowledge – normally inadmissible in a case.
      - ☐ **Computer-generated records** - For us, that means log files are considered hearsay, but case law and updates to the Federal Rule of Evidence have changed that.

        Rule 803 provides for the admissibility of a record or report that was:

        "made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation."

- **Best Evidence Rule** – The courts prefer the best evidence possible.
  - Evidence should be accurate, complete, relevant, authentic, and convincing.
- **Secondary Evidence** – This is common in cases involving IT.
  - Logs and documents from the systems are considered secondary evidence.

- **Evidence Integrity** – It is vital that 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** – This is done to prove the integrity of the data; that no tampering was done.
  - Who handled it?
  - When did they handle it?
  - What did they do with it?
  - Where did they handle it?

- **Reasonable Searches:**
  - The Fourth Amendment to the United States Constitution protects citizens from unreasonable search and seizure by the government.
  - In all cases, the court will determine if evidence was obtained legally.
  - Exigent circumstances apply if there is an immediate threat to human life or of evidence destruction.
  - Your organization needs to ensure that our employees are aware their actions are monitored.
- **Entrapment and Enticement:**
  - **Entrapment** (Illegal and unethical): When someone is persuaded to commit a crime, they had no intention of committing and is then charged with it.
  - **Enticement** (Legal and ethical): Making committing a crime more enticing, but the person has already broken the law or at least has decided to do so.
    - Honeypots can be a good way to use Enticement.
      - ☐ If there is a gray area in some cases between Entrapment and Enticement, it is ultimately up to the jury to decide which one it was.
      - ☐ Check with your legal department before using honeypots. They pose both legal and practical risks.
- **Intellectual Property:**
  - **Copyright ©** - (Exceptions: first sale, fair use).
    - Books, art, music, software.
    - Automatically granted and lasts **70 years after creator's death or 95 years after creation by/for corporations.**
  - **Trademarks ™** and **®** (Registered Trademark).

        - Brand names, logos, slogans – Must be registered, is valid for 10 years at a time, can be renewed indefinitely.
    - **Patents: Protects inventions for 20 years** (normally) –
        - **Cryptography algorithms can be patented.**
        - Inventions must be:
            - ☐ **Novel** (New idea no one has had before).
            - ☐ **Useful** (It is actually possible to use and it is useful to someone).
            - ☐ **Nonobvious** (Inventive work involved).
    - **Trade Secrets.**
        - You tell no one about your formula, your secret sauce. If discovered, anyone can use it; you are not protected.
    - **Attacks on Intellectual Property:**
        - **Copyright.**
            - ☐ Piracy - Software piracy is by far the most common attack on Intellectual Property.
            - ☐ Copyright infringement – Use of someone else's copyrighted material, often songs and images.
        - **Trademarks.**
            - ☐ Counterfeiting – Fake Rolexes, Prada, Nike, Apple products – Either using the real name or a very similar name.
        - **Patents.**
            - ☐ Patent infringement – Using someone else's patent in your product without permission.
        - **Trade Secrets.**
            - ☐ While an organization can do nothing if their Trade Secret is discovered, *how* it is done can be illegal.

        - **Cyber Squatting** – Buying a URL you know someone else will need (gray area legally).
        - **Typo Squatting** – Buying a URL that is VERY close to real website name (Can be illegal in certain circumstances).

- **Privacy:**
    - You as a citizen and consumer have the right that your Personally Identifiable Information (PII) is being kept securely.
        - There are a number of Laws and Regulations in place to do just that.
    - US privacy regulation is a patchwork of laws, some overlapping, and some areas with no real protection.
    - EU Law – Very pro-privacy, strict protection on what is gathered, how it is used and stored.
        - There are a lot of large lawsuits against large companies for doing what is legal in the US (Google, Apple, Microsoft, etc.)

- **Rules, Regulations and Laws you should know for the exam (US):**
  - **HIPAA** (Not HIPPA) – Health Insurance Portability and Accountability Act.
    - Strict privacy and security rules on handling of PHI (Protected Health Information).
  - **Security Breach Notification Laws.**
    - NOT Federal, all 50 states have individual laws, know your state.
  - **Electronic Communications Privacy Act (ECPA):**
    - Protection of electronic communications against warrantless wiretapping.
    - The Act was weakened by the Patriot Act.
  - **PATRIOT Act of 2001:**
    - Expands law enforcement electronic monitoring capabilities.
    - Allows search and seizure without immediate disclosure.
  - **Computer Fraud and Abuse Act (CFAA) – Title 18 Section 1030:**
    - Most commonly used law to prosecute computer crimes.
  - **Gramm-Leach-Bliley Act (GLBA):**
    - Applies to financial institutions; driven by the Federal Financial Institutions
  - **Sarbanes-Oxley Act of 2002 (SOX):**
    - Directly related to the accounting scandals in the late 90s.
  - **Payment Card Industry Data Security Standard (PCI-DSS)**

    Technically not a law, created by the payment card industry.
    - The standard applies to cardholder data for both credit and debit cards.
    - Requires merchants and others to meet a minimum set of security requirements.
    - Mandates security policy, devices, control techniques, and monitoring.
    - NOT Federal, all 50 states have individual laws, know your state.
    -
- **General Data Protection Regulation (GDPR)**
  - **Restrictions:** Lawful Interception, national security, military, police, justice
  - **Personal data –** covers a variety of data types including: Names, Email Addresses, Addresses, Unsubscribe confirmation URLs that contain email and/or names, IP Addresses
    - **Right to access:** Data controllers must be able to provide a free copy of an individual's data if requested.
    - **Right to erasure:** All users have a "right to be forgotten".
    - **Data portability:** All users will be able to request access to their data "in an electronic format".
    - **Data breach notification:** Users and data controllers must be notified of data breaches within 72 hours.
    - **Privacy by design:** When designing data processes, care must be taken to ensure personal data is secure. Companies must ensure that only data is "absolutely necessary for the completion of duties".
    - **Data protection officers:** Companies whose activities involve data processing and monitoring must appoint a data protection officer.

- **Rules, Regulations and Laws you should know for the exam (EU):**
  - Legacy laws in the EU and between the EU and the US
    - EU Data Protection Directive
    - EU-US Safe Harbor
    - Privacy Shield

- **Organization for Economic Cooperation and Development (OECD) Privacy Guidelines** (International)**:**
  - 30 member nations from around the world, including the U.S.
  - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued in 1980, updated in 2013.
  - **Eight driving principles:**
    1. Collection limitation principle.
    2. Data quality principle.
    3. Purpose specification principle.
    4. Use limitation principle.
    5. Security safeguards principle.
    6. Openness principle.
    7. Individual participation principle.
    8. Accountability principle.

- **Wassenaar Arrangement** – Export/Import controls for Conventional Arms and Dual-Use Goods and Technologies.
  - 41 countries are a part of the arrangement.
  - Cryptography is considered "Dual-Use".
    - Iran, Iraq, China, Russia, and others have import restrictions on strong cryptography.
    - If it is too strong, it cannot be broken; they want to be able to spy on their citizens.
    - Companies have to make "country specific" products with different encryption standards.
  - The arrangement is used both to limit what countries want to export and to what some want to import.
  - It is the responsibility of the organization to know what is permitted to import/export from and to a certain country.
  - The Arrangement covers 10 Categories:
    1. Special materials and related equipment
    2. Materials processing
    3. Electronics
    4. Computers

    5.1– Telecommunications, 5.2 "Information security"
    6. Sensors and "Lasers"
    7. Navigation and avionics
    8. Marine
    9. Aerospace and propulsion.

- **3rd party, Acquisitions and Divesture.**
  - As our organizations rely more and more on 3rd party vendors for services and applications, we need to ensure their security standards, measures, and controls meet the security standards of our organization.
  - **Procurement**: When we buy products or services from a 3rd party, security is included and not an afterthought.
  - A common agreement is a **SLA** (Service Level Agreement) where for instance a 99.9% uptime can be promised.
  - Industry Standard Attestation should be used:
    - The 3rd party vendor must be accredited to the standards of your industry. This could be ISO, SOC, PCI-DSS.
    - "Rights to penetration test" and "Rights to audit" are often part of agreement (clearly defined).
  - **Acquisitions**: Your organization has acquired another.
    - How do you ensure their security standards are high enough?
    - How do you ensure data availability in the transition?
  - **Divestures**: Your organization is being split up.
    - How do you ensure no data crosses boundaries it shouldn't?
    - Who gets the IT Infrastructure?

Professional Ethics

- **ISC2 Code of Ethics**
  - You agree to this before the exam, and the code of ethics is **very testable**.
  - There are only four mandatory canons in the code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.
  - **Code of Ethics Preamble:**
    - The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
    - Therefore, strict adherence to this code is a condition of certification.
  - **Code of Ethics Canons:**
    - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
    - Act honorably, honestly, justly, responsibly, and legally.
    - Provide diligent and competent service to principals.
    - Advance and protect the profession.

- **Computer Ethics Institute**
  - **Ten Commandments of Computer Ethics:**
    - Thou shalt not use a computer to harm other people.
    - Thou shalt not interfere with other people's computer work.
    - Thou shalt not snoop around in other people's computer files.

- Thou shalt not use a computer to steal.
- Thou shalt not use a computer to bear false witness.
- Thou shalt not copy or use proprietary software for which you have not paid.
- Thou shalt not use other people's' computer resources without authorization or proper compensation.
- Thou shalt not appropriate other people's' intellectual output.
- Thou shalt think about the social consequences of the program you are writing or the system you are designing.
- Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

- **IABs Ethics and the Internet**
  - Defined as a Request For Comment (RFC), #1087 - Published in 1987
  - Considered unethical behavior:
    - Seeks to gain unauthorized access to the resources of the Internet.
    - Disrupts the intended use of the Internet.
    - Wastes resources (people, capacity, computer) through such actions :
      - ☐ Destroys the integrity of computer-based information.
      - ☐ Compromises the privacy of users.

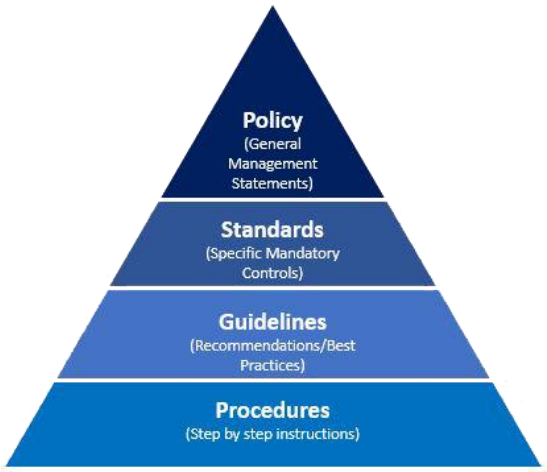
- **Your Organization's Ethics:**
  - You need to know the Internal Code of Ethics of your organization
    - If you don't, how can you adhere to it?

Information Security Governance

- **Security governance principles.**
  - **Values:**
    - What are our values? Ethics, Principles, Beliefs.
  - **Vision:**
    - What do we aspire to be? Hope and Ambition.
  - **Mission:**
    - Who do we do it for? Motivation and Purpose**.**
  - **Strategic Objectives:**
    - How are we going to progress? Plans, goals, and sequencing.

- **Action & KPIs**
  - What do we need to do and how do we know when we achieved it? Actions, Recourses, Outcomes, Owners, and Timeframes.

  - **Policies – Mandatory.**
    - High level, non-specific.
    - They can contain "Patches, updates, strong encryption"
    - They will not be specific to "OS, encryption type, vendor Technology"
  - **Standards – Mandatory.**
    - Describes a specific use of technology (All laptops are W10, 64bit, 8gig memory, etc.)
  - **Guidelines – non-Mandatory.**
    - Recommendations, discretionary – Suggestions on how you would to do it.
  - **Procedures – Mandatory.**
    - Low level step-by-step guides, specific.
    - They will contain "OS, encryption type, vendor Technology"
  - **Baselines (Benchmarks) - Mandatory.**
    - Benchmarks for server hardening, apps, network. Minimum requirement, we can implement stronger if needed.



- **Personnel Security – Users often pose the largest security risk:**
  - **Awareness** – Change user behavior - this is what we want, we want them to change their behavior.
  - **Training** – Provides users with a skillset - this is nice, but if they ignore the knowledge, it does nothing.
  - **Hiring Practices** – We do background checks where we check: References, degrees, employment, criminal, credit history (less common, more costly). We have new staff sign a NDA (Non-Disclosure Agreement).
  - **Employee Termination Practices** – We want to coach and train employees before firing them. They get warnings.
    - When terminating employees, we coordinate with HR to shut off access at the right time.
  - **Vendors, Consultants and Contractor Security.**
    - When we use outside people in our environments, we need to ensure they are trained on how to handle data. Their systems need to be secure enough for our policies and standards.

- **Outsourcing and Offshoring** - Having someone else do part of your (IT in our case) work.
  - This can lower cost, but a thorough and accurate Risk Analysis must be performed. Offshoring can also pose problems with them not having to comply with the same data protection standards.

Access Control Defensive Categories and Types

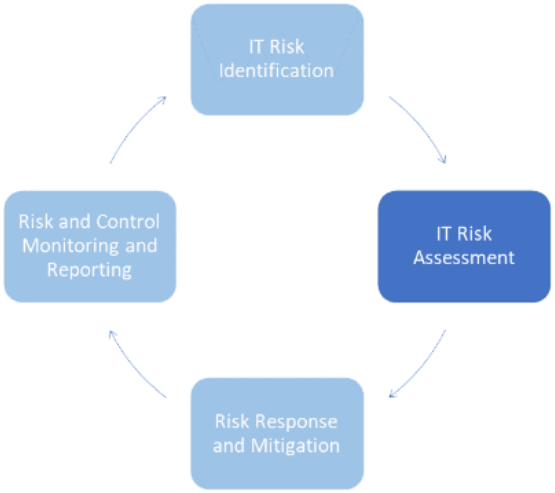
- **Access Control Categories:**
  - **Administrative (Directive) Controls:**
    - Organizational policies and procedures.
    - Regulation.
    - Training and awareness.
  - **Technical Controls:**
    - Hardware/software/firmware – Firewalls, routers, encryption.
  - **Physical Controls:**
    - Locks, fences, guards, dogs, gates, bollards.

- **Access Control Types** (Many can be multiple types – On the exam look at question content to see which type it is).
  - **Preventative:**
    - Prevents action from happening – Least privilege, drug tests, IPS, firewalls, encryption.
  - **Detective:**
    - Controls that Detect during or after an attack – IDS, CCTV, alarms, anti-virus.
  - **Corrective:**
    - Controls that Correct an attack – Anti-virus, patches, IPS.
  - **Recovery:**
    - Controls that help us Recover after an attack – DR Environment, backups, HA Environments .
  - **Deterrent:**
    - Controls that Deter an attack – Fences, security guards, dogs, lights, Beware of the dog signs.
  - **Compensating:**
    - Controls that Compensate – other controls that are impossible or too costly to implement.

Risk Identification, Assessment, Response, Monitoring and Reporting

- **Risk Management - Identification:**
  *Risk = Threat * Vulnerability*

- **The Risk Management lifecycle is iterative**.
  Identify our Risk Management team.
  - What is in and what is out of scope?
  - Which methods are we using?
  - Which tools are we using?
  - What are the acceptable risk levels, which type of risk appetite do we have in our enterprise?
  - Identify our assets.
    - Tangible: Physical hardware, buildings, anything you can touch.
    - Intangible: Data, trade secrets, reputation, etc.



- **Risk Assessment.**
  - Quantitative and Qualitative Risk Analysis.
  - Uncertainty analysis.
  - Everything is done using cost-benefit analysis.
  - Risk Mitigation/Risk Transference/Risk Acceptance/Risk Avoidance.
  - Risk Rejection is **NEVER** acceptable.
  - We assess the current countermeasures.
    - Are they good enough?
    - Do we need to improve on them?
    - Do we need to implement entirely new countermeasures?

- **Risk Analysis:**
  - **Qualitative vs. Quantitative Risk Analysis.**
    For any Risk analysis we need to identify our assets. What are we protecting?
  - **Qualitative Risk Analysis** – How likely is it to happen and how bad is it if it happens?
  - **Quantitative Risk Analysis** – What will it actually cost us in $? This is fact based analysis, Total $ value of asset, math is involved.
  - **Threat** – A potentially harmful incident (Tsunami, Earthquake, Virus, ...)

- **Vulnerability** – A weakness that can allow the Threat to do harm. Having a data center in the tsunami flood area, not earthquake resistant, not applying patches and anti-virus, …
- **Risk** = Threat x Vulnerability.
- **Impact** - Can at times be added to give a fuller picture. Risk = Threat x Vulnerability x Impact (How bad is it?).
- **Total Risk** = Threat x Vulnerability x Asset Value.
- **Residual Risk** = Total Risk – Countermeasures.

- **Qualitative Risk Analysis with the Risk Analysis Matrix.**

  Pick an asset: A laptop.

  - How likely is one to get stolen or left somewhere? I would think possible or likely.
  - How bad is it if it happens? That really depends on a couple of things:
    - Is it encrypted?
    - Does it contain classified or PII/PHI content?

Likelihood \ Consequences	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Possible	L	M	H	H	E
Unlikely	L	L	M	H	E

Where the L, M, H, E is for your organization can be different from this.
L = Low, M = Medium, H = High, E = Extreme Risk

  - Let's say it is likely and a minor issue, that puts the loss the high risk category.
  - It is normal to move high and extreme on the quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to "Low" or "Medium".

- **Risk Registers:**
  - A risk category to group similar risks.
  - The risk breakdown structure identification number.
  - A brief description or name of the risk to make the risk easy to discuss.
  - The impact (or consequence) if event actually occurs rated on an integer scale.
  - The probability or likelihood of its occurrence rated on an integer scale.
  - The Risk Score (or Risk Rating) is the multiplication of Probability and Impact, and is often used to rank the risks.
  - Common mitigation steps (e.g. within IT projects)
    - Identify
    - Analyze
    - Plan Response
    - Monitor
    - Control

Category	Name	Risk #	Probability	Impact	Mitigation	Contingency	Risk Score after Mitigation	Action By	Action When

- **Quantitative Risk Analysis**

  This is where we put a number on our assets and risks.

  - We find the asset's value: How much of it is compromised, how much one incident will cost, how often the incident occurs and how much that is per year.
    - Asset Value (**AV**) – How much is the asset worth?
    - Exposure factor (**EF**) – Percentage of Asset lost?
    - Single Loss Expectancy (**SLE**) = (**AV** x **EF**) – What does it cost if it happens once?
    - Annual Rate of Occurrence (**ARO**) – How often will this happen each year?
    - Annualized Loss Expectancy (**ALE**) – This is what it costs per year if we do nothing.
  - Total Cost of Ownership (**TCO**) – The mitigation cost: upfront + ongoing cost (Normally Operational

Let's look at a few examples.

Laptop – Theft/Loss (unencrypted)

	Value
Asset Value (AV)	$10,000
Exposure factor (EF)	100%
Single Loss Expectancy (SLE) – (AV x EF)	$10,000
Annual Rate of Occurrence (ARO)	25
Annualized Loss Expectancy (ALE)	$250,000

The Laptop ($1,000) + PII ($9,000) per loss (AV)
It is a 100% loss, it is gone (EF)
Loss per laptop is $10,000 (AV) x 100% EF) = (SLE)
The organization loses 25 Laptops Per Year (ARO)
The annualized loss is $250,000 (ALE)

Data Center – Flooding

	Value
Asset Value (AV)	$10,000,000
Exposure factor (EF)	15%
Single Loss Expectancy (SLE) – (AV x EF)	$1,500,000
Annual Rate of Occurrence (ARO)	0.25
Annualized Loss Expectancy (ALE)	$375,000

The Data Center is valued at $10,000,000 (AV)
If a flooding happens 15% of the DC is compromised (EF)
Loss per Flooding is $10,000,000 (AV) x 15% EF) = (SLE)
The flooding happens every 4 years = 0.25 (ARO)
The annualized loss is $375,000 (ALE)

Quantitative Risk Analysis

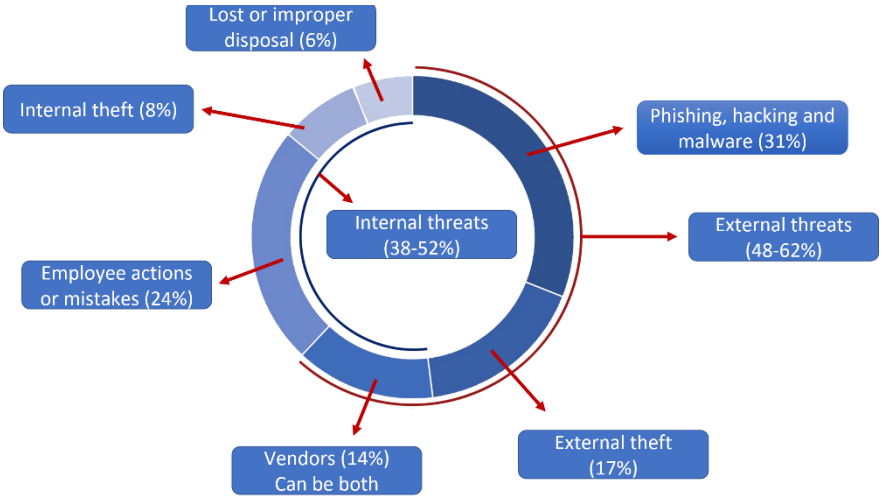
For the example, let's use a 4-year tech refresh cycle.

- Full disk encryption software and support = $75,000 initial and $5,000 per year.
- Remote wipe capabilities for the laptop = $20,000 initial and $4,000 per year.
- Staff for encryption and help desk = $25,000 per year

Doing nothing costs us $1,000,000 per tech refresh cycle ($250,000 per year).
Implementing full disk encryption and remote wipe will cost $231,000 per tech refresh cycle ($57,750 per year).

The laptop hardware is a 100% loss, regardless. What we are mitigating is the 25 x $9,000 = $225,000 by spending $57,750.

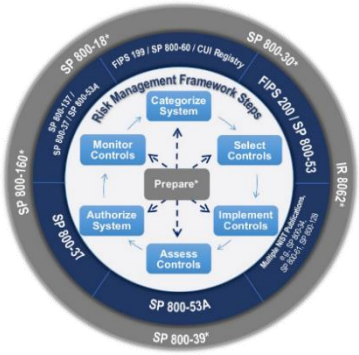
This is our ROI (Return On Investment): TCO ($57,750) < ALE ($250,000). This makes fiscal sense, we should implement.



- **Types of risk responses:**
  - **Accept the Risk** – We know the risk is there, but the mitigation is more costly than the cost of the risk (Low risks).
  - **Mitigate the Risk (Reduction)** – The laptop encryption/wipe is an example – acceptable level (Leftover risk = Residual).
  - **Transfer the Risk** – The insurance risk approach.
  - **Risk Avoidance** – We don't issue employees laptops (if possible) or we build the data center in an area that doesn't flood.
  - **Risk Rejection** – You know the risk is there, but you are ignoring it. This is **never** acceptable. (You are liable).
  - **Secondary Risk** – Mitigating one risk may open up another risk.

- This area is very testable. Learn the formula, the risk responses to differentiate Qualitative and Quantitative Risk.
  - **Qualitative** = Think "quality." This concept is semi-vague, e.g., "pretty good quality. "
  - **Quantitative** = Think "quantity." How many; a specific number.

- **NIST 800-30** - United States National Institute of Standards and Technology Special Publication
  - A 9-step process for Risk Management.
    1. System Characterization (Risk Management scope, boundaries, system and data sensitivity).
    2. Threat Identification (What are the threats to our systems?).
    3. Vulnerability Identification (What are the vulnerabilities of our systems?).
    4. Control Analysis (Analysis of the current and planned safeguards, controls and mitigations).
    5. Likelihood Determination (Qualitative – How likely is it to happen)?
    6. Impact Analysis (Qualitative – How bad is it if it happens? Loss of CIA).
    7. Risk Determination (Look at 5-6 and determine Risk and Associate Risk Levels).
    8. Control Recommendations (What can we do to Mitigate, Transfer, … the risk).
    9. Results Documentation (Documentation with all the facts and recommendations).

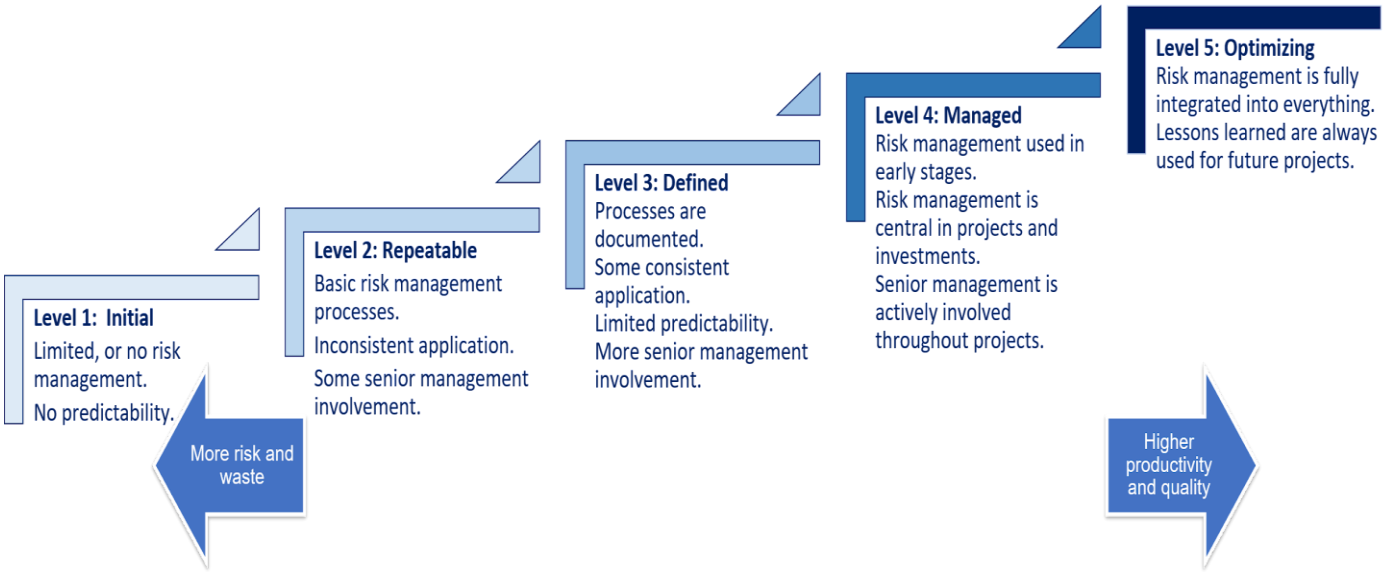


- **KGIs, KPIs and KRIs**
  - **KGI (Key Goal Indicators)**
    - Define measures that tell management, after the fact – whether an IT process has achieved its business requirements.
  - **KPI (Key Performance Indicators)**
    - Define measures that determine how well the IT process is performing in enabling the goal to be reached.
  - **KRI (Key Risk Indicators)**
    - Metrics that demonstrate the risks that an organization is facing or how risky an activity is.
    - They are the mainstay of measuring adherence to and establishing enterprise risk appetite.
    - Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.
    - KRI gives an early warning to identify potential event that may harm continuity of the activity/project.

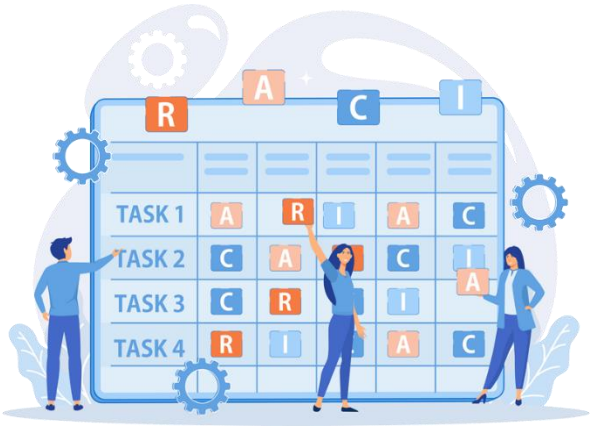
- **Risk Response and Mitigation**
  - Risk mitigation, transference, acceptance or avoidance.
  - We act on senior managements choices, which they made based on our recommendations from the assessment phase.

- Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?
- We update the risk register, with the mitigations, the risk responses we chose and see if the new risk level is acceptable.

- **Risk and Control Monitoring and Reporting**
  - The process is ongoing, we have to keep monitoring both the risk and the controls we implemented.
  - This is where we could use the KRIs (Key Risk Indicators)
  - We would also use KPIs (Key Performance Indicators)
  - You are the translating link, you have to be able to explain IT and IT Security to Senior Management in terms they can understand.
  - It is normal to do the Risk Management lifecycle on an annual basis, and do out-of-cycle Risk Management on critical items.
- **Risk Management Maturity Model**
  - Sponsor and Management
  - Identify Risk
  - Analyze Risk
  - Plan Risk response
  - Integrate risk management and project management systems
  - Trust in and a culture of risk management



RACI Chart



- **Responsible, Accountable, Consulted, Informed**
  - R (Responsible) - The person or people that does the actual work to complete the task.
  - A (Accountable) - The person ultimately accountable for the correct and thorough completion of the task.
  - C (Consulted) - The people who provide information for the task and with whom there is two-way communication.
  - I (informed) - The people who are kept informed about the task's progress and with whom there is one-way communication.

Tasks/Processes	IT Manager	Network Engineer	Security Analyst	Database Admin	Software Developer
Manage IT infrastructure	A	R	I	I	I
Maintain network security	I	R	A	I	I
Ensure data integrity	I	I	C	A	R
Update security policies	R	C	A	I	I
Perform risk assessment	C	I	A	I	I
Monitor system performance	I	A	I	R	C
Implement new software solutions	C	I	I	C	A
Data backup and recovery	I	R	C	A	I
Audit IT Systems	R	C	A	C	I
User access management	I	A	R	C	I

Governance, Risk Management, Compliance

- GRC – aligning our risk management strategies to our business objectives and compliance standards.
    - **Governance** – ensures that IT goals and processes aligns with our business objectives.
    - **Risk Management** – the process of identifying, assessing, and responding to risks.
    - **Compliance** – conforming with a stated requirement.
        - Laws and regulations.
        - Auditing and monitoring.
        - Ethics and privacy.

NIST 800-53 rev. 5

- **Security and Privacy Controls for Information Systems and Organizations**
    - Provides detailed security controls for US federal systems.
    - Guides us on how to create, operate, and maintain security systems.
    - Gives us a comprehensive risk-based approach to information security.

- **Control Families –** focus on a specific aspect of security and privacy.
- **Control Classes –** Management, Operational, Technical.
- **Baseline Controls –** the minimum level of security in a system.

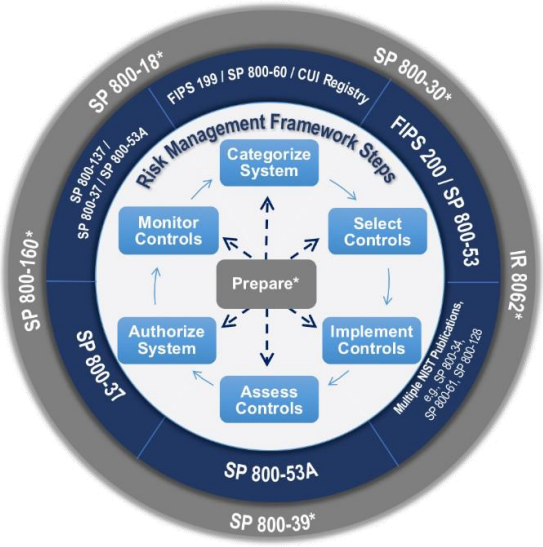
- The inclusion of privacy controls.
- Outcome-based approach.
- More focus on supply chain management.
- Protection against insider threats.

NIST 800-37 Rev. 1 and 2

- Revision 1: Date Published: February 2010 (Updated 6/5/2014).
- Revision 2: Date Published: December 2018.

- **There are seven major objectives for this update:**
    1. To provide closer linkage and communication between the risk management processes and activities at the C-suite.
    2. To institutionalize critical risk management preparatory activities at all risk management levels.
    3. To demonstrate how the NIST Cybersecurity Framework [NIST CSF] can be aligned with the RMF and implemented using established NIST risk management processes.

4. To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible.
5. To promote the development of trustworthy secure software and systems.
6. To integrate security-related, supply chain risk management (SCRM) concepts into the RMF.
7. To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5.



NIST Cyber Security Framework Rev. 1.1

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

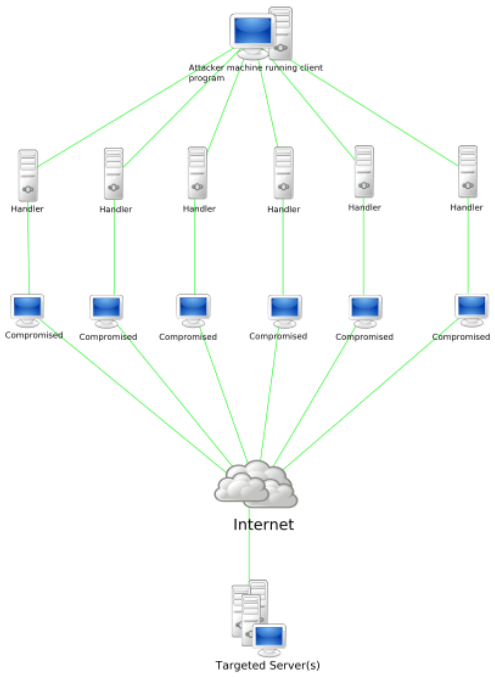
Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

- **Types of attackers**
  - **Hackers:**
    - **Now:** Anyone trying to get access to or disrupt any leg of the CIA Triad (Confidentiality, Integrity, Availability).
    - **Original use:** Someone using something in a way not intended.
    - **White Hat hackers:** Professional pen testers trying to find flaws so we can fix it (Ethical hackers).
    - **Black Hat hackers:** Malicious hackers, trying to find flaws to exploit them (Crackers – they crack the code).
    - **Gray/Grey Hat hackers:** They are somewhere between the white and black hats, they go looking for vulnerable code, systems or products.
    - **Script Kiddies:**
      - ☐ They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use.
  - **Outsiders:**
    - Unauthorized individuals - Trying to gain access; they launch the majority of attacks, but are often mitigated if the organization has good Defense in Depth.
    - Interception, malicious code (e.g. virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage or unauthorized system access.
    - 48-62% of risks are from outsiders.

- **Insiders:**
  - Authorized individuals - Not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
  - This could be: Assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified or corrupted data.
  - 38-52% of risks are from insiders, another reason good Authentication and Authorization controls are needed.
- **Hacktivism/Hacktivist (hacker activist):** Hacking for political or socially motivated purposes.
  - Often aimed at ensuring free speech, human rights, freedom of information movement.
- **Governments:**
  - State sponsored hacking is common; often you see the attacks happening between the hours of 9 and 5 in that time zone; this is a day job.
  - Approximately 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), …

- **Bots and botnets** (short for robot):
  - **Bots** are a system with malware controlled by a botnet.
  - The system is compromised by an attack or the user installing a remote access trojan (game or application with a hidden payload).
  - They often use IRC, HTTP, or HTTPS.
  - Some are dormant until activated.
  - Others are actively sending data from the system (Credit card/bank information for instance).
  - Active bots can also can be used to send spam emails.
- **Botnets** is a C&C (Command and Control) network, controlled by people (bot-herders).
  - There can often 1,000s or even 100,000s of bots in a botnet.



- **Types of Attacks**
  - **Phishing, spear phishing and whale phishing** (Fisher spelled in hacker speak with Ph not F).
    - **Phishing** (Social engineering email attack):
      - ☐ Click to win, Send information to get your inheritance …
      - ☐ Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.
    - **Spear Phishing:** Targeted phishing, not just random spam, but targeted at specific individuals.
      - ☐ Sent with knowledge about the target (person or company); familiarity increases success.
    - **Whale Phishing (Whaling):** Spear phishing targeted at senior leadership of an organization.
      - ☐ This could be: "Your company is being sued if you don't fill out the attached documents (with trojan in them) and return them to us within 2 weeks".
    - **Vishing (Voice Phishing):** Attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.
      - ☐ These are: "Your taxes are due", "Your account is locked" or "Enter your PII to prevent this" types of calls.

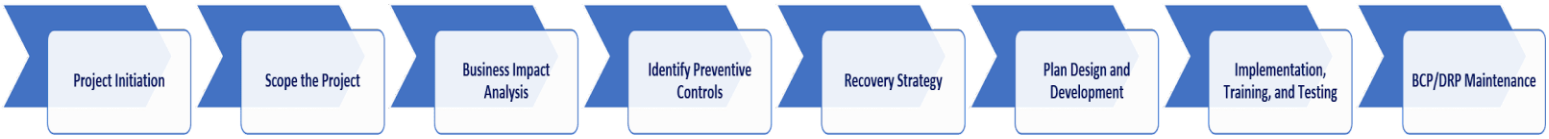
Business Continuity Plan (BCP) and Business Impact Analysis (BIA)

- **Business Continuity Plan (BCP)** 
  - 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.
  - BCPs 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.
  - 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.

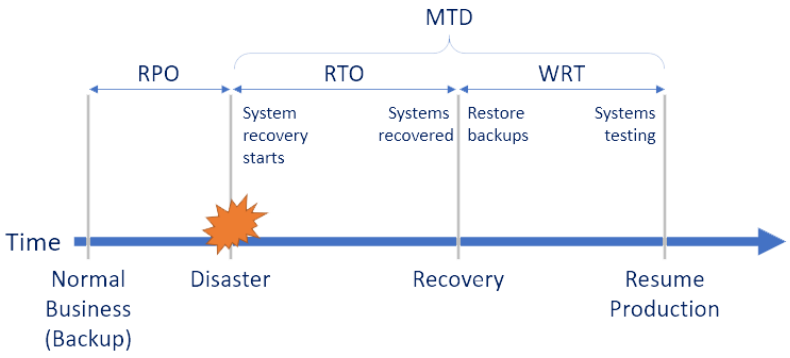
- **Developing our BCP:**

  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.



- **Business Impact Analysis (BIA)**
  - 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 RPO must ensure that the maximum tolerable data loss for the system, function, or activity is not exceeded.
- **MTD** (Maximum Tolerable Downtime): **MTD ≥ RTO + WRT:**
  - System rebuild time, configuration, and 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.
  - **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/component will function on average.
- **MTTR** (Mean Time to Repair): How long it will take to recover a failed system.
- **MOR** (Minimum Operating Requirements): The minimum requirements for our critical systems to function.

Final Points to Remember

- **Finding the right mix of Confidentiality, Integrity, and Availability is a balancing act.**
  - This is really the cornerstone of IT Security – finding the RIGHT mix for your organization.
    - Too much Confidentiality and the Availability can suffer.
    - Too much Integrity and the Availability can suffer.
    - Too much Availability and both the Confidentiality and Integrity can suffer.
- **IT Security is there to Support the organization.**
  - We are there to enable the organization to fulfil its mission statement and the business' goals.
  - We are **not** the most important part of the organization, but we span the entire organization.
  - We are Security leaders **and** Business leaders – Answer exam questions wearing BOTH hats.
- **GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).**
  - It does **not** matter where we are based, if we have customers in EU/EEA we have to adhere to the GDPR.
  - Violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

  - Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so.

- **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.

- **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 who should 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.

- **BCPs/DRPs are often built using the waterfall project management methodology.**

What we covered in the first CBK Domain:

- ✓ How we want our data to be confidential, keep its integrity, and have it available when we need to access it.
- ✓ How we identify, authenticate, authorize our employees, and keep them accountable (IAAA).
- ✓ Need to know, least privilege, non-repudiation, subjects, and objects.
- ✓ The governance structure we have in our organization, the control frameworks we use how we use defense in depth.
- ✓ Laws and regulations in our field and in general.
- ✓ How we use due care, due diligence to avoid negligence, and who is liable when.
- ✓ What constitutes evidence, how we collect, and handle it properly.
- ✓ The different kinds of intellectual property, the laws around them, and the attacks on them.
- ✓ The ISC2 code of ethics – You agree to them before taking the exam and they are very testable.
- ✓ The qualitative risk analysis that then leads into the quantitative risk analysis, where we put numbers, and dollars on the risks and then choose mitigation strategies.
- ✓ The attackers we need to protect ourselves against.
- ✓ How we build our BCP and do our BIA and what we have to consider for each of them.

Additional graphics