Thor's Study Guide - CISM® Domain 1

Contents

Thor's Study Guide – CISM® Domain 1

Introduction to Domain 1: Information Security Governance

- This chapter is **VERY** important because:
  - Every other knowledge domain build on top of this chapter
  - This is the **foundation**.
- 17% of the exam questions on the certification are from this domain.

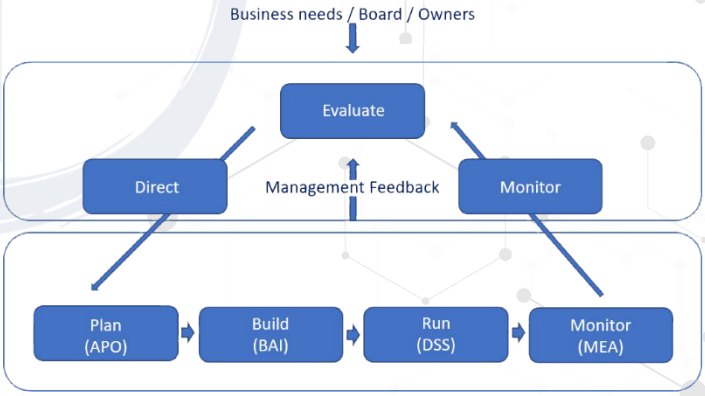
- We will be covering our govern, our values, vision, mission, our strategies, policies, standards, and processes.
- We look at the policies, the procedures, the laws we need to adhere to.
- Data protection, the NIST Cyber Security framework, NIST Risk management framework, NIST 800-37, 800-53, ISO 27001 and 27002
- We talk about the CIA triad, which is the foundation of Information Security.
- Administrative security controls, roles, and responsibilities.

- This should be what you are tested on for Domain 1 until the next planned CISM curriculum change in 2027.

Security Governance Principles

Governance vs. Management

- **Governance** – This is C-level Executives (Not you).
  - Stakeholder 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.



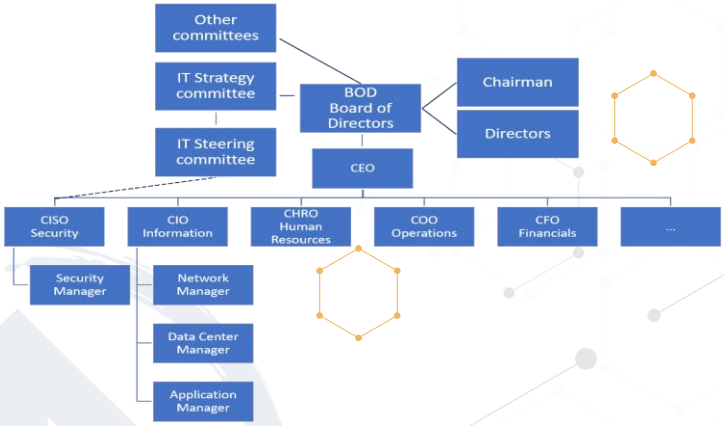
- **Management** – How do we get to the destination (This is you).
  - Plans, builds, runs, and monitors activities in alignment with the direction set by the governance to achieve the objectives.
  - Risk tolerance – How are we going to practically work with our risk appetite and our environment?

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

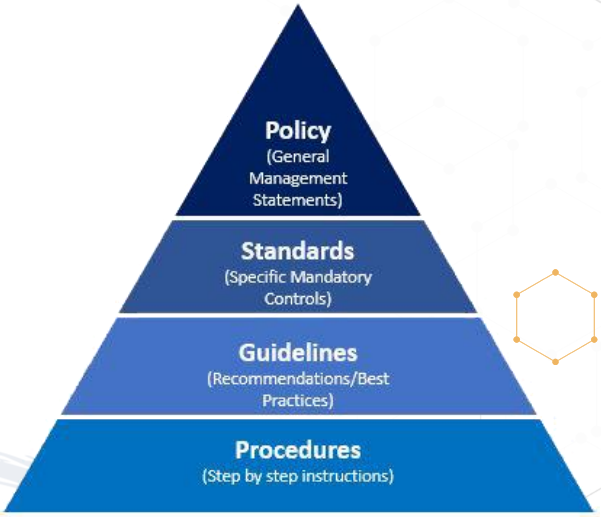
- We implement multiple overlapping security controls to protect an asset.
- This applies both to physical and logical controls.
  - To get to a server, you may have to go through multiple locked doors, security guards, man traps.
  - To get to the data, you may need to get past firewalls, routers, switches, the server, and the application's 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.

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 an 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.

Gap Analysis

- **Identify the existing process:**
  - What are we doing?
- **Identify the existing outcome:**
  - How well do we do it?
- **Identify the desired outcome:**
  - How well do we want to do?
- **Identify and document the gap:**
  - What is the difference between now and desired result?

Area	Current state	Target state	Difference	Action plan	Priority
Lemonade	$10 per day	$30 per day	$20	Build new stand	High
Cookies	$0 per day	$25 per day	$25	Add to lemonade stand	Medium

- **Identify the process to achieve the desired outcome:**
  - How can we possibly get to the desired result?
- **Develop the means to fill the gap:**
  - Build the tool or processes to get the result.
- **Develop and prioritize Requirements to bridge the gap.**

SWOT (Strengths, Weaknesses, Opportunities, and Threats)

- **Internal Factors:**
  - **Strengths:** What we do well, skilled staff, assets, and advantages over competitors.
  - **Weaknesses:** Things we are missing, resource limitations.
    - Human resources, physical resources, financials, activities and processes, and past experiences.
- **External Factors:**
  - **Opportunities:** Elements in the environment that the business or project could exploit to its advantage.
  - **Threats:** Elements in the environment that could cause trouble for the business or project.
    - Future trends, the economy, funding, our physical environment, legislation, national, or international events

Organizational Finances

- **OPEX vs. CAPEX:**
  - **OPEX (Operating Expense)** is the ongoing cost for running a product, business, or system. (Keeping the lights on).
  - **CAPEX (Capital Expenditure)** is the money a company spends to buy, maintain, or improve its fixed assets, such as buildings, vehicles, equipment, or land.
- **Business plans, roadmaps:**
  - We build our organizational business plans based on the organizations mission statement and vision at the direction of senior leadership.
  - We have 1-year, 3-year, and 5-year business plans and roadmaps.

- **Fiscal years (budget year):**
  - We plan our budgets according to our organization's fiscal year.

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.

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

- 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.

- 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.

Confidentiality, Integrity, and Availability

- **Threats:**
  - Alterations of our data.
  - Code injections.
  - Attacks on your encryption (cryptanalysis).

- **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.

Confidentiality, Integrity, and Availability

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

- **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).

Confidentiality, Integrity, and Availability

- 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.
- The opposites of the CIA Triad are DAD (Disclosure, Alteration and Destruction).
  - 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.

Sensitive Information and Media Security

Sensitive Information

- Any organization has data that is considered sensitive for a variety of reasons.
- We want to protect the data from Disclosure, Alteration and Destruction **(DAD).**
- **Data has 3 States:** We want to protect it as well as we can in each state.
    - **Data at Rest** (Stored data): This is data on disks, tapes, CDs/DVDs, USB sticks
        - We use disk encryption (full/partial), USB encryption, tape encryption (avoid CDs/DVDs).
        - Encryption can be hardware or software encryption.
    - **Data in Motion** (Data being transferred on a network).
        - We encrypt our network traffic, end to end encryption, this is both on internal and external networks.
    - **Data in Use:** (We are actively using the files/data, it can't be encrypted).
        - Use good practices: Clean desk policy, print policy, allow no 'shoulder surfing', may be the use of view angle privacy screen for monitors, locking computer screen when leaving workstation.

Data Classification and Policies

Top Secret (TS) - Exceptionally grave damage Weapon blueprints, theater or war plans, espionage data.	**Confidential - Exceptionally grave damage** Proprietary information, trade secrets, source code, anything that gives us a competitive advantage.
Secret (S) - Serious damage Troop plans, deployment plans, plans not included in TS plans, reports on shortages or weaknesses.	**Private - Serious damage** PHI, PII, financial data, employee data, payroll.
Confidential (C) - Damage Intelligence reports, operational or battle reports, mobilization plans.	**Sensitive - Damage** Networking diagrams, IP assignments, system and software specific information.
Unclassified (U) Available upon request, does not need a particular classification or has been declassified.	**Public** Websites, advertisements, any information we make publicly available.

- **Labels: Objects have Labels** assigned to them.
    - The label is used to allow Subjects with the right clearance to access them.
    - Labels are often more granular than just "Top Secret" they can be "Top Secret – Nuclear."
- **Clearance: Subjects have Clearance** assigned to them.
    - A formal decision on a subject's current and future trustworthiness.

- The higher the clearance, the more in-depth the background checks should be (always in military, not always in business).

- **Formal Access Approval:**
  - Document from the data owner approving access to the data for the subject.
  - Subject must understand all requirements for accessing the data and the liability involved if compromised, lost, or destroyed.
  - Appropriate Security Clearance is required as well as the Formal Access Approval.
- **Need to know:**
  - Just because you have access does not mean you are allowed the data.
  - You need a **valid** reason for accessing the data. If you do not have one you can be terminated/sued/jailed/fined.
    - Leaked information about Octomom Natalie Suleman cost 15 Kaiser employees fines or terminations because they had no valid reason for accessing her file.
    - We may never know who actually leaked the information. It may not be one of the 15, but they violated HIPAA by accessing the data.
- **Least privilege:** Users have the minimum necessary access to perform their job duties.

Sensitive Information and Media Security

Sensitive Information

- **Data handling:**
  - Only trusted individuals should handle our data; we should also have policies on how, where, when, and why the data was handled. Logs should be in place to show these metrics.
- **Data storage:**
  - Where do we keep our sensitive data? It should be kept in a secure, climate-controlled facility, preferably geographically distant or at least far enough away that potential incidents will not affect that facility too.
    - Many older breaches were from bad policies around tape backups.
    - Tapes were kept at the homes of employees instead of at a proper storage facility or in a storage room with no access logs and no access restrictions (often unencrypted).
- **Data retention:**
  - Data should not be kept beyond the period of usefulness or beyond the legal requirements (whichever is greater).
  - Regulation (HIPAA or PCI-DSS) may require a certain retention of the data (1, 3, 7 years, or infinity).
  - Each industry has its own regulations and company policies may differ from the statutory requirements.
  - Know your retention requirements!

Data, System, Mission Ownership, Custodians and Users

Each role has unique roles and responsibilities to keep the data safe.

- **Mission/business owner:**
  - Senior executives make the policies that govern our data security.
- **Data/information owners:**
  - Management level, they assign sensitivity labels and backup frequency.
  - This could be you or a data owner from HR, payroll, or other departments.
- **Data custodians:**
  - These are the technical hands-on employees who do the backups, restores, patches, system configuration. They follow the directions of the data owner.
- **System owner:**
  - Management level and the owner of the systems that house the data.
  - Often a data center manager or an infrastructure manager.
- **Data controllers and data processors:**
  - Controllers create and manage sensitive data in the organization (HR/Payroll)
  - Processors manage the data for controllers (Outsourced payroll)
- **Security Administrators:**
  - Responsible for firewalls, IPS' (Intrusion Prevention Systems), IDS' (Intrusion Detection Systems), security patches, create accounts, and assigns access to the data following the data owners' directions.
- **Supervisors:**
  - Responsible for user behavior and assets created by the users. Directly responsible for user awareness and needs to inform the security administrator if there are any changes to user employment status, user access rights, or any other pertinent changes to an employee's status.
- **Users:**
  - These are the users of the data. User awareness must be trained; they need to know what is acceptable and what is not acceptable, and the consequences for not following the policies, procedures, and standards.
- **Auditors:**
  - Responsible for reviewing and confirming our security policies are implemented correctly, we adhere to them, and that they provide the protection they should.

Ethics

ISACA professional Code of Ethics: You sign this before the exam.

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security, and risk management.
2. Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.

4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge, and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security, and risk management.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

Computer Ethics Institute

Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

IAB's 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 do not, how can you adhere to it?

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, and 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 first-hand witness, what they experienced with their 5 senses.
  - **Circumstantial Evidence:** Evidence to support circumstances for a point or other evidence.
  - **Corroborative Evidence:** Supports facts or elements of the case; not facts on their own but they 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.

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 Law:**
    - 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 90's.
- **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.

GDPR (General Data Protection Regulation)

- 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.
- **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.

Legal and Regulatory Issues

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:**
  - Collection limitation principle.
  - Data quality principle.
  - Purpose specification principle.

- Use limitation principle.
- Security safeguards principle.
- Openness principle.
- Individual participation principle.
- 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 the laws concerning import/export from and to a certain country.
- The Arrangement covers 10 Categories:
  - Special materials and related equipment
  - Materials processing
  - Electronics
  - Computers
  - Telecommunications, "Information security"
  - Sensors and "Lasers"
  - Navigation and avionics
  - Marine
  - Aerospace and propulsion.

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).

Administrative Personnel Security Controls

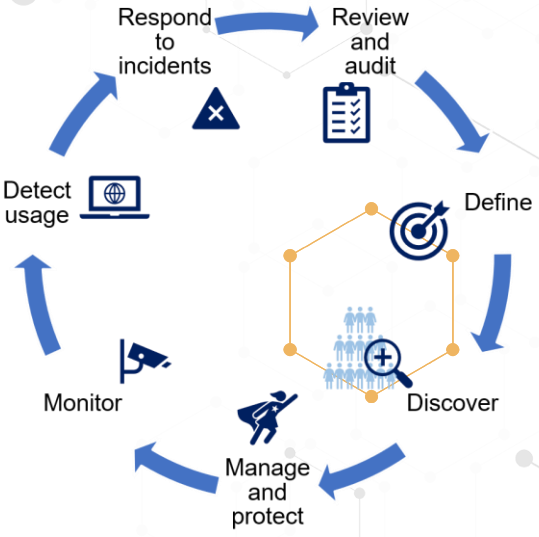
Administrative Security

- Provides the means to control people's operational access to data.
- **Least Privilege:**
  - We give employees the minimum necessary access they need, no more, no less.
- **Need to know:**
  - Even if you have access, if you do not need to know, then you should not access the data. (Kaiser employees).
- **Separation of duties:**
  - More than one individual in one single task is an internal control intended to prevent fraud and error.
  - We do not allow the same person to enter the purchase order and issue the check.
  - For the exam assume the organization is large enough to use separation of duties, in smaller organizations where that is not practical, compensating controls should be in place.
- **Job rotation:**
  - For the exam think of it to detect errors and frauds. It is easier to detect fraud and there is less chance of collusion between individuals if they rotate jobs.

- It also helps with employee's burnout, and it helps employees understand the entire business.
- This can be to cost prohibitive for the exam/real life, make sure on the exam the cost justifies the benefit.

- **Mandatory vacations:**
  - Done to ensure one person is not always performing the same task, someone else has to cover and it can keep fraud from happening or help us detect it.
  - Their accounts are locked, and an audit is performed on the accounts.
  - If the employee has been conducting fraud and covering it up, the audit will discover it.
  - The best way to do this is to not give too much advance notice of vacations.
- With the combination of all 5 we minimize some of the insider threats we may have.
- **NDA (non-disclosure agreement):**
  - We covered NDAs between our and other organizations, it is also normal to have them for internal employees.
  - Some employment agreements will include a clause restricting employees' use and dissemination of company-owned confidential information.
- **Background checks:**
  - References, Degrees, Employment, Criminal, Credit history (less common, more costly).
  - For sensitive positions the background check is an ongoing process.
- **Privilege monitoring:**
  - The more access and privilege an employee have the more we keep an eye on their activity.
  - They are already screened more in depth and consistently, but they also have access to many business-critical systems, we need to audit their use of that access.
  - With more access comes more responsibility and scrutiny.

- **Privileged Account/Access Management (PAM):**
  - Account (account safeguarded) vs. Access (Account + what can the account access/do).
  - We want to identify and monitor anyone with more access than the normal user. The higher privileges they have the closer they should be monitored.
  - We monitor the what/when/how/why/where of what is accessed.
  - Full monitoring, limit privileges, MFA, monitor remote connections, logs/records are immutable, anomaly detection, continuous monitoring, full visibility of all admins, and no group accounts.
  - **Users:**
    - **Regular users:** Analyze performance, improve efficiency.

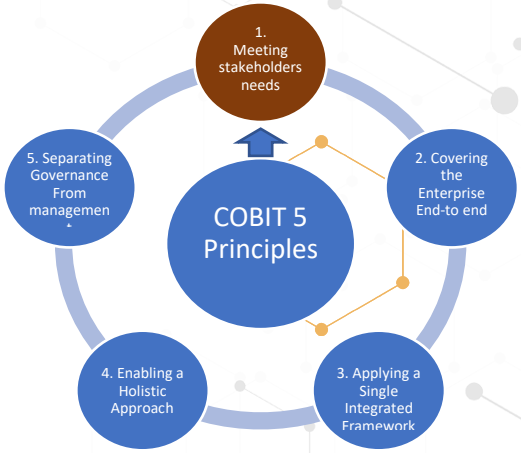


The Privileged Access Management lifecycle

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

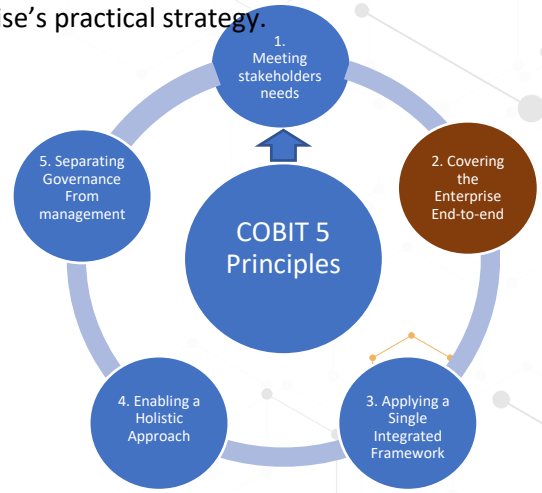
Cobit 5

- **Principle 1: Meeting Stakeholder Needs**
    - Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them.
    - Governance is about negotiating and deciding amongst different stakeholders' value interests.
    - The governance system should consider all stakeholders when making benefit, resource, and risk assessment decisions.
    - For each decision, the following can and should be asked:
        - Who receives the benefits?
        - Who bears the risk?
        - What resources are required?

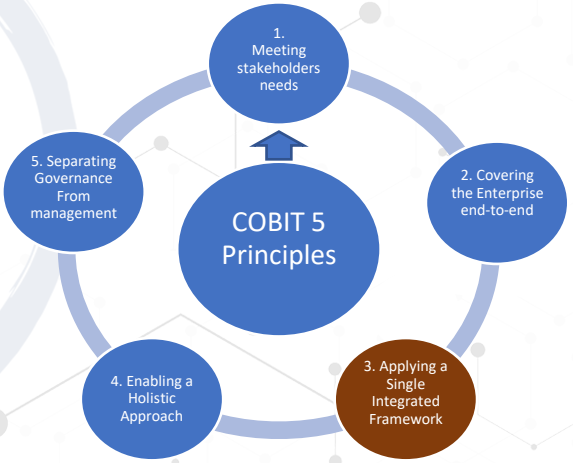


- Stakeholder needs have to be transformed into an enterprise's practical strategy.

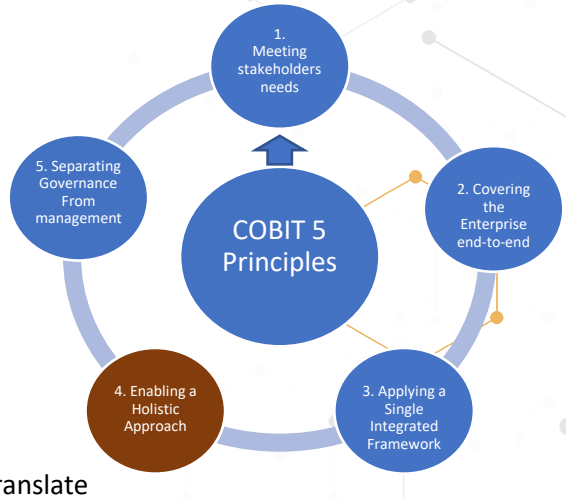
- **Principle 2: Covering the Enterprise End-to-End**
  - COBIT 5 addresses the governance and management of information and related technology from an enterprise wide, end-to-end perspective.
  - This means that COBIT 5:
    - Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance.
    - Covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.



- **Principle 3: Applying a Single, Integrated Framework**
  - COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:
    - Enterprise: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
    - IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI
  - This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
  - ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.

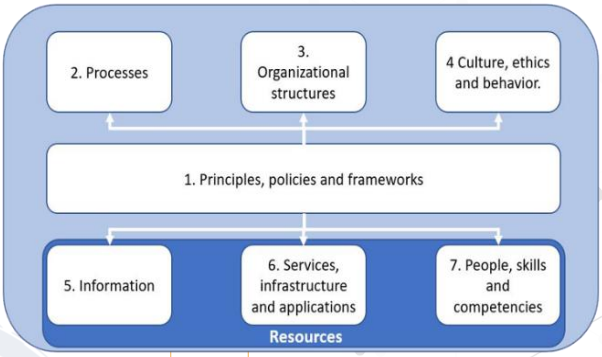


- **Principle 4: Enabling a Holistic Approach**
  - COBIT 5 enablers are:
  - Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT
  - Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve
  - Described by the COBIT 5 framework in seven categories:
    1. **Principles, policies, and frameworks:** Are the vehicles to translate

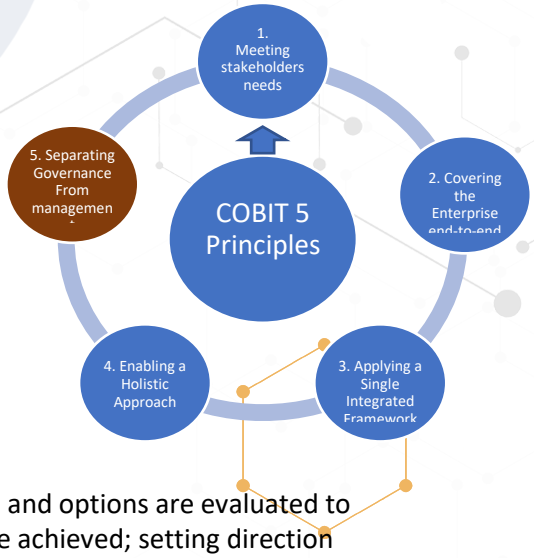


the desired behavior into practical guidance for day-to-day management

2. **Processes:** Describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals
3. **Organizational structures:** Are the key decision-making entities in an organization
4. **Culture, ethics, and behavior:** Of individuals and of the organization; very often underestimated as a success factor in governance and management activities
5. **Information:** Is pervasive throughout any organization, it deals with all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. **Services, infrastructure, and applications:** Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services
7. **People, skills and competencies:** Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions

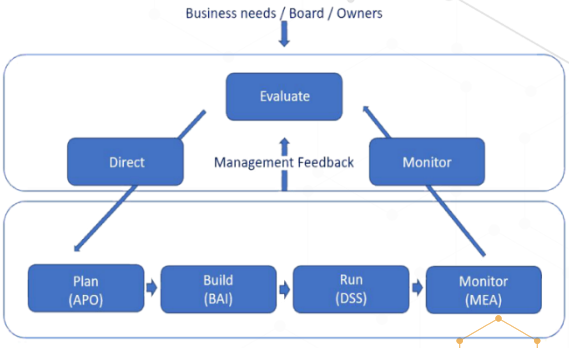


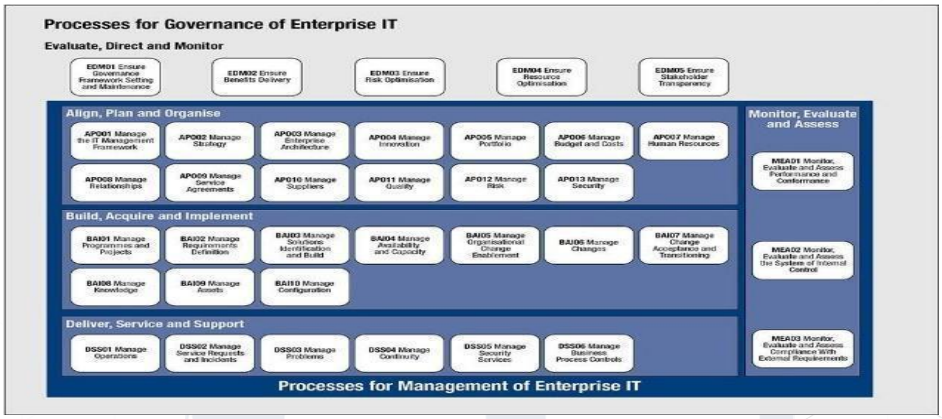
- **Principle 5: Separating Governance from Management**
  - The COBIT 5 framework makes a clear distinction between governance and management.
  - These two disciplines:
    - Encompass different types of activities.
    - Require different organizational structures
    - Serve different purposes
  - **Governance**: In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
  - **Management**: In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.
  - **Governance** ensures that stakeholders' needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction



through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

- **Management** plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.





ISO/IEC 27001 and 27002

- Most organizations have many different information security controls, if we do not have an information security management system (ISMS), our controls are often disorganized and only cover some of our organization.
- ISO/IEC 27001 is a management system that is used to bring information security under management control and gives **specific** requirements. It is the framework, and we can get certified against ISO27001.
- ISO/IEC 27002 provides **best practice** recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining ISMS. Much more in detail, how we implement our ISMS.

NIST 800-53 Rev. 5

Security and Privacy Controls for Federal 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.

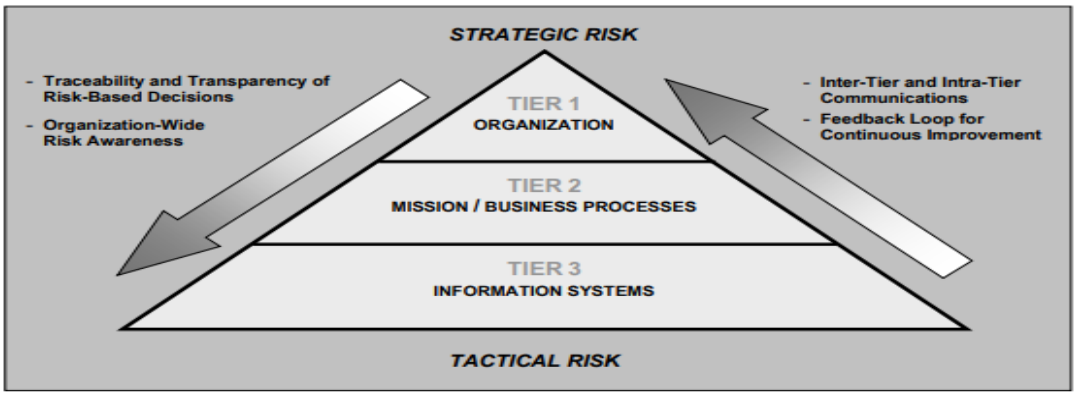
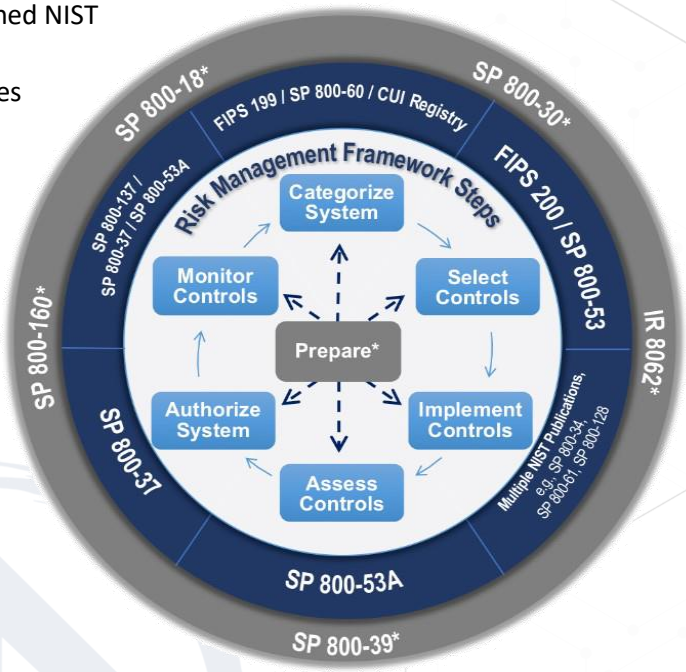


FIGURE 1: THREE-TIERED RISK MANAGEMENT APPROACH

There are seven major objectives or 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

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.

Data Security Frameworks

We use standards, baselines, scoping, and tailoring to decide which controls we use, and how we deploy them.

- Different controls are deployed for data at rest and data in motion.
- Some of the standards and frameworks used could be PCI-DSS, ISO27000, OCTAVE, COBIT, or ITIL.
- **Scoping** is determining which portion of a standard we will deploy in our organization.
    - We take the portions of the standard that we want or that apply to our industry and determine what is in scope and what is out of scope for us.
- **Tailoring** is customizing a standard to your organization.
    - This could be, we will apply this standard, but we use a stronger encryption (AES 256bit).
- **Certification:** A system, and the security measures to protect it, meet the security requirements set by the data owner or by regulations/laws.
- **Accreditation:** The data owner accepts the certification and the residual risk. This is required before the system can be put into production.

Data Protection

- **Digital Rights Management (DRM)** - Uses technology and systems to protect copyrighted digital media.
    - Encryption – Regional DVDs.
    - Permissions management and limiting access.
    - Serial numbers, limit installations, expiry dates, IP addresses, geolocation, VPN.
    - Copy restrictions: Copy, edit, saving, screenshots, screen recording, printing.
    - Persistent authentication and audit trails.
    - Tracking – watermarks or meta data embedded in files.
- **Cloud Access Security Broker (CASB)** – on-premises or cloud software between our users and our cloud applications.
    - Monitors user activity warns admins about possible malicious/dangerous actions, malware prevention, protects against shadow IT, and enforces security policy compliance.
- **Data Loss Prevention (DLP)**
    - Loss vs. leak.
    - Data in use, in motion, and at rest.
    - Network and endpoint DLP.

Security Models and Fundamental Concepts

Security models provide the rules for how we secure our data, while focusing on different goals and what they provide.

- **DAC** - (Discretionary Access Control) gives subjects full control of objects they have created or been given access to.
- **MAC** - (Mandatory Access Control) is system-enforced access control based on a subject's clearance and an object's labels.

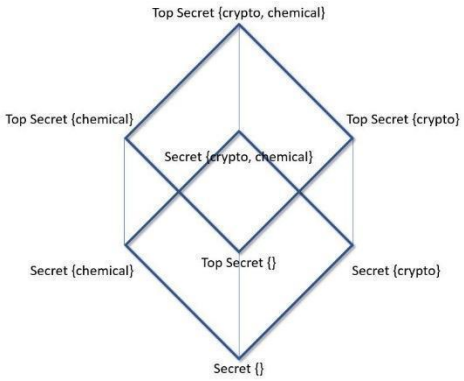
- **RBAC** - (Role Based Access Control) is where access to objects is granted based on the role of the subject.
- **ABAC** - (Attribute Based Access Control) is where access to objects is granted based on subjects, objects, and environmental conditions.
    - Attributes could be:
        - Subject (user) – Name, role, ID, clearance, etc.
    - Object (resource) – Name, owner, and date of creation.
    - Environment – Location, and/or time of access, and threat levels.
- **RUBAC** - (Rule Based Access Control) is access that's granted based on IF/THEN statements.

- **Bell-LaPadula: (Confidentiality)** (Mandatory Access Control):
    - **Simple Security Property** "No Read UP".
        - Subjects with Secret clearance can't read Top Secret data.
    - *** Security Property:** "No Write DOWN".
        - Subjects with Top Secret clearance can't write Top Secret information to Secret folders.
    - **Strong * Property:** "No Read or Write UP and DOWN".
        - Subjects can ONLY access data on their own level.
- **BIBA: Integrity** (Mandatory Access Control):
    - **Simple Integrity Axiom:** "No Read DOWN".
        - Subjects with Top Secret clearance can't read Secret data.
        - Remember that integrity is the purpose here; we don't want to have wrong or lacking lower clearance level data confuse us.

    - *** Integrity Axiom:** "No Write UP".
        - Subjects with Secret clearance can't write Secret information to Top Secret folders.
        - We don't want wrong or lacking lower-level information to propagate to a higher level.

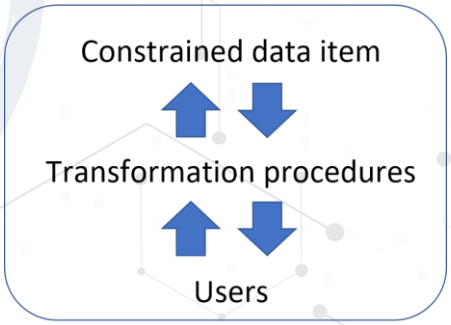
    - **Invocation Property:** "No Read or Write UP".
        - Subjects can never access or alter data on a higher level.

- **Lattice Based Access Control (LBAC) (MAC):**
    - A subject can have multiple access rights.
        - A Subject with "Top Secret" {crypto, chemical} would be able to access everything in this lattice.
        - A Subject with "Secret" {crypto} would only have access to that level.
        - A subject with "Top Secret" {chemical} would have access to only {chemical} in Top Secret and Secret.
    - These are obviously vastly more complex in real life.
    - For the exam, just know what they are and how they work.



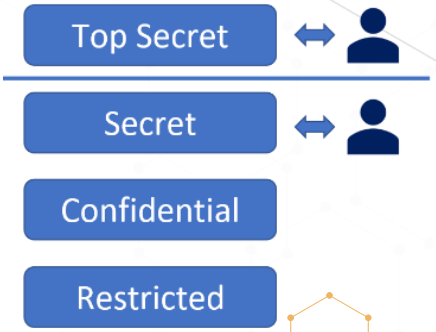
- **Graham-Denning Model** – uses Objects, Subjects, and Rules.
  - The 8 rules that a specific subject can execute on an object are:
    1. Transfer Access.
    2. Grant Access.
    3. Delete Access.
    4. Read Object.
    5. Create Object.
    6. Destroy Object.
    7. Create Subject.
    8. Destroy Subject.

- **HRU** model (Harrison, Ruzzo, Ullman):
  - An operating system level computer security model that deals with the integrity of access rights in the system.
  - It is an extension of the Graham-Denning model, based around the idea of a finite set of procedures being available to edit the access rights of a subject on an object.
  - Considers Subjects to be Objects too (unlike Graham-Denning).
  - Uses six primitive operations:
    - Create object.
    - Create subject.
    - Destroy subject.
    - Destroy object.
    - Enter right into access matrix.
    - Delete right from access matrix.



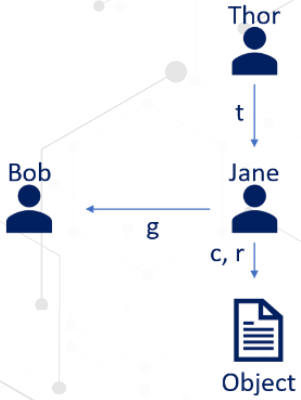
- **Clark-Wilson - Integrity:**
  - Separates end users from the back-end data through 'Well-formed transactions' and 'Separation of Duties'.
  - The model uses Subject/Program/Object.
    - We have discussed the Subject/Object relationship before, but this puts a program between the two.
    - We don't allow people access to our inventory when they buy from us.
    - We give them a limited functionality interface they can access.
  - **Separation of duties:**
    - The certifier of a transaction and the implementer are different entities.
    - The person making purchase orders should not be paying the invoices.
  - **Well-formed transactions** are a series of operations that transition a system from one consistent state to another consistent state.

- **Brewer-Nash** (Chinese Wall or Information Barriers):
  - Designed to provide controls that mitigate conflict of interest in commercial organizations and is built upon an information flow model.
  - No information can flow between the subjects and objects in a way that would create a conflict of interest.



- **Non-Interference Model:**
  - Ensures that any actions that take place at a higher security level do not affect or interfere with actions that take place at a lower level.
  - The model is not concerned with data flow, but with what a subject knows about the state of the system.
  - Any changer by a higher-level subject will never be noticed by a lower-level subject.

- **Take-Grant Protection Model:**
  - Uses rules that govern the interactions between subjects and objects.
  - It uses permissions that subjects can grant to (or take from) other subjects.
  - It has 4 rules:
    - **Take** rule allows a subject to take rights of another object.
    - **Grant** rule allows a subject to grant own rights to another object.
    - **Create** rule allows a subject to create new objects.
    - **Remove** rule allows a subject to remove rights it has over another object.



  - Thor can Take (t) Jane's rights for the object.
  - Jane can Create (c) and Remove (r) rights for the object.
  - Jane can Grant (g) any of her rights to Bob.
- **Access Control Matrix:**
  - Model describing the rights of every subject for every object in the system.
  - An access matrix is like an Excel sheet.
    - One row per subject.
    - One column per object.
    - The **rows** are the rights of each subject, each row is called a capability list.
    - The **columns** show the ACL (Access Control List) for each object or application.

Subject/Object	Object #1	Object #2	Object #3
Thor	Read	Read, Write	Full Control
Jane	Full Control	Read	No access
Bob	No Access	Full Control	Read, Write

- **Zachman Framework** (for Enterprise Architecture):
  - Provides six frameworks:
    - What, How, Where, Who, When, and Why.
  - Mapping those frameworks to rules for:
    - Planner, Owner, Designer, Builder, Programmer, and User.

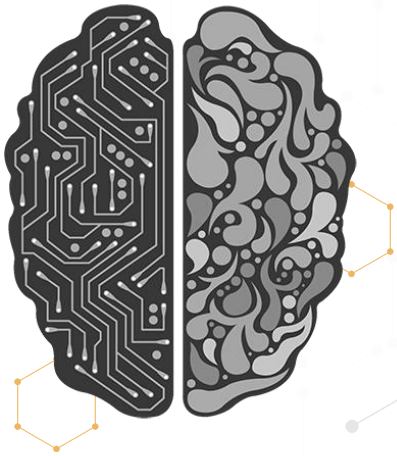
- **Security Modes** - can be MAC or DAC (Mandatory or Discretionary Access Control):
  - The systems contain information at various levels of security classification.
  - **The mode is determined by:**
    - The type of users who will be directly or indirectly accessing the systems.
    - The type of data, including classification levels, compartments, and categories that are processed on the system.
    - The type of levels of users, their need to know, and formal access approvals that the users will have.

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (*Contextual*) *→ Role: Planner*	List of Things important in the Business	List of Core Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goals/Strategies
Enterprise Model (*Conceptual*) *→ Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (*Logical*) *→ Role: Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (*Physical*) *→ Role: Builder*	Physical Data/ Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Representations (*Out of Context*) *→ Role: Programmer*	Data Definitions	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
Functioning Enterprise *→ Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

  - **Dedicated security mode** - All users must have:
    - Signed NDA for ALL information on the system.
    - Proper clearance for ALL information on the system.
    - Formal access approval for ALL information on the system.
    - A valid need to know for ALL information on the system.
    - users can access ALL data.
  - **System High Security Mode -** All users must have:
    - Signed NDA for ALL information on the system.
    - Proper clearance for ALL information on the system.
    - Formal access approval for ALL information on the system.
    - A valid need to know for SOME information on the system.
    - All users can access SOME data, based on their need to know.

  - **Compartmented Security Mode** - All users must have:
    - Signed NDA for ALL information on the system.
    - Proper clearance for ALL information on the system.
    - Formal access approval for SOME information they will access on the system.
    - A valid need to know for SOME information on the system.
    - All users can access SOME data, based on their need to know and formal access approval.
  - **Multilevel Security Mode** - (Controlled Security Mode) - All users must have:
    - Signed NDA for ALL information on the system.
    - Proper clearance for SOME information on the system.
    - Formal access approval for SOME information on the system.
    - A valid need to know for SOME information on the system.
    - All users can access SOME data, based on their need to know, clearance and formal access approval.

Artificial Intelligence



- Intelligence exhibited by machines, rather than humans or other animals.
- What true AI is, is a topic of discussion, what was considered AI years ago we have achieved and when once goal is reached the AI definition is tweaked a little.
- From what we are seeing published we do in my mind not currently have true AI, but very highly simulated intelligence, that being said IBM and Google do seem to be getting a lot closer.
- It is also used when a machine mimics cognitive functions that humans associate with other human minds, such as learning and problem solving.
- AI currently defined as advice that perceives its environment and takes actions that maximize its chance of success at some goal, not through experience/programming, but through reasoning.
- **Expert systems:**
    - A computer system that emulates the decision-making ability of a human expert.
    - Designed to solve complex problems by reasoning about knowledge, represented mainly as if–then rules rather than through conventional procedural code.
    - An expert system is divided into two subsystems:
        - The knowledge base represents facts and rules.
        - The inference engine applies the rules to the known facts to deduce new facts and can also include explanation and debugging abilities.
- **ANN's (Artificial neural networks):**
    - Computing systems inspired by the biological neural networks that constitute animal brains, we make decisions based on 1000's of memories, stories, the situation and many other factors, the ANN tries to emulate that.
    - The systems learn and progressively improve their performance, to do tasks, generally without task-specific programming.
    - They can learn to identify images that contain geckos by analyzing example images that have been manually labeled as "gecko" or "no gecko" and using the analytic results to identify geckos in other images.
    - They are mostly used in areas that are difficult to express in a traditional computer algorithm using rule-based programming.
    - An ANN is based on a collection of connected units called artificial neurons.
    - Each connection (synapse) between neurons can transmit a signal to another neuron.
    - Typically, neurons are organized in layers, different layers may perform different transformations on their inputs.
    - Signals travel from the first input to the last output layer, at times after traversing the layers multiple times.

- **GP (Genetic Programming):**
  - A technique where computer programs are encoded as a set of genes that are then modified (evolved) using an evolutionary algorithm often a GA (Genetic Algorithm).
  - The results are computer programs able to perform well in a predefined task.
  - The methods used to encode a computer program in an artificial chromosome and to evaluate its fitness with respect to the predefined task are central in the GP technique and still the subject of active research.
  - GP evolves computer programs, traditionally represented in memory as tree structures.
  - Trees can be easily evaluated in a recursive manner.
  - Every tree node has an operator function, and every terminal node has an operand, making mathematical expressions easy to evolve and evaluate.
  - Traditionally GP favors the use of programming languages that naturally embody tree structures for example, Lisp or other functional programming languages.

What we covered in Domain 1

- Congratulations on finishing Domain 1: Information Security governance. This is the CISM foundation.
- 17% of the exam questions on the certification are from this domain.

- We will be covering our govern, our values, vision, mission, our strategies, policies, standards, and processes.
- We look at the policies, the procedures, the laws we need to adhere to.
- Data protection, the NIST Cyber Security framework, NIST Risk management framework, NIST 800-37, 800-53, ISO 27001 and 27002
- We talked about the CIA triad, which is the foundation of Information Security
- Administrative security controls, roles, and responsibilities.

- This should be what you are tested on for Domain 1 until the next planned CISM curriculum change in 2027.