Module III:
Information Security Policies, Procedures, Standards and Guidelines

Prepared by
Dr. P. Vijayakumar
Associate professor / SENSE
VIT Chennai

Content

- **Information Security Policies**
- **Key Elements of Security Policy**
- **Security Standards** Guidelines & Frameworks
- Security Standards Organizations
- Information Security Laws
- Regulations and Guidelines

Information Security Policies

- Security policies are the **foundation** of your security infrastructure.

- Without them, you **cannot protect your company** from possible lawsuits, lost revenue and bad publicity, not to mention basic security attacks.

- A security policy is a **document or set of documents** that describes, at a high level, the security controls that will be implemented by the company.

Policies are not technology specific and do three things for an organisation:

- **Reduce** or eliminate legal liability to employees and third parties.

- **Protect confidential**, proprietary information from theft, misuse, unauthorized disclosure or modification.

- **Prevent waste** of company computing resources.

- Organisations are **giving more priority** to development of information security policies, protecting their assets is one of the prominent things that needs to be considered.

- **Lack of clarity in InfoSec policies** can lead to catastrophic damages which cannot be recovered.

- An information security policy provides **management direction and support for information security** across the organisation.

There are two types of basic security policies:

- **Technical security policies:** these include **how technology should be configured and used.**

- **Administrative security policies**: these include how people (**both end users and management**) should behave/ respond to security.

Persons responsible for the implementation of the security policies are:

- Director of Information Security
- Chief Security Officer
- Director of Information Technology
- Chief Information Officer

- Information in an organisation will be **both electronic and hard copy,** and this information needs to be secured properly against the consequences of breaches of confidentiality, integrity and availability.

- Proper security measures need to be implemented **to control and secure information from unauthorized changes**, **deletions and disclosures**.

- To find the level of security measures that need to be applied, a **risk assessment is mandatory**.

- Security policies are intended to define **what is expected from employees within an organisation** with respect to information systems.

- The objective is to **guide or control** the use of systems to reduce the risk to information assets.

- It also gives the **staff who are dealing** with information systems an acceptable use policy, explaining what is allowed and what not.

- **Security policies of all companies are not same**, but the key motive behind them is to protect assets.

- Security policies are **tailored to the specific mission goals**.

A security policy should determine rules and regulations for the following systems:

- Encryption mechanisms
- Access control devices
- Authentication systems
- Firewalls
- Anti-virus systems
- Websites
- Gateways
- Routers and switches
- Necessity of a security policy

- A security policy is that plan that provides for the **consistent application of security principles** throughout your company.

- After implementation, it **becomes a reference guide** when matters of security arise.

- A security policy can provide **legal protection to your company**.

- By specifying to your users exactly how they **can and cannot use the network**, how they should **treat confidential information**, and the proper use of encryption, you are **reducing your liability and exposure** in the event of an incident.

- Security policy provides a **written record of your company’s policies** if there is ever a question about what is and is not an approved act.

- Security policies are often required by **third parties that do business** with your company as part of their due diligence process.

- Some examples of these might be **auditors, customers, partners and investors.**

- Companies that do business with your company, particularly those that will be **sharing confidential data or connectivity to electronic systems**, will be concerned about your security policy

- Most common reasons why companies create security policies today is to **fulfill regulations and meet standards** that relate to security of digital information.

- Once the security policy is implemented, it will be a part of **day-to-day business activities**.

- Security policies that are implemented need to be **reviewed whenever there is an organizational change**.

- **Policies can be monitored** by depending on any monitoring solutions like **SIEM** and the violation of security policies can be seriously dealt with.

- There should also be a **mechanism to report** any violations to the policy.

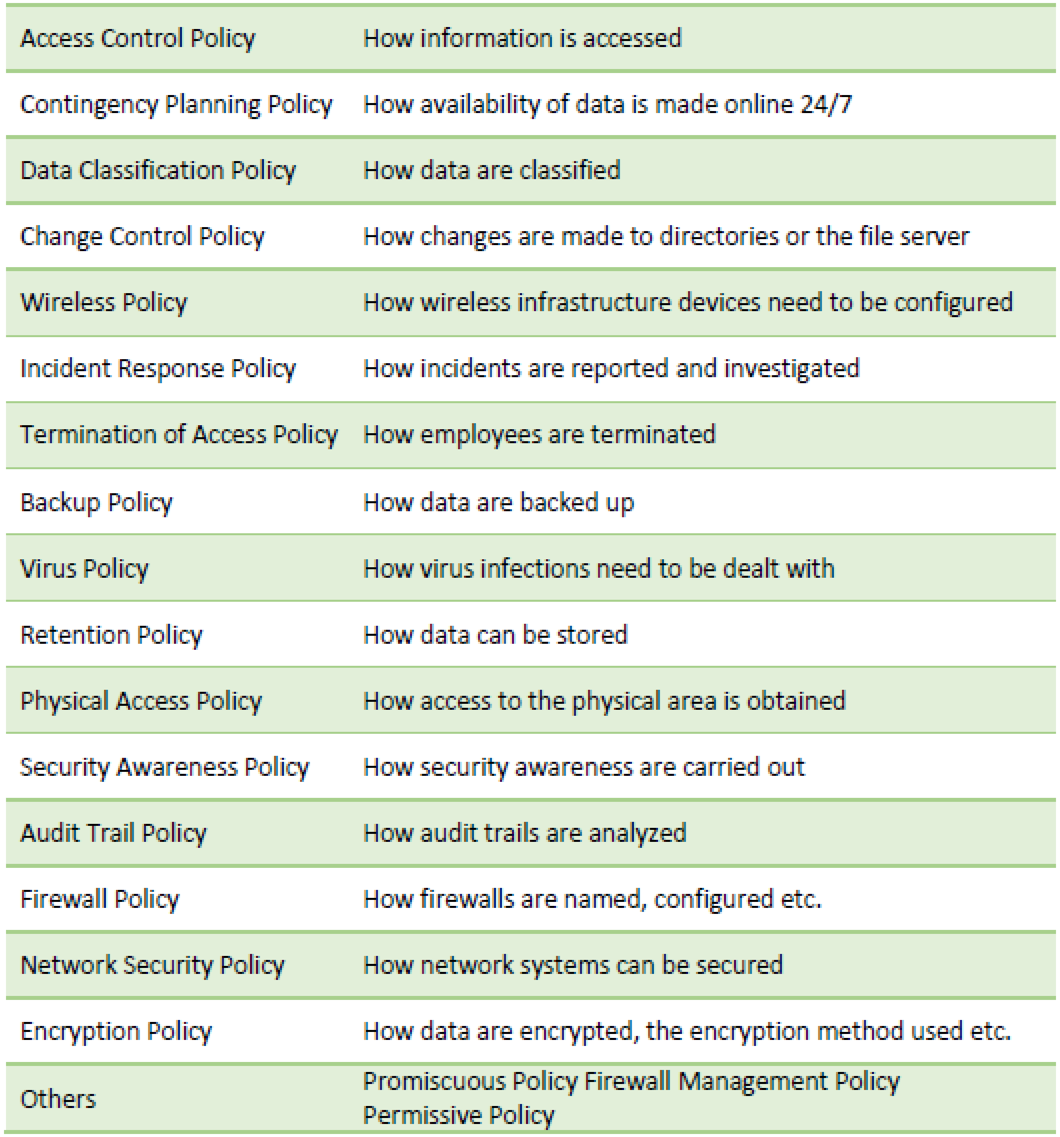
- Develop the policies as **simple** as possible because complex policies are less secure than simple systems.

- Security policies **can be modified at a later time** i.e. not to say that you can create a violent policy now and a perfect policy can be developed some time later.

- It is also mandatory to update the policy based upon the **environmental changes** that an organization goes into when it progresses.

- The policy updates also need to be **communicated with all employees as well as the person** who authorized to monitor policy violations as they may flag for some scenarios which have been ignored by the organization.
- **Management** is responsible for establishing controls and should regularly review the status of controls.

Below is a list of some of the security policies that an organization may have:



Access Control Policy	How information is accessed
Contingency Planning Policy	How availability of data is made online 24/7
Data Classification Policy	How data are classified
Change Control Policy	How changes are made to directories or the file server
Wireless Policy	How wireless infrastructure devices need to be configured
Incident Response Policy	How incidents are reported and investigated
Termination of Access Policy	How employees are terminated
Backup Policy	How data are backed up
Virus Policy	How virus infections need to be dealt with
Retention Policy	How data can be stored
Physical Access Policy	How access to the physical area is obtained
Security Awareness Policy	How security awareness are carried out
Audit Trail Policy	How audit trails are analyzed
Firewall Policy	How firewalls are named, configured etc.
Network Security Policy	How network systems can be secured
Encryption Policy	How data are encrypted, the encryption method used etc.
Others	Promiscuous Policy Firewall Management Policy Permissive Policy

Acceptable Usage Policy

- Acceptable Usage Policy (AUP) is the policy that **one should adhere to while accessing the network**.

- Assets that this policy covers are mobile, wireless, desktop, laptop and tablet computers, email, servers, internet etc.

- For each asset, has to **protect it, manage it**, **authorised persons to use** and administer the asset, accepted methods of communication in these assets etc.

Acceptable Usage Policy

- A template for AUP is published in SANS **http://www.sans.org/securityresources/** policies/Acceptable_Use_Policy.pdf and a security analyst will get an idea of how an AUP actually looks.

- Some of the regulatory compliances mandate that **a user should accept the AUP before getting access** to network devices.

- Implementing these controls makes the organization a bit more **risk free**, even though it is very costly.

- Once a reasonable security policy has been developed, an engineer has to look at the country’s laws, which should be incorporated in security policies.

- One example is the **use of encryption** to create a secure channel between two entities.

- Some encryption algorithms and their levels (128,192) **will not be allowed** by the government for a standard use.

- **Legal experts need to be consulted** if you want to know what level of encryption is allowed in an area.

- This would become a **challenge if security policies are derived for a big organisation** spread across the globe.

Some of the laws, regulation and standards used for policy definition include:

- The PCI Data Security Standard (PCIDSS)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act (SOX)
- The ISO family of security standards
- The Graham-Leach-Bliley Act (GLBA)

Key Elements of Security Policy

A policy should contain:

- **Policy Content** When developing content, many go about creating a policy **exactly the wrong way**.

- The goal is not to create hundreds of pages of impressive looking information, but rather to create an **actionable security plan.**

- The following guidelines apply to the content of successful IT security policies.

Key Elements of Security Policy

- A security policy should be **no longer than** absolutely necessary.

- Policies are **more impressive** when they fill enormous binders or contain hundreds or even thousands of policies.

- These types of policies are frequently advertised on the internet.

- Brevity is of utmost importance.

- A security policy should be written in "**plain English**."

- **Technical topics** will be covered

- Policy be **clear and understood** by the target audience for that particular policy.

- If there is a doubt, the policy should be written so that more people can understand it rather than fewer.

- **Clarity must be a priority** in security policies so that a policy isn't misunderstood during a crisis or otherwise misapplied, which could lead to a critical vulnerability.

- A security policy must be consistent with **applicable laws and regulations.**

- Some states have **specific disclosure laws or regulations governing** the protection of citizens’ personal information, and some industries have regulations governing security policies.

- It is recommended that you **research and become familiar** with any regulations or standards that apply to your company’s security controls.

- A security policy should be **reasonable**.

- The point of this process is to **create a policy that you can actually use** rather than one that makes your company secure on paper but is impossible to implement.

- Keep in mind that the **more secure a policy** is, the **greater the burden** it places on your users and IT staff to comply with.

- Find a middle ground in the balance between security and usability that will work for you.

- A security policy must be **enforceable**.

- A policy should clearly state **which actions are permitted** and which of those are in violation of the policy.

- A policy should spell out enforcement options when non-compliance or violations are discovered, and must be consistent with applicable laws.

- A security policy can be formatted to be consistent with your **company's internal documentation**, however certain information should be placed on each page of the policy.

- At a minimum, this information should include: **policy name, creation date, target audience and a clear designation** that the policy is company confidential.

Security Standards, Guidelines and Frameworks

- **Security governance frameworks** represent solutions to the question of how to manage security effectively.

- The manner in which a company builds a **governance structure** is a reflection of the organization of the company and the laws and business environment in which it finds itself.

- **Auditing the security governance practices** of a company requires understanding how the organization manages the processes and procedures that make up its security program and compare those aspects to recognized governance frameworks.

- An auditor can use to **identify best practices** in building a manageable, measurable and effective security governance program.

COSO

- The Foreign Corrupt Practices Act of 1977 (FCPA) is a law that requires any publicly traded company to **accurately document any transactions or monetary exchanges.**

- The law requires that a publicly traded company also have a system of **internal accounting controls to monitor fraud and abuse and test** them through compliance auditing.

- This law had little guidance from the **Securities and Exchange Commission (SEC)**, and in response to this, a consortium of private organizations created the **Treadway Commission to figure out** what companies needed to do to comply with this law.

- The COSO report lists a few main concepts that **guided the development of the COSO framework** and define what internal controls can and cannot do for an organization.

- These concepts show the **relationship between people and processes** in respect to the effectiveness of controls, and they define the principles with which to implement them.

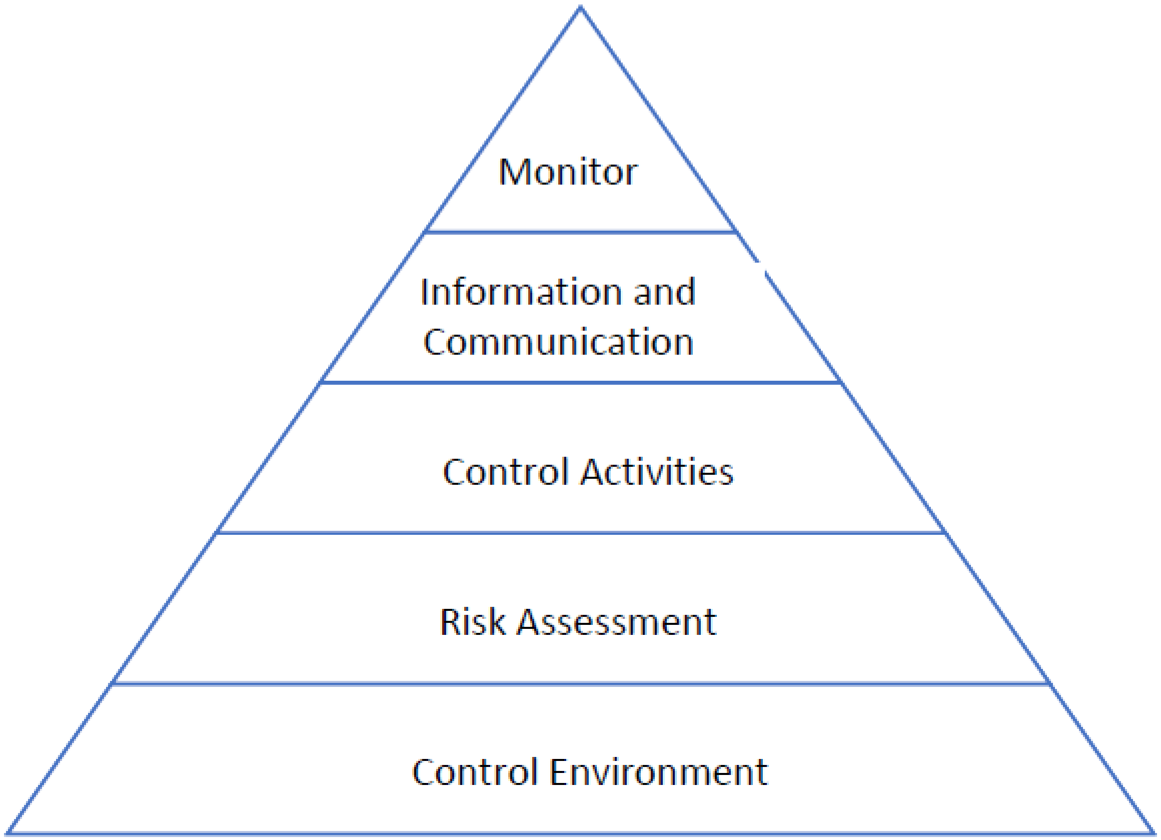
- **Internal control is a process and not a one-time activity.**
- **Internal control is affected by people; it must be adopted through the organization and is not simply a policy document that gets filed away.**
- **An internal control can provide only reasonable assurance, not absolute assurance to the management and board of a business. A control cannot ensure success.**
- **Internal controls are designed for the achievement of business objectives.**

COSO

- The COSO internal controls framework consists of five main control components as seen in the figure below.

- These controls are the foundation of the COSO framework and provide a means for **auditors to assess a company’s** control efficiency, effectiveness, reliability of financial reporting and compliance with the law.

COSO



Monitor

Information and Communication

Control Activities

Risk Assessment

Control Environment

Figure *COSO Internal Controls Framework*

Control environment

- The **control environment** defines how an organization builds its **internal governance program** and affects the company as a whole.

- The CEO, Board of Directors, and Executive Management are mostly involved at this level, **creating the ethics environment and organizational structure** and **defining the roles and responsibilities.**

- The control environment consists of the **people, culture and ethics** of the business.

Risk assessment

- Solid risk assessment methodologies are important to any successful governance program.

- COSO identifies this area as critical to all control development activities and for **identifying business objectives**.

- Risk assessment provides the data to help a company design controls to protect its assets and achieve its strategic goals.

Control activities

- This section covers the controls that COSO recommends to **help mitigate risk**.

- The main categories for controls in COSO are **operational, financial reporting and compliance**.

- The controls identified are broad in nature and cover some IT related issues, but COSO doesn’t address this area as well for IT as it does the accounting side.

- It does highlight the various activities that should be controlled, but leaves it up to management to figure out how to do it.

Information and communication

- Having an organization in which information and communication are free to flow between all aspects of the business is addressed in this component of COSO.

- Information, according to COSO, is the data used to run the business, whereas communication is defined as the method used to disseminate information to the appropriate individuals.

-

- People cannot do their jobs efficiently and effectively if they are not provided with the necessary information.

- Without the appropriate lines of communication and timely action, problems can turn into catastrophes.

- Communication is the mechanism that drives the other four components of the COSO framework.

Monitoring

- Auditing and measurement are essential in determining how controls perform.

- Monitoring can be the alarm system that identifies a problem and provides valuable data for fixing issues for the future.

- Monitoring can consist of periodic reports, audits or testing mechanisms that provide the status of individual controls.

- COSO is one of the more widely adopted internal control frameworks for large companies due in no small part to the mandates set forth through SOX 404.

Monitoring

- The COSO framework represents the grandfather of internal controls and though it was designed primarily for accounting controls, it still provides value for companies building out a security governance strategy.

- **From an IT perspective, the five main components are entirely relevant to securing information, but the actual controls themselves don’t go to the same level of depth as other frameworks such as Control Objects for Information and related Technologies (COBIT).**

COBIT

- The COBIT framework was created by the Information Systems Audit and Control.

- Association (ISACA) and IT Governance Institute (ITGI) as a response to the needs of the IT community for a less generalized and more actionable set of controls for securing information systems.

- The ITGI is a non-profit organization that leads the development of COBIT through committees consisting of experts from universities, governments and auditors across the globe.

- The COBIT framework is a series of manuals and implementation guidelines for creating a full IT governance, auditing and service delivery program for any organization.

COBIT

- COBIT is not a replacement but an augmentation to COSO, and maps directly to COSO from an IT perspective.

- Although COSO covers the whole enterprise from an accounting perspective, it does so by providing high level objectives that require the business to figure out how to accomplish them.

- COBIT on the other hand, works with COSO by fully detailing the necessary controls required and how to measure and audit them.

- The built-in auditable nature of COBIT is why it has become one of the leading IT governance frameworks as it gets as close as can be expected to a turnkey governance program.

COBIT

- COBIT does not dig down into the actual tasks and procedures however, which necessitates using other sources to develop standards and procedures for implementing the controls.

- COBIT won’t tell you the best way to configure AES encryption for your wireless infrastructure, but it will provide you with a mechanism for identifying where and why you need to apply it based on risk.

- The role of COBIT in IT governance is to provide a model that takes the guesswork out of how to bridge the gap between business and IT goals.

- COBIT considers business the customer of IT services.

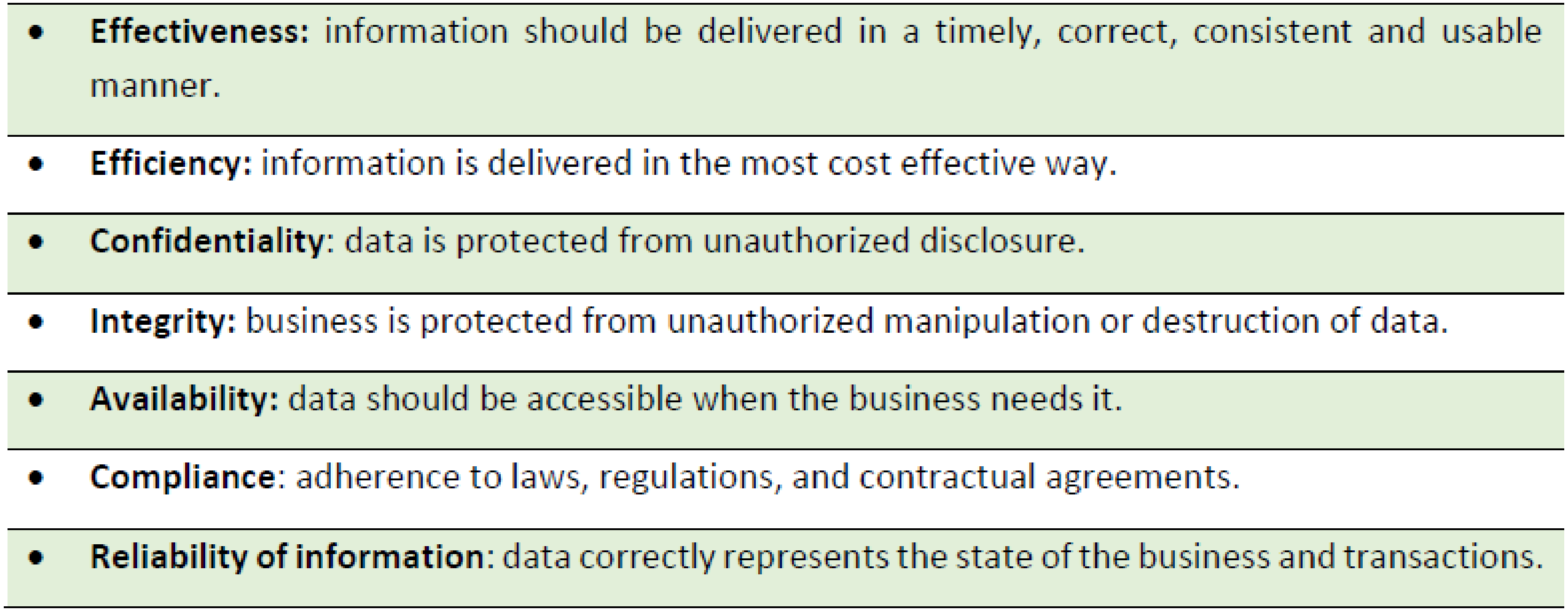
COBIT

- Business requirements (needs) ultimately drive the investment in IT resources, which in turn need processes that can deliver enterprise information back to the business.

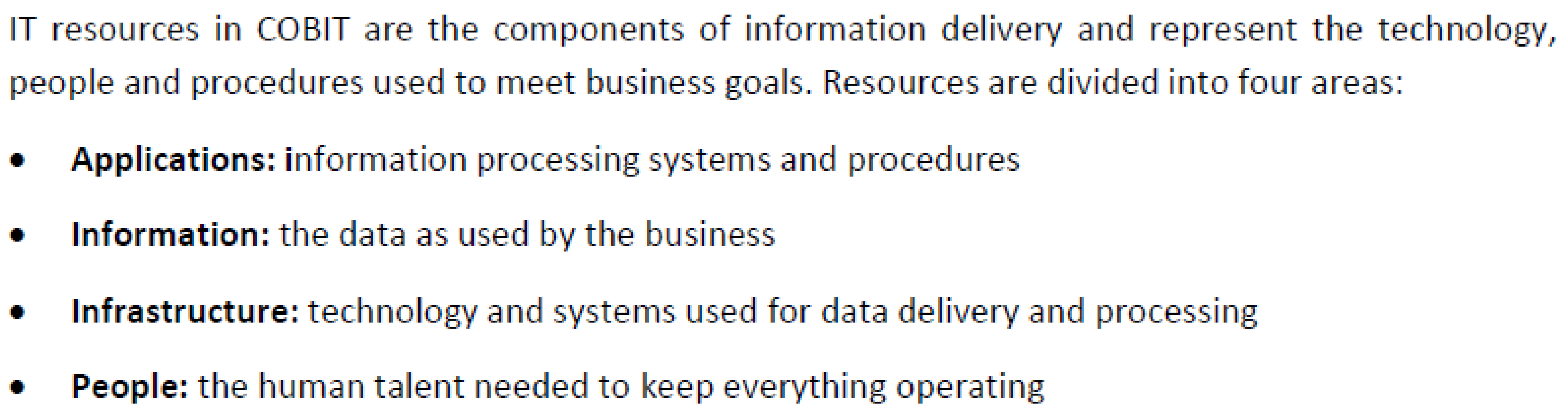
- At the foundation of COBIT is the cyclical nature of business needing information and IT delivering information services.

- Information is what IT provides to the business and COBIT defines the following seven control areas as business requirements for information:

COBIT



- **Effectiveness:** information should be delivered in a timely, correct, consistent and usable manner.
- **Efficiency:** information is delivered in the most cost effective way.
- **Confidentiality**: data is protected from unauthorized disclosure.
- **Integrity:** business is protected from unauthorized manipulation or destruction of data.
- **Availability:** data should be accessible when the business needs it.
- **Compliance**: adherence to laws, regulations, and contractual agreements.
- **Reliability of information**: data correctly represents the state of the business and transactions.



IT resources in COBIT are the components of information delivery and represent the technology, people and procedures used to meet business goals. Resources are divided into four areas:

- **Applications:** information processing systems and procedures
- **Information:** the data as used by the business
- **Infrastructure:** technology and systems used for data delivery and processing
- **People:** the human talent needed to keep everything operating

- IT processes (or activities) are the planned utilization of resources and divided into four inter-related domains.

- Each process has its own controls that govern how the process is to be accomplished and measured.

- There are 34 high level processes and hundreds of individual controls. The domains and processes are:

- **Plan and Organize (PO):** Defines strategy and guides the creation of a service and solutions delivery organization. The high level process for this domain is as follows:
    - PO1 Define a strategic IT plan
    - PO2 Define the information architecture
    - PO3 Determine technological direction
    - PO4 Define the IT processes, organization and relationships
    - PO5 Manage the IT investment
    - PO6 Communicate management aims and direction
    - PO7 Manage IT Human Resources
    - PO8 Manage quality
    - PO9 Assess and manage IT risks
    - PO10 Manage projects

- **Acquire and Implement (AI):** Builds IT solutions and creates services. The high level process for this domain is as follows:
    - AI1 Identify automated solutions
    - AI2 Acquire and maintain application software
    - AI3 Acquire and maintain technology infrastructure
    - AI4 Enable operation and use
    - AI5 Procure IT resources
    - AI6 Manage changes
    - AI7 Install and accredit solutions and changes

- **Deliver and Support (DS):** User facing delivery of services and solutions. The high level process for this domain is as follows:
    - DS1 Define and manage service levels
    - DS2 Manage third-party services
    - DS3 Manage performance and capacity
    - DS4 Ensure continuous service
    - DS5 Ensure systems security
    - DS6 Identify and allocate costs
    - DS7 Educate and train users
    - DS8 Manage service desk and incidents
    - DS9 Manage the configuration
    - DS10 Manage problems
    - DS11 Manage data
    - DS12 Manage the physical environment
    - DS13 Manage operations

- **Monitor and Evaluate (ME):** Monitors IT processes to ensure synergy between business requirements. The high level process for this domain is as follows:
    - ME1 Monitor and evaluate IT performance
    - ME2 Monitor and evaluate internal control
    - ME3 Ensure compliance with external requirements
    - ME4 Provide IT governance
- Each of the processes in COBIT is written for managers, users and auditors by addressing each group's needs. Each process control objective is built using a template that includes:
    - a general statement that provides answers to why management needs the control and were it fits
    - the key business requirements that the control addresses
    - how the controls are achieved
    - control goals and metrics
    - who is responsible for each individual control activity
    - how the controls can be measured
    - clear descriptions of measuring how mature the organization is in accomplishing the control using a detailed 0–5 scale Maturity Model

- Measurement of each process and control is accomplished through a Maturity Model.

- The COBIT Maturity Model is based on the Capabilities Maturity Model pioneered by Carnegie Mellon’s Software Engineering Institute (SEI).

- The Capabilities Maturity Model was designed as a tool for ensuring quality software development.

- COBIT has modified the model to deliver a measurement and tracking tool that identifies the current state of adoption (maturity level) for each process so as to compare an organization execution with industry averages and business targets.

- This helps management identify where the company’s performance is in relation to its peers and provides a path to improve with specific and prescriptive steps used to get there.

The COBIT Maturity Model scale provides the following measurements:

COBIT Maturity Scale

0 Non existent

Not performed.

1 Initial/ Ad hoc

Process is chaotic, not standardized and done case by case.

2 Repeatable

Relies on individual knowledge, no formal training and no process intuitive management.

3 Defined process

Standardized and documented processes and formal training to communicate standards.

4 Managed

Processes are monitored and checked for compliance by management, measurable processes are reviewed for improvement and limited automation.

5 Optimized

Processes are refined and compared with others based on maturity, processes are automated through workflow tools to improve quality and effectiveness.

- Using COBIT requires customization to better align with the company implementing it.

- COBIT is not designed as a governance strategy in a box, but as a reference for building a process focused system, utilizing international standards and good practices.

- Companies still need to determine a risk management methodology and build out a technical infrastructure to automate the various COBIT processes identified.

- COBIT’s real value is in providing the management, measurement and organizational glue to tie these functions together.

- IT auditors like to use COBIT mainly because it creates a well-documented set of processes and controls that can be assessed along with the metrics and requirements for each control.

- COBIT’s usefulness is also apparent when the organization under audit does not use COBIT as a governance framework because an auditor can build checklists and plan audits based on COBIT to ensure that all aspects of the IT process are performed.

- COBIT is also an invaluable resource when writing the audit report because it allows the auditor to justify and compare his findings to a well-respected standard.

ITIL

- The Information Technology Infrastructure Library (ITIL) provides **documentations for best practices for IT Service Management.**

- A study was conducted and generated a significant amount of information (roughly 40 books) that became known as ITIL.

- The books were **revised and consolidated** in 2004 and became a series of eight books focused on IT services management.

- This version 2 of ITIL became popular among organizations looking for an **internationally recognized, proactive framework for managing IT services, reducing cost and improving quality**.

ITIL

- Version 3 of ITIL was released in June 2007 to refresh the core service and support delivery material that many companies have implemented, and to move the ITIL framework towards **a life cycle model** that includes management of all lifecycle services provided by IT.

- The five books that make up Version 3 are:

- **Service Strategy:** This book is the foundation for the others by defining business to IT alignment, value to business, services strategy and service portfolio management.
- **Service Design:** Focused on the design of IT processes, policies and architectures. Includes service level, management, capacity management, information security management and availability management.
- **Service Transition:** Covers moving from the design phase to production business services and change management. It also includes service asset and configuration management, service validation and testing, evaluation and knowledge management.
- **Service Operation:** Provides information on the day-to-day support of production systems. This includes service delivery and services support, service desk design, application management, problem management and technical management.
- **Continual Service Improvement:** This book covers service improvements and service retirement strategies.

- ITIL is primarily about delivering IT as a **service and the lifecycle of service development, implementation, operation and management**.
- ITIL is used by companies for **overall management of IT** and also for managing security processes.
- Auditing an ITIL shop requires that the auditor understand the basics of ITIL to speak the same language.
- ITIL also works well with COBIT as a means for **fleshing out the service delivery of each process**.
- The **ITGI** even creates a **mapping between COBIT and ITIL** for organizations that want to utilize the two standards.
- ITIL also meets the criteria for ISO 20000, which means that it can be used **to achieve international certification**.
- Whether a company chooses to go for certification or not, ITIL gives guidance about how to **move from a reactive to a proactive approach** to managing IT and security as a service.

Technology: Standards Procedures and Guidelines

- Knowing what processes and controls need to be in place is half the job.

- The other half is implementing the technology and procedures that allow the control to work as intended.

- Most auditors focus their efforts on testing and validating controls to ensure that they are functional and dependable.

- **Penetration testing, configuration review and architecture review** are all part of this type of assessment, so auditors needs to know where to go to find guidance, templates and sample designs that have been proven to work through consensus and extensive testing.

Technology: Standards Procedures and Guidelines

- The best security programs don’t provide much benefit if the execution of those programs relies on poor control choices.

- The following standards and best practices can help the **auditor distinguish good security designs from bad and provide reference architectures to compare**

ISO 27000 Series of Standards

- The **ISO 27000 series** are internationally recognized security control standards for **the creation and operations of an Information Security Management System** (ISMS).

- Previously known as ISO 17799 and originating from British Standard 7799, the ISO 27000 series is one of the **most widely used and cited documents** in information security today.

- All the major governance frameworks reference ISO when discussing key controls, and it is a great resource to address a wide range of security needs from data-handling standards, to physical security, to policy.

- ISO 27000 is broad and covers a great deal of **content that is broken into seven published standards** documents with ten more currently in preparation.

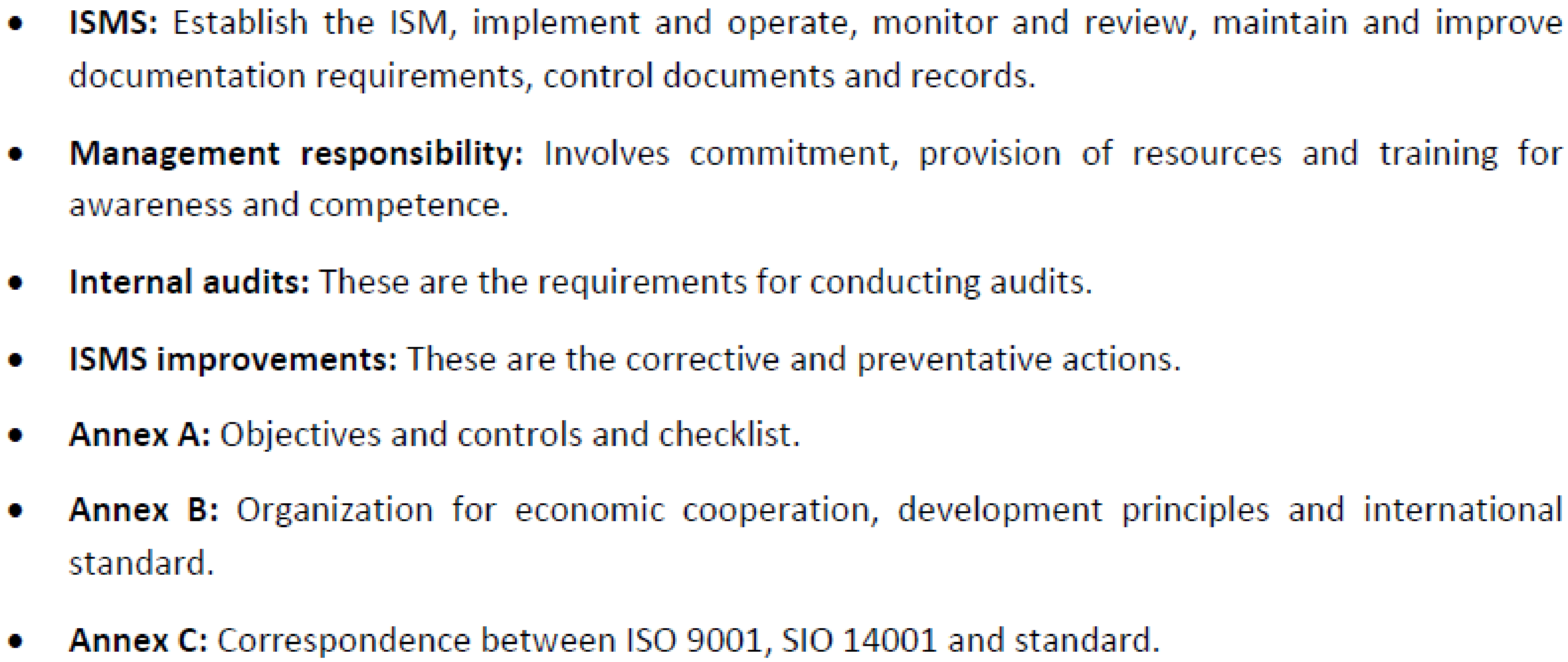
- This overview is centered on the first two standards: **ISO 27001 and 27002.**

- The **first ISO standard** is *ISO 27001:2005* Information Technology Techniques Information Security Management Systems.

- It provides the requirements for a security management system in accordance with ISO 27002 best practices.

- ISO 27001 identifies generic **technological controls and processes** that must be in place if a business wants to be certified as compliant with the ISO standard.

The contents of ISO 27001 are:



- **ISMS:** Establish the ISM, implement and operate, monitor and review, maintain and improve documentation requirements, control documents and records.
- **Management responsibility:** Involves commitment, provision of resources and training for awareness and competence.
- **Internal audits:** These are the requirements for conducting audits.
- **ISMS improvements:** These are the corrective and preventative actions.
- **Annex A:** Objectives and controls and checklist.
- **Annex B:** Organization for economic cooperation, development principles and international standard.
- **Annex C:** Correspondence between ISO 9001, SIO 14001 and standard.

- A key concept used in 27001 is the Deming Cycle process improvement approach: Plan, Do, Check and Act.

- This continuous improvement cycle was made famous by Dr. W. Edwards Deming whose quality control techniques methodology is a way to show that a process can be continually improved by learning from mistakes and monitoring the things done correctly to further refine the capabilities of the system.

The Deming Cycle is simple yet powerful, and ISO 27001 applies it to security management in the following manner:

Step 1. Plan: Establish the ISM according to the policies, processes and objectives of the organization to manage risk.

Step 2. Do: Implement and operate the ISM.

Step 3. Check: Audit, assess and review the ISM against policies, objectives and experiences.

Step 4. Act: Take action to correct deficiencies identified for continuous improvement.

Topics : Digital Assignment II

- ISO 27000 Series of Standards
- NIST
- Centre for Internet Security
- NSA
- DISA
- SANS
- ISACA
- ISO 27003
- ISO 27004
- ISO 15408 Evaluation Common Criteria Evaluation for Security
- ISO/IEC 13335 (IT Security Management)
- ISO 27005
- ISO Standard 24762 for Technical Disaster Recovery
- ISO Standard for BCM – 22301
- IEEE Standards
- ISO 17799
- BS 7799

Security Standards Organizations

Internet Corporation for Assigned Names and Numbers (ICANN)

- ICANN’s role is to oversee the **huge and complex interconnected network of unique identifiers** that allow computers on the Internet to find one another.

- To **reach another person on the Internet** you have to type an address into your computer - a name or a number.

- That address has to be unique so computers know where to find each other.

- **ICANN coordinates** these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

Security Standards Organizations

- **ICANN** was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated **to keeping the Internet secure, stable and interoperable**.

- It promotes **competition and develops policy on the Internet's unique identifiers**. This is commonly termed "universal resolvability" and means that wherever you are on the network – and hence the world – that you receive the same predictable results when you access the network.

- Without this, you could end up with an Internet that worked entirely differently depending on your location on the globe.

International Organization for Standardization (ISO)

- ISO (International Organization for Standardization) is an **independent, non-governmental membership organization** and the world's largest developer of **voluntary International Standards**.

- They are made up of 162 member countries who are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland.

- International Standards make things work.

- They **give world-class specifications for products**, services and systems, to ensure quality, safety and efficiency.

International Organization for Standardization (ISO)

- They are instrumental in **facilitating international trade**.

- ISO has published more than 19500 International Standards covering almost every industry, from technology, to food safety, to agriculture and healthcare.

- ISO International Standards impact everyone, everywhere.

Consultative Committee For Telephone and Telegraphy (CCITT)

- The CCITT, now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union), is the primary international body for **fostering cooperative standards for telecommunications equipment and systems**.

- It is located in Geneva, Switzerland.

American National Standards Institute(ANSI)

- American National Standards Institute (ANSI) oversees the **creation, promulgation and use of thousands of norms and guidelines** that directly impact businesses in America in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more.

- ANSI is also actively engaged in **accreditation - assessing** the competence of organizations determining **conformance to standards**.

Institute Of Electronics and Electrical Engineers (IEEE)

- IEEE is the world's largest professional association dedicated to advancing technological **innovation and excellence** for the benefit of humanity.

- IEEE and its members inspire a global community through IEEE's **highly cited publications, conferences, technology standards, and professional and educational activities**.

- IEEE, pronounced "Eye-triple-E," stands for the **Institute of Electrical and Electronics Engineers**.

Electronic Industries Association

- The Electronic Industries Association (EIA) comprises individual organizations that together have agreed on certain **data transmission standard**s such as EIA/TIA-232 (formerly known as RS-232).

- The Electronics Industries Alliance (EIA) is an alliance of **trade organizations** that lobby in the interest of companies **engaged in the manufacture of electronics-related products**.

National Center for Standards and Certification Information (NIST)

- National Institute of Standards and Technology's web site. Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the **nation's oldest physical science laboratories**.

- Today, NIST measurements support the smallest of technologies - **nanoscale devices** so tiny that tens of thousands can fit on the end of a single human hair to the largest and most complex of human made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

National Center for Standards and Certification Information (NIST)

- The National Centre for Standards and Certification Information provides **research services on standards, technical regulations and conformity assessment procedures** for nonagricultural products.

- The Centre is a central repository for standards-related information in the United States and has access to U.S., foreign and international documents and contact points through its role as the U.S. national inquiry point under the World Trade Organization Agreement on Technical Barriers to Trade.

- The Program maintains a database on NIST and Department of Commerce staff participation in standards developing activities.

World Wide Web Consortium (W3C)

- The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to **develop Web standards**.

- Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the **Web to its full potential**.

Information Security Laws, Regulations & Guidelines

- India’s Ministry of Communications and Information Technology (“Department of Information Technology”) has **implemented the Information Technology** (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“Privacy Rules”).

- Clarifications to the Privacy Rules were issued via Press Note by the Ministry.

- India’s enabling legislation is India’s Information Technology Act 2000 (the “Act”).

Information Security Laws, Regulations & Guidelines

- The Bill seeks to further refine provisions of the Rules, with a focus on **protection of personal data through limitations** on use and requirements for notice.

- The **collection of personal data would be prohibited** unless “necessary for the achievement of a purpose of the person seeking its collection,” and, subject to sections 6 and 7 of the Bill, “no personal data may be collected under this Act prior to the data subject being given notice, in such form and manner as may be prescribed, of the collection.”

- The Bill acknowledges the **collection of data with and without consent**; the regulation of personal data storage, processing, transfer, and security; and discusses the different types of disclosure.

- http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
- http://pib.nic.in/newsite/erelease.aspx?relid=74990
- http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan010239.pdf

Data Protection Authority and Registration Requirements

- **No specific data protection authority exists**, but the Privacy Rules state that in the case of a breach, a "Body Corporate," as defined under the Act, must answer to "the agency mandated under the law" (presumably, the Ministry).

- There are no registration requirements for the collection of data. However, the Data Security Council of India (the "DSCI") provides a certification service by which organizations within India may become "DSCI Privacy Certified."

Protected Personal Data

- Personal information is defined as any information that relates to a natural person, which,
  - either directly or indirectly, in combination with other information available or
  - likely to be available with a corporate entity,
  - is capable of identifying such person.

- **Data or information is not sensitive and personal if it is available in the public domain** or furnished under the Right to Information Act of 2005.

Protected Personal Data

- Sensitive personal data or information is defined as “personal information” which consists of information relating to any of the following:
  - passwords;
  - financial information such as bank account or credit card or debit card or other payment instrument details;
  - physical, physiological and mental health condition;
  - sexual orientation;
  - medical records and history;
  - biometric information;
  - any detail relating to any of the above as provided to a corporate entity for providing service; and
  - any of the information received under the above by a corporate entity for processing, stored or processed under lawful contract or otherwise.

Data Collection and Processing

- The **Privacy Rules apply to data collection**, but do not define processing.
- The **Privacy Rules** requires a Body Corporate that collects, receives, possesses, stores, deals, or handles sensitive or personal data to provide a privacy policy for handling of such data and ensure that the policies are available for view by the data subjects who have provided the information under contract.
- The policy shall provide for:
  - clear and easily accessible statements of its practices and policies;
  - the type of personal or sensitive personal data or information collected;
  - the purpose of collection and usage of such information;
  - the disclosure of information including sensitive personal data or information; and
  - reasonable security practices and procedures.

Data may be collected and processed when all of the following conditions are met:

- the data subject has provided written consent and is aware at the time of collection that the information is being collected, the purpose of collection, the intended recipients of the information; and the name and address of the agency that is collecting and will retain the information;
- the data subject has been provided with the option not to provide its sensitive personal data or information;
- the data subject is permitted to withdraw his/her consent, in writing, at any time;
- the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
- the collection of the sensitive personal data or information is considered necessary for that lawful purpose.

Data Transfer

- Disclosure of data to a third party requires prior permission of the data subject, whether the information is provided under contract or otherwise, except in the following situations:
  - the disclosure has already been agreed to in a contract;
  - the disclosure is necessary for compliance with a legal obligation;
  - the data is shared with government agencies with the authority to obtain the data for the purpose of verification of identity, or for the prevention, detection, investigation, prosecution, and punishment of offenses, including cyber incidents; or
  - the disclosure is pursuant to an order under the law.

- **Data may be transferred domestically or internationally** to any person or Body Corporate that ensures the same level of data protection that is adhered to by the Body corporate, but the transfer is allowed only if:

  - the data subject consents; or

  - the transfer is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and the data subject.

Data Security

- A Body Corporate is required to **implement reasonable security practices and procedures**.

- The **Privacy Rules** indicate that reasonable practice methodologies include IS/ISO/EIC 27001 or other measures that have been pre-approved by the central government and are subject to annual audits by a central government approved auditor.

Breach Notification

- There is no mandatory requirement to report data security breach incidents under the **Privacy Rules.**

Other Considerations

- **Data retention rules** state that information should not be retained longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.

- A clarification to the Privacy Rules stating that a "**Body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information** under contractual obligation with any legal entity located within or outside India is exempt from the requirement to obtain consent" was issued via Press Note by the Department of Information and Technology.

- Accordingly, outsourcing service providers in India should be exempt from obtaining consent from the individuals whose data they process.

Enforcement & Penalties

- A corporate entity may be liable for up to Rs. 50,000,000 for the **negligent failure** to implement and maintain reasonable practices and procedures, causing wrongful loss or gain.

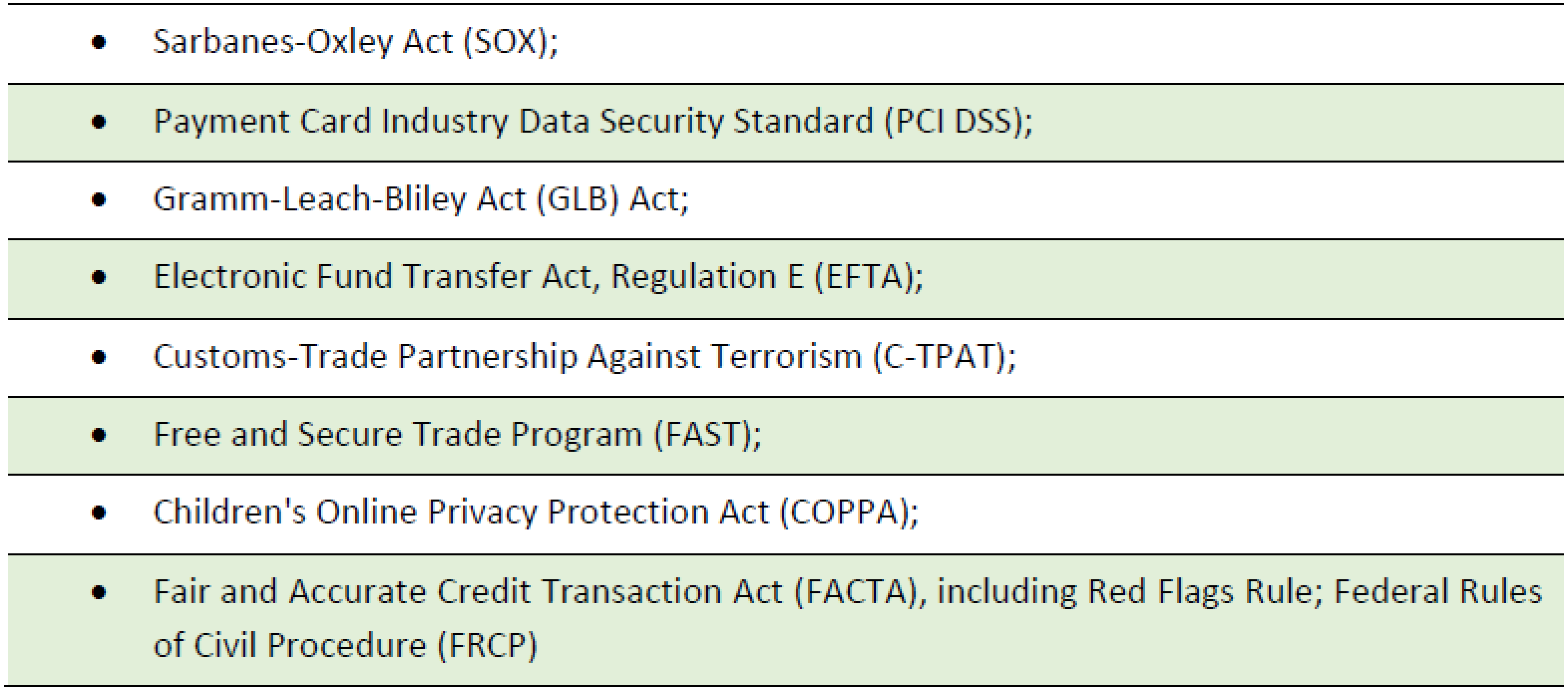
International Directory of laws:

- This directory includes **laws, regulations and industry guidelines** with significant security and privacy impact and requirements.

- This is largely USA focused but used ***by International agencies*** as a reference point.

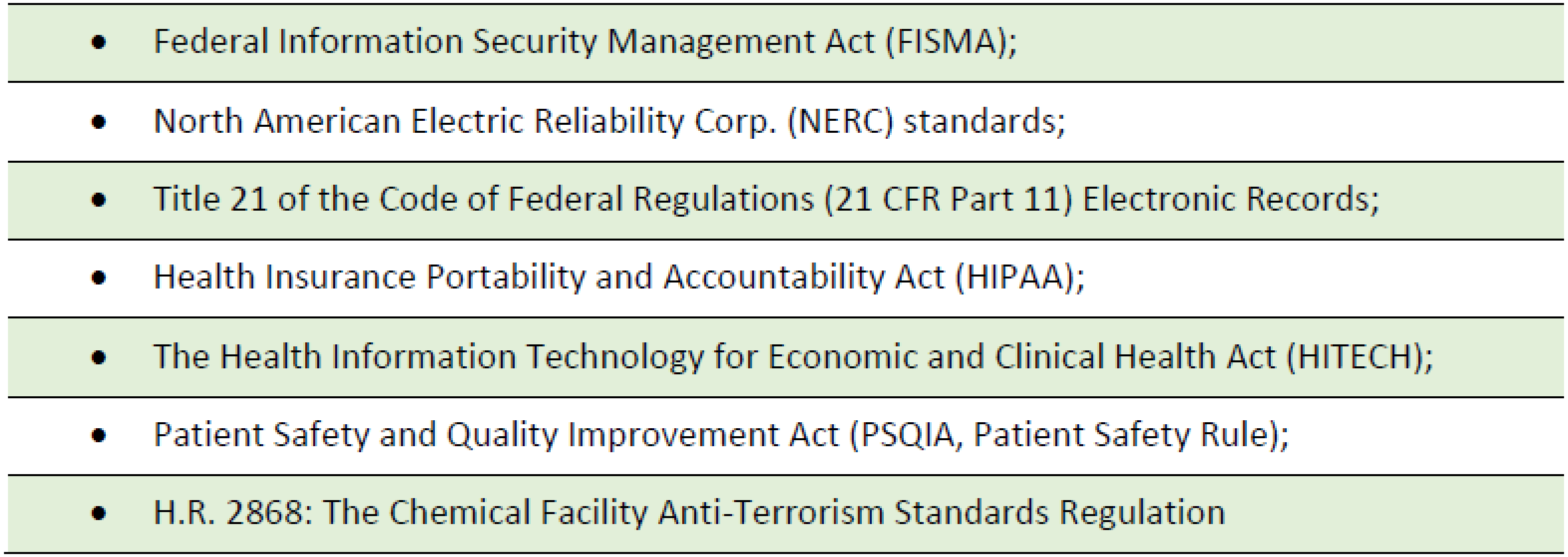
Broad laws:

-



- Sarbanes-Oxley Act (SOX);
- Payment Card Industry Data Security Standard (PCI DSS);
- Gramm-Leach-Bliley Act (GLB) Act;
- Electronic Fund Transfer Act, Regulation E (EFTA);
- Customs-Trade Partnership Against Terrorism (C-TPAT);
- Free and Secure Trade Program (FAST);
- Children's Online Privacy Protection Act (COPPA);
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule; Federal Rules of Civil Procedure (FRCP)

Industry specific laws:



- Federal Information Security Management Act (FISMA);
- North American Electric Reliability Corp. (NERC) standards;
- Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records;
- Health Insurance Portability and Accountability Act (HIPAA);
- The Health Information Technology for Economic and Clinical Health Act (HITECH);
- Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule);
- H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation