

Security and Risk Management

Welcome to the first Domain.

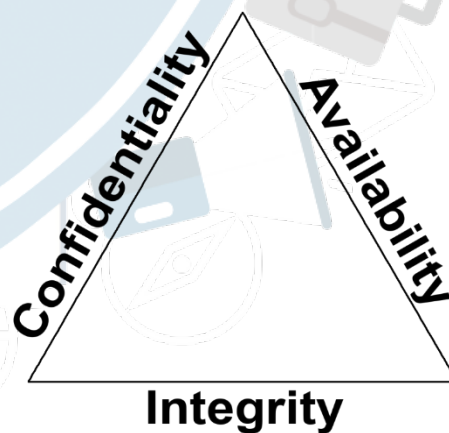
- This domain is **VERY** important because:
 - Every other knowledge domain build on top of this chapter
 - This is the **foundation**.
- This domain is very testable.
 - I think they are weighted high.
- IT Security should be based on a cost benefit analysis.
 - What will a compromise cost us?
 - How likely is a compromise?
 - What will the countermeasure cost us?
- We want EXACTLY enough security and to base it on the ROI from the cost benefit analysis.

Security, Risk, Compliance, Law, Regulations, and Business Continuity.

- **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.
- **Compliance.**
- **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 analysis:**
 - How we determine the quantitative and qualitative risks to our assets, and types of attackers.

Confidentiality, Integrity and Availability.

- **The CIA Triad (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.



Security and Risk Management

- 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.

- **System integrity and Data integrity**
 - **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).

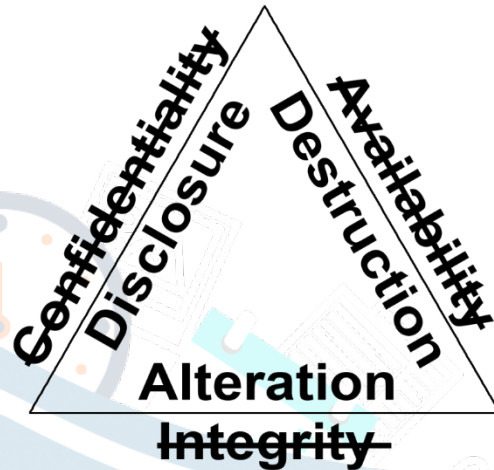
Confidentiality, Integrity and Availability.

- **System integrity and Data availability.**
 - **We use:**
 - IPS/IDS.
 - Patch Management.
 - Redundancy on hardware power (Multiple power supplies/UPS'/generators), Disks (RAID), Traffic paths (Network design), HVAC, staff, HA (high availability) and much more.
 - SLA's – How high uptime to we want (99.9%?) – (ROI)
 - **Threats:**
 - Malicious attacks (DDOS, physical, system compromise, staff).
 - Application failures (errors in the code).
 - Component failure (Hardware).

Security and Risk Management

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 is 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.



IAAA (Identification and Authentication, Authorization and Accountability):

- **Identification**
 - Your name, username, ID number, employee number, SSN etc.
 - “I am Khurram”.
- **Authentication**
 - “Prove you are Khurram”. – 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.).
 - **Somewhere you are** - **Type 4** Authentication (IP/MAC Address).
 - **Something you do** - **Type 5** Authentication (Signature, pattern unlock).

IAAA:

- **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 Domain 5 - Identity and Access Management (DAC, MAC, RBAC, 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 and Risk Management

IT Security is there to Support the organization.

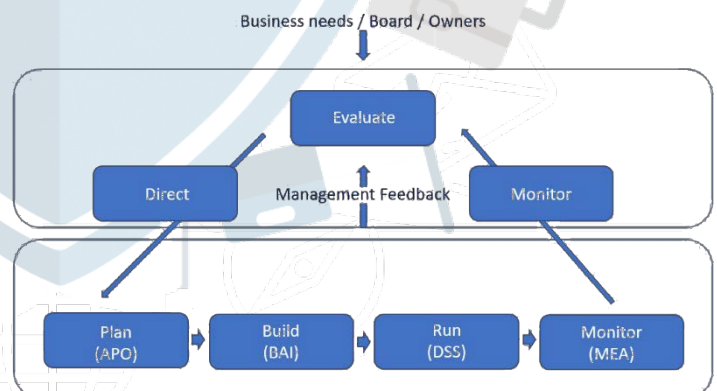
- We are there to enable the organization to fulfil its mission statement and the business' goals.
- We are **not** the most important part of the organization, but we span the entire organization.
- We are Security leaders **and** Business leaders – Answer exam questions wearing BOTH hats.

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.

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.



Security and Risk Management

- 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.

Security governance principles.

- **Top-Down vs. Bottom-Up Security Management and Organization structure.**
 - **Bottom-Up:** IT Security is seen as a nuisance and not a helper, often change 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.
 - **CSO:** Chief Security Officer.
 - **CIO:** Chief Information Officer.
 - **CFO:** Chief Financial Officer.



Normal organizations obviously have more C-Level executives, the ones listed here you need to know.

Security governance principles.

- **Governance standards and control frameworks.**
 - **PCI-DSS** - Payment Card Industry Data Security Standard (While a standard it is required: more on this one later).
 - **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.
 - Analyses one business unit, application or system at a time in a roundtable brainstorm with **internal** employees. Impact analyzed, threats and risks prioritized.

Security governance principles.

- **Governance standards and control frameworks.**
 - **ISO 27000 series:**
 - **ISO 27001:** Establish, implement, control and improvement of the ISMS. Uses PDCA (Plan, Do, Check, Act)

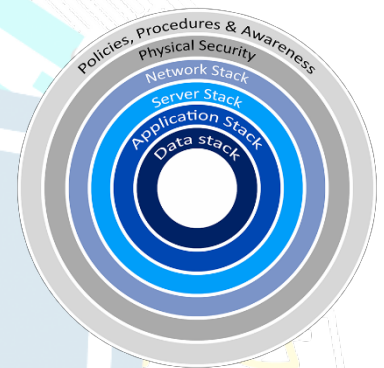
Security and Risk Management

- **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.

Security governance principles.

- **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 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.

As IT Security Professionals we need to understand that laws and regulations have a huge influence on how we work.

We need to know some of them and understand how the rest work.

- There are 4 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.) Proof “More likely than not”.
 - **Private Regulations:**
 - Compliance is required by contract (For instance PCI-DSS).

Security and Risk Management

Legal and regulatory issues.

- **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.

Legal and regulatory issues.

- **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 and with that log files were 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.”

Security and Risk Management

Legal and regulatory issues.

- **Evidence:**
 - **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?

Legal and regulatory issues.

- **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. If not, it is inadmissible in court.
 - Exigent circumstances apply if there is an immediate threat to human life or of evidence destruction.
 - This will later be decided by a court if it was justified.
 - Only applies to law enforcement and those operating under the "color of law" – Title 18. U.S.C. Section 242 – Deprivation of Rights Under the Color of Law.
 - Your organization needs to be very careful when ensuring that employees are made aware in advance that their actions are monitored, that their equipment, and maybe even personal belongings, can be subjected to searches.
 - Notifications like that should only be made if your organization has security policies in place for it, and it must take into account the privacy laws in your county/state/country.

Legal and regulatory issues.

- **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.
 - Openly advertising sensitive data and then charging people when they access them.
 - Entrapment is a solid legal defense.

Security and Risk Management

- **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.
 - Have open ports or services on a server that can be attacked.
 - Enticement is not a valid defense.
- 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.

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

GDPR (General Data Protection Regulation):

- **Restrictions:** Lawful interception, national security, military, police, justice.
- **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.

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.

Legal and regulatory issues.

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 a organization can do nothing if their Trade Secret is discovered, *how* it is done can be illegal.
- **Cyber Squatting** – Buying an URL you know someone else will need (To sell at huge profit – not illegal).
- **Typo Squatting** – Buying an URL that is VERY close to real website name (Can be illegal in certain circumstances).

Legal and regulatory issues.

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.)

Legal and regulatory issues.

Rules, Regulations and Laws you should know for the exam (US):

- **HIPAA** (Not HIPPA) – Health Insurance Portability and Accountability Act.
 - Puts strict privacy and security rules on how PHI (Protected Health Information) is handled by health insurers, providers and clearing house agencies (Claims)).
 - HIPAA has 3 rules – Privacy rule, Security rule and Breach Notification rule.
 - The rules mandate Administrative, Physical and Technical safeguards.
 - Risk Analysis is required.
- **Security Breach Notification Laws.**
 - NOT Federal, 48 states have individual laws, know the one for your state (none in Alabama and South Dakota).
 - They normally require organizations to inform anyone who had their PII compromised.
 - Many have an encryption clause.
 - Lost encrypted data may not require disclosure.

Legal and regulatory issues.

Rules, Regulations and Laws you should know for the exam (US):

- **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.
 - Enacted in 1986 and amended in 1989, 1994, 1996, 2001, 2002 (PATRIOT Act), and 2008 (Identity Theft Enforcement and Restitution Act).

Legal and regulatory issues.

Rules, Regulations and Laws you should know for the exam (US):

- **Gramm-Leach-Bliley Act (GLBA):**
 - Applies to financial institutions; driven by the Federal Financial Institutions Examination Council (FFIEC), enforced by member agencies, OCC, FDIC, FRB, NCUA, and CFPB.

- Enacted in 1999, requires protection of the confidentiality and integrity of consumer financial information.
- **Sarbanes-Oxley Act of 2002 (SOX):**
 - Directly related to the accounting scandals in the late 90's.
 - Regulatory compliance mandated standards for financial reporting of publicly traded companies.
 - Intentional violations can result in criminal penalties.

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.

Legal and regulatory issues.

Rules, Regulations and Laws you should know for the exam (EU):

- **EU Data Protection Directive**
 - Very aggressive pro-privacy law.
 - Organizations must notify individuals of how their data is gathered and used.
 - Organizations must allow for opt-out for sharing with 3rd parties.
 - Opt-in is required for sharing “most” sensitive data.
 - No transmission out of EU unless the receiving country is perceived to have adequate (equal) privacy protections; the US does NOT meet this standard. EU-US Safe Harbor, optional between organization and EU.

Legal and regulatory issues.

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
 - Eight driving principles:
 - Collection limitation principle: Collection of personal data should be limited, obtained by lawful and fair means, and with the knowledge of the subject.
 - Data quality principle: Personal data should be kept complete and current and be relevant to the purposes for which it is being used.
 - Purpose specification principle: Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose.
 - Use limitation principle: Only with the consent of the subject or by the authority of law should personal data be disclosed, made available, or used for purposes other than those previously stated.

Legal and regulatory issues.

Organization for Economic Cooperation and Development (OECD) Privacy Guidelines (International):

- Eight driving principles (continued):
 - Security safeguards principle: Reasonable safeguards should be put in place to protect personal data against risks such as loss, unauthorized access, modification, and disclosure.
 - Openness principle: Developments, practices, and policies regarding personal data should be openly communicated. In addition, subjects should be able to easily establish the existence and nature of personal data, its use, and the identity and usual residence of the organization in possession of that data.
 - Individual participation principle: Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so.
 - Accountability principle: Organizations should be accountable for complying with measures that support the previous principles.

Legal and regulatory issues.

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.

Legal and regulatory issues.

3rd party, Acquisitions and Divestiture security.

- 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 an **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?
- **Divestitures:** Your organization is being split up.
 - How do you ensure no data crosses boundaries it shouldn’t? Who gets the IT Infrastructure?

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 principles.
 - Advance and protect the profession.

Ethics:

- **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.

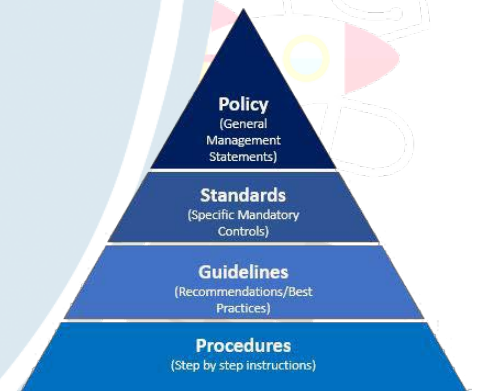
- Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethics:

- **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 don't, how can you adhere to it?

Information Security Governance:

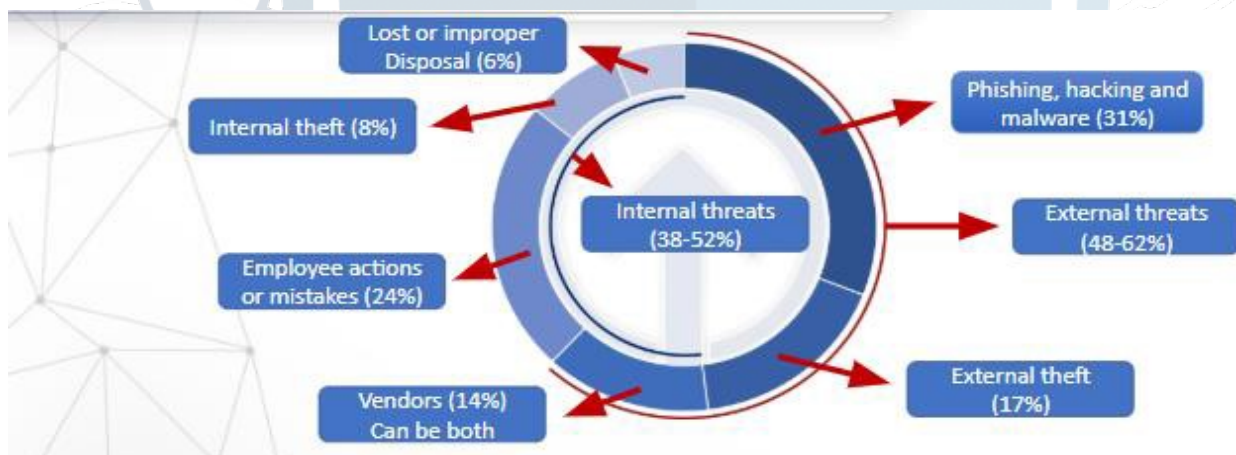
- **Policies – Mandatory.**
 - High level, non-specific.
 - They can contain "Patches, updates, strong encryption"
 - They will not be specific to "OS, encryption type, vendor Technology"
- **Standards – Mandatory.**
 - Describes a specific use of technology (All laptops are W10, 64bit, 8gig memory ...)
- **Guidelines – non-Mandatory.**
 - Recommendations, discretionary – Suggestions on how you would 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.



Information Security Governance:

- **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 Defensive Categories and Types:

- **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 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? This is a vague guess or a feeling, and relatively quick to do. Most often done to know where to focus the Quantitative Risk Analysis.
 - **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.

Risk Analysis:

- **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?
 - 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 to quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to “Low” or “Medium”.

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

Risk Analysis:

- Quantitative Risk Analysis** – We want exactly enough security for our needs.
 - This is where we put a number on that.
 - 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 Value 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 cost per year if we do nothing.
 - Total Cost of Ownership (**TCO**) – The mitigation cost: upfront + ongoing cost (Normally Operational)

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	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
	Rare	L	L	M	H	H

Let’s look at a few examples.

Risk Analysis:

Quantitative Risk Analysis

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)
compromised (EF)
Loss per laptop is \$10,000 (AV) x 100% EF) = (SLE)
= (SLE)
The organization loses 25 Laptops Per Year (ARO)
(ARO)

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
Loss per Flooding is \$10,000,000 (AV) x 15% EF)
The flooding happens every 4 years = 0.25

The annualized loss is \$250,000 (ALE)

The annualized loss is \$375,000 (ALE)

Risk Analysis:

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 $25 \times \$9,000 = \$225,000$ by spending \$57,750.

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

Risk Analysis:

- **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). We ensure we have a paper trail, and this was a calculated decision.
- **Mitigate the Risk (Reduction)** – The laptop encryption/wipe is an example – acceptable level (Leftover risk = Residual).
- **Transfer the Risk** – The insurance risk approach – We could get flooding insurance for the data center, the flooding will still happen, we will still lose 15% of the infrastructure, but we are insured for cost.
- **Risk Avoidance** – We don't issue employees laptops (if possible) or we build the data center in an area that doesn't flood. (Most often done before launching new projects – this could be the data center build).
- **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 is area 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.

Risk Analysis:

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).

Risk Analysis:

- **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. They often just publicize the vulnerability (which can lead to black hats using it before a patch is developed). Gray hats sometimes also approach the company with the vulnerability and ask them to fix it and if nothing happens, they publish.
- **Script Kiddies:**
 - They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use. They pose a very real threat. They are just as dangerous as skilled hackers; they often have no clue what they are doing.

Risk Analysis:

Types of attackers:

- **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.

Risk Analysis:

Types of attackers:

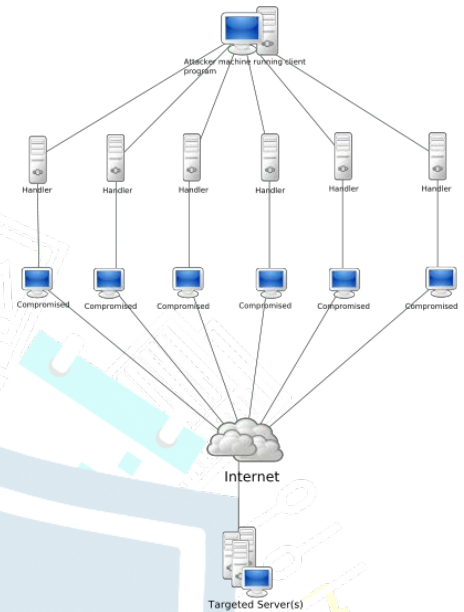
- **Hacktivism/Hacktivist (hacker activist):** Hacking for political or socially motivated purposes.
 - Often aimed at ensuring free speech, human rights, freedom of information movement.
 - Famous attacks: Anonymous – DDOS attack on Visa, Mastercard, PayPal to protest the arrest of Julian Assange (WikiLeaks). Google/Twitter/SayNow worked together to provide communication for the Egyptian people when the government orchestrated an internet blackout during the 2011 protests.
- **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), ...

Risk Analysis:

Types of attackers:

- **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 be used to send spam emails.
- **Botnets** is a C&C (Command and Control) network, controlled by people (bot-herders).
 - There can often be 1,000's or even 100,000's of bots in a botnet.



Risk Analysis:

Types of attackers:

- **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.
 - A public treasurer in Michigan sent \$1.2m to Nigeria (\$1.1m of taxpayer funds and \$72,000 of his own).
 - **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.

Risk Analysis:

