Thor's Quick Sheets – CISSP® Domain 1

Contents

Thor's Quick Sheets – CISSP® Domain 1

The CIA Triad

Confidentiality: We keep our data and secrets secret. We ensure no one unauthorized can access the data.
Disclosure: The opposite of Confidentiality.
Integrity: How we protect against modifications of the data and the systems. We ensure the data has not been altered.
Alteration: The opposite of Integrity.
Availability: We ensure authorized people can access the data they need when they need to.
Destruction: The opposite of Availability.

IAAA

Identification: Your name, username, ID number, employee number, SSN, etc. **"I am Thor."**
Authentication: "Prove you are Thor." It should always be done with multi-factor authentication!

- Something you know: **Type 1** Authentication (passwords, passphrase, PIN, etc.).
- Something you have: **Type 2** Authentication (ID, passport, smart card, token, cookie on PC, etc.).
- Something you are: **Type 3** Authentication (Biometrics) (Fingerprint, iris scan, facial geometry, etc.).

Authorization: What is Thor allowed to access?

- We use Access Control models; what and how we implement depends on the organization and what our security goals are.

Accountability (**Auditing**): We trace an Action to a Subject's Identity; **what did Thor do?**

- Prove who/what a given action was performed by (non-repudiation).

Security Governance Principles

Least Privilege: We give our 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.
Subject: (Active) Most often users but can also be programs. Subject manipulates Object.
Object: (Passive) Any passive data (both physical paper and data). The Object is manipulated by the Subject. Some can be both at different times; an active program is a subject; when closed, the data in the program can be an Object.
Governance: This is C-level (Not you). They decide our 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 will we practically work with our risk appetite and our environment.
PCI:DSS: Payment Card Industry Data Security Standard.
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. Analyze one business unit, app, or system at a time in brainstorming with internal employees. The impact is analyzed, and the threats and the risks are prioritized.
ISO 27001: Establish, implement, control, and improve the ISMS. (**Plan, Do, Check, Act**).

ISO 27002: (From BS 7799, 1/2, ISO 17799) Provides practical advice on implementing security controls. It has ten 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 protecting PHI (Protected Health Information).

Types of Laws and Definitions

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, HIPAA, FAA, etc.).
Private Regulations: Requires compliance by contract. (For instance, PCI-DSS).
Customary Law: Mostly handles personal conduct and behavior patterns founded on the traditions and customs of the area or region.
Religious Law: Based on the religious beliefs in that area or country, which often upholds and includes a code of ethics and morality.
Liability: If the question is who is **ULTIMATELY** liable, the answer is Senior Leadership, but this does not mean that 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: 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?

- Implement the IT Security architecture; keep systems patched. If compromised, fix the issue, and 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 did NOT perform Due Care, you are most likely liable.

Evidence

Real Evidence: Tangible and physical objects in IT Security: Hard **disks**, USB drives; NOT the data.
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.
Hearsay: Not first-hand knowledge, normally inadmissible in a case. Computer-generated records (logs) are considered hearsay, but case law and updates to the Federal Rule of Evidence have changed that.
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.
Entrapment (Illegal and unethical): When someone is persuaded to commit a crime, they have no intention of committing and is then charged with it.

Intellectual Property

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.
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 ten 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. If discovered, anyone can use it; you are not protected.

Laws and Regulations

HIPAA (Not HIPPA): Health Insurance Portability and Accountability Act. Strict privacy and security rules on the handling of PHI (Protected Health Information).
Security Breach Notification Laws: NOT Federal. All 50 states have individual laws; know your state. **Electronic Communications Privacy Act (ECPA):** Protection of electronic communications against warrantless wiretapping. The Act was weakened by the Patriot Act.
PATRIOT Act of 2001: Expands law enforcement electronic monitoring capabilities and allows search and seizure without immediate disclosure.
Computer Fraud and Abuse Act (CFAA): The most commonly used law to prosecute computer crimes.
Gramm-Leach-Bliley Act (GLBA): Applies to financial institutions; 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.
GDPR: 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.
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.
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".**

Thor's Quick Sheets – CISSP® Domain 1

Third-party Software, Acquisitions, and Divestitures

Procurement: We buy products or services; security is designed in and not an afterthought.
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 we ensure no data crosses boundaries it should not? Who gets the IT Infrastructure?

ISC2 Code of Ethics

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.

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?

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 W10, 64bit, 8gig memory, …)
Guidelines: Non-mandatory. Recommendations, discretionary: Suggestions on how you implement 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.

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, the credit history (less common, more costly). We have new staff sign an NDA.
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.

Thor's Quick Sheets – CISSP® Domain 1

Access Control Categories and Types

Administrative (Directive): Org. policies/procedures, regulation, training, and awareness.
Technical: Hardware/software/firmware; firewalls, routers, encryption, ...
Physical: Locks, fences, guards, dogs, gates, bollards, ...
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 when other controls are impossible or too costly.

Risk Management

The Risk Management lifecycle is iterative.
Risk Identification:

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

Risk Assessment:

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

It is impossible to eliminate risk 100%, we can mitigate it to an acceptable level.
Risk Response and Mitigation:

- Risk mitigation, transference, acceptance, or avoidance. We act on senior management's choices, which they made based on our recommendations from the assessment phase.
- Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?
- We update the risk register with the mitigations of the chosen risk responses and see if the new risk level is acceptable.

Risk and Control Monitoring and Reporting:

- The process is ongoing, we must keep monitoring both the risk and the controls we implemented.
- You are the translating link; you must be able to explain IT and IT Security to Senior Management in terms they can understand. It is normal to do the Risk Management lifecycle annually and do out-of-cycle Risk Management on critical items.

Qualitative Risk Analysis: How likely is it to happen, and how bad is it if it happens?
Quantitative Risk Analysis: What will it actually cost us in $? This is fact-based analysis. Total $value of the 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, …

Impact: Can at times be added to give a full picture.
Risk = Threat x Vulnerability x Impact (How bad is it?).
Total Risk = **Threat x Vulnerability x Asset Value.**
Residual Risk = **Total Risk - Countermeasures**.
Asset Value (AV): How much is the asset worth?
Exposure factor (EF): Percentage of asset lost?
Single Loss Expectancy (SLE) = (AV x EF): What does it cost if it happens once?
Annual Rate of Occurrence (ARO): How often will this happen each year?
Annualized Loss Expectancy (ALE): This is what it costs per year if we do nothing **(ALE = SLE x ARO).**
Total Cost of Ownership (TCO): The mitigation cost: upfront + ongoing cost (Normally Operational)**.**

Types of Risk Responses

Accept the Risk: We know the risk is there. The mitigation is more costly than the (low) risk cost.
Mitigate the Risk (Reduction): We reduce the risk to an acceptable level (Leftover risk = Residual).
Transfer the Risk: The insurance risk approach.
Risk Avoidance: We don't issue employees laptops (if possible) or build the data center in an area that doesn't flood.
Risk Rejection: You know the risk is there; you ignore it. This is never acceptable (You are liable).
Secondary Risk: Mitigating one risk may open up another risk.

KGIs, KPIs, and KRIs

KGI (Key Goal Indicator): 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 a potential event that may harm the continuity of the activity/project.

Types of Attackers

Hackers: Now: Anyone trying to get access to or disrupt any leg of the CIA Triad (Confidentiality, Integrity, and 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.
Gray/Grey Hat Hackers: They are somewhere between the white and black hats. They go looking for vulnerable code, systems, or products.
Script Kiddies: They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use.
Outsiders: Unauthorized individuals trying to gain access; launch most 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.

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.

Hacktivism/Hacktivist (hacker activist): Hacking for political or socially motivated purposes. Often aimed at ensuring free speech, human rights, freedom of information movement.
Governments: State-sponsored hacking is common; often, you see the attacks happening between 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 and government computer systems and utilities.
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.

Phishing, Spear Phishing, and more

Phishing (Social engineering email attack): Click to win, Send information to get your inheritance, …
Sent to hundreds of thousands of people; if just 0.02% follow the instructions, they have 200 victims.
Spear Phishing: Targeted phishing, not just random spam, but targeted at specific individuals.
Sent with knowledge about the target (person or company); familiarity increases success.
Whale Phishing (Whaling): Spear phishing targeted at senior leadership of an organization. This could be "Your company is being sued if you don't fill out the attached documents (with trojan in them) and return them to us within two 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.
Smishing: Short Message Service (SMS) phishing or smishing is phishing using text messages.

Developing our BCP

- Process of creating long-term strategic business plans, policies, and procedures for continued operation after a disruptive event.
- For **the entire organization**, it is everything that could be impacted, not just IT.
- Lists a range of disaster scenarios and the steps the organization must take in any particular scenario to return to regular operations. We look at what we would do if a critical supplier closed, the facility was hit by an earthquake, what if we were snowed in and staff couldn't get to work, ...
- They are written ahead of time, and continually improved upon. It is an iterative process.
- We write the BCP with input from key staff and at times, outside BCP consultants.

BCP Phases:
Project Initiation: Project start, identify stakeholders, C-level approval, formalize project.
Scope the Project: We identify exactly what we are trying to do and what we are not.
Business Impact Analysis: We identify and prioritize critical systems and components.
Identify Preventive Controls: We identify current/possible preventative controls we can deploy.
Recovery Strategy: How do we recover efficiently? What are our options? DR site, system restore, cloud, ...
Plan Design and Development: We build a specific plan for recovery from a disaster, procedures, guidelines, and tools.
Implementation, Training, and Testing: We test the plan to find gaps and train staff to act on the plan.

BCP/DRP Maintenance: It is an iterative process. Our organization develops additional systems, facilities, or technologies, and the threat landscape constantly changes. We have to keep improving and tweaking our BCP and DRP.

Senior management **needs to be involved** and committed to the BCP/DRP process. They need to be part of at least the initiation and the final approval of the plans.

BIA (Business Impact Analysis):
Identifies critical and non-critical organization systems, functions, and activities. Critical is where disruption is considered unacceptable, the acceptability is also based on the cost of recovery. A function may also be considered critical if dictated by law. For each critical (in scope) system, function, or activity, two values are then assigned:
RPO (Recovery Point Objective): The acceptable amount of data that cannot be recovered.
The RPO must ensure that the maximum tolerable data loss for the system, function, or activity is not exceeded.
MTD (Maximum Tolerable Downtime) **MTD ≥ RTO + WRT**: System rebuild time, configuration, and reinsertion into production must be less than or equal to our MTD. The total time a system can be inoperable before our organization is severely impacted.

- **RTO** (Recovery Time Objective): The amount of time it takes to restore the system (hardware). The recovery time objective must ensure that the MTD for each system, function, or activity is not exceeded.
- **WRT** (Work Recovery Time): How much time is required to configure a recovered system (software).

MTBF (Mean Time Between Failures): How long will a new or repaired system/component function on average.
MTTR (Mean Time to Repair): How long it will take to recover a failed system.
MOR (Minimum Operating Requirements): The minimum requirements for our critical systems to function.