300 LEVEL CYBERSECURITY

DEPARTMENT OF COMPUTER SCIENCE, BINGHAM UNIVERSITY, KARU

CYB 307 – INFORMATION SECURITY ENGINEERING
LECTURE I – INTRODUTION

“The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location—and I’m not completely confident of that one, either” (Schneier 1995).

Course Content

- System and management view of information security
- System and management view of information security
- Requirements for information security
- System design process and life-cycle security management of information systems
- Basic policies on information security and methodologies
- Information security risk management
- Security in the systems engineering process
- Laws related to information security and management of operational systems

Introduction – Security Engineering

What is Security Engineering?

Is the process of incorporating security controls into the information system so that they become an integral part of the system's operational capabilities. Its objectives are to:

- ❖build systems to remain dependable and resilient in the face of threats (technology, human, nature)
- ❖It focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves in the context of security.
- ❖Requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to economics, applied psychology, organizations and the law.
- ❖It ensures that the right assets are protected in the right way – involves figuring out what needs protection and how it would be protected.

System and Management View of Information security

Security engineering principles and practices apply most directly to the design, development, and implementation of technical controls. like:
Encryption
Firewalls
Access control
Intrusion detection (IDS),
Intrusion prevention (IPS)
etc

System View of Information Security

Management View of Information Security

Cybersecurity management mitigates the risk exposure of organisations using a range of:

- managerial,
- legal,
- technological,
- Process,
- social controls,
- strategic,
- personnel,
- infrastructure,
- requirements,
- policy enforcement,
- emergency planning,
- security awareness,
- and other resources.

Requirements for Information Security

Security requirements are generally categorised into two: namely;

- Security Functional Requirements - Describe what a system should do. That is, security services that needs to be achieved by the system under inspection. For example: authentication, authorization, backup, server-clustering
- Security Assurance Requirements - describe how functional requirements should be implemented and tested

Security Functional Requirements

Security Audit – the need to recognise, record, store, and analyse security-relevant activities. Identify only audit-relevant activities and enable them.

Non-repudiation - Is it important that an originator cannot deny having sent a message, or that a recipient cannot deny having received it.

Cryptographic Support - If you are using cryptography, what operations use cryptography, what algorithms and key sizes are you using, and how are you managing their keys (including distribution and destruction)?

User Data Protection - This class specifies requirement for protecting user data. The basic idea is that you should specify a policy for data (access control or information flow rules), develop various means to implement the policy, possibly support off-line storage, import, and export, and provide integrity when transferring user data

Security Functional Requirements

Identification and authentication- users should not just report who they are (identification) – system should verify their identity (authentication). Passwords are the most common mechanism for authentication. It is often useful to limit the number of authentication attempts (if you can) and limit the feedback during authentication (e.g., displaying asterisks instead of the actual password). Certainly, limit what a user can do before authenticating; in many cases, do not let the user do anything without authenticating.

Security Management (Authorization)- Many systems will require some sort of management (e.g., to control who can do what), generally by those who are given a more trusted role (e.g., administrator). Be sure you think through what those special operations are, and ensure that only those with the trusted roles can invoke them. You want to limit trust; ideally, even more trusted roles should be limited in what they can do.

Security Assurance Requirements

Configuration management - At least, have unique a version identifier for each release, so that users will know what they have. You gain more assurance if you have good automated tools to control your software, and have separate version identifiers for each piece. The more that's under configuration management, the better; don't just control your code, but also control documentation, track all problem reports (especially security-related ones), and all development tools.

Delivery and operation - Your delivery mechanism should ideally let users detect unauthorized modifications to prevent someone else masquerading as the developer, and even better, prevent modification in the first place. You should provide documentation on how to securely install, generate, and start-up the TOE, possibly generating a log describing how the TOE was generated.

Development - These CC requirements deal with documentation describing the TOE implementation, and that they need to be consistent between each other (e.g., the information in the ST, functional specification, high-level design, low-level design, and code, as well as any models of the security policy).

Security Assurance Requirements – cont’d

- Guidance documents (AGD). Users and administrators of your product will probably need some sort of guidance to help them use it correctly. It doesn’t need to be on paper; on-line help and "wizards" can help too. The guidance should include warnings about actions that may be a problem in a secure environemnt, and describe how to use the system securely.
- Life-cycle support (ALC). This includes development security (securing the systems being used for development, including physical security), a flaw remediation process (to track and correct all security flaws), and selecting development tools wisely.

Tests (ATE). Simply testing can help, but remember that you need to test the security functions and not just general functions. You should check if something is set to permit, it’s permitted, and if it’s forbidden, it is no longer permitted. Of course, there may be clever ways to subvert this, which is what vulnerability assessment is all about (described next).

Security Assurance Requirements – cont’d

Vulnerability Assessment (AVA). Doing a vulnerability analysis is useful, where someone pretends to be an attacker and tries to find vulnerabilities in the product using the available information, including documentation (look for "don’t do X" statements and see if an attacker could exploit them) and publicly known past vulnerabilities of this or similar products. This book describes various ways of countering known vulnerabilities of previous products to problems such as replay attacks (where known-good information is stored and retransmitted), buffer overflow attacks, race conditions, and other issues that the rest of this book describes. The user and administrator guidance documents should be examined to ensure that misleading, unreasonable, or conflicting guidance is removed, and that security procedures for all modes of operation have been addressed. Specialized systems may need to worry about covert channels; read the CC if you wish to learn more about covert channels.

Maintenance of assurance (AMA). If you’re not going through a CC evaluation, you don’t need a formal AMA process, but all software undergoes change. What is your process to give all your users strong confidence that future changes to your software will not create new vulnerabilities? For example, you could establish a process where multiple people review any proposed changes.

System Design Process and LIFE-CYCLE Security Management of IS

The life-cycle describes the phases that are involved in developing or acquiring an Information System (IS) and how security is built-in at each phase to ensure security of the IS by default.

This is achieved through the mapping of relevant security engineering principles at every stage of the system design life-cycle. We consider a system design life-cycle with five phases.

i. Initiation

ii. Development or acquisition (system design and implementation)

iii. Implementation (Testing, deployment and conversion)

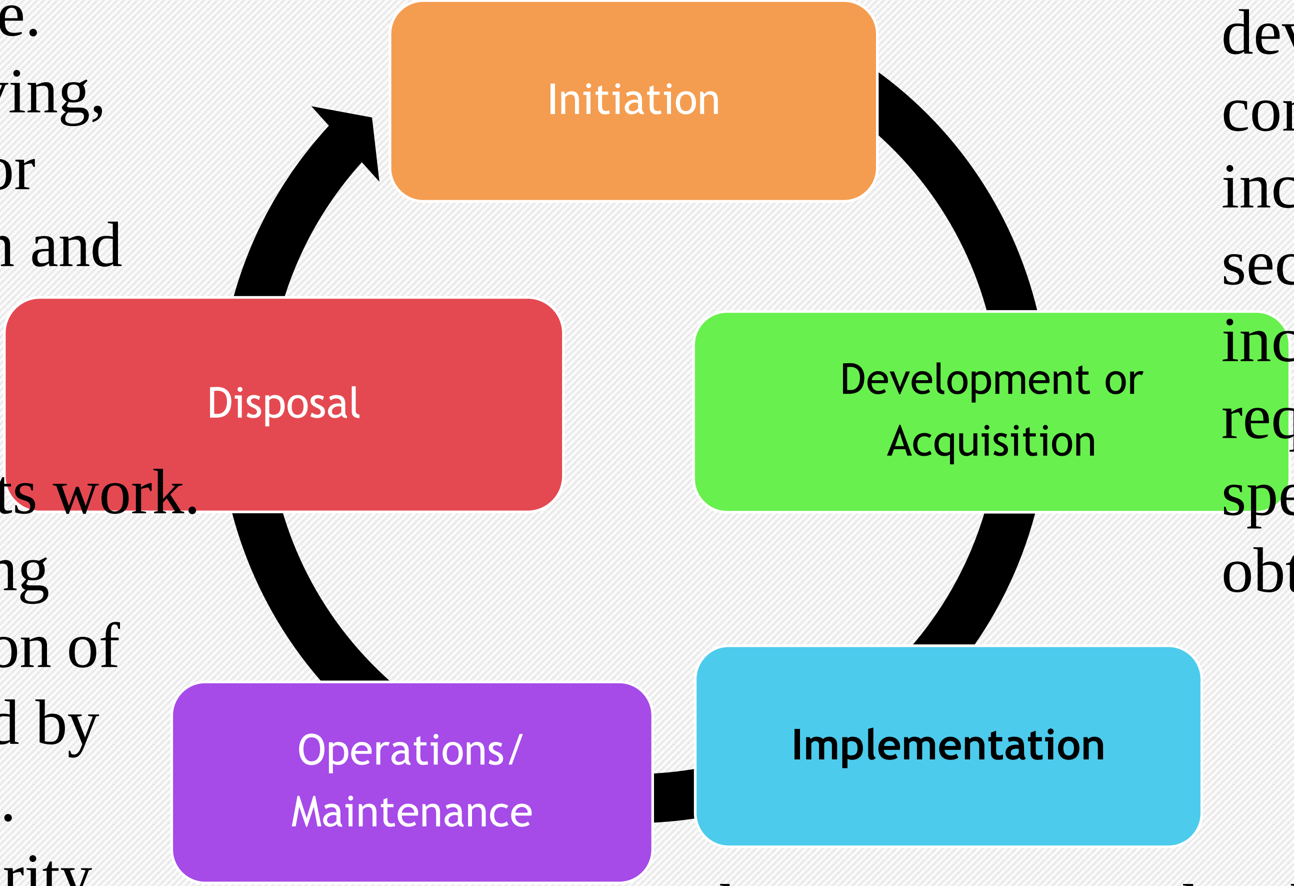
iv. Operations and maintenance

v. Disposal

Life-cycle Description

Disposition of information, hardware, and software. Activities include moving, archiving, discarding or destroying information and sanitizing the media

The need for a system is expressed and the purpose of the system is documented



The system is designed, purchased, programmed, developed, or otherwise constructed. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining the system

The system is tested and installed or fielded. Activities include installing/turning on controls, security testing, certification, and accreditation.

The system performs its work. The system is also being modified by the addition of hardware, software and by numerous other events. Activities include security operations, administration, operational assurance, audits and monitoring.

Security Engineering Principles

To aid in designing a secure information system, NIST compiled a set of engineering principles for system security.

- These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed.
- The primary focus of these principles is the implementation of technical controls,
- However, the principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education and training.

These security engineering principles are separated into six phases, namely:

- ✓ Security Foundation
- ✓ Risk-Based
- ✓ Ease of Use
- ✓ Increased Resilience
- ✓ Reduced Vulnerabilities
- ✓ Design with Network in Mind

System Design Process and LIFE-CYCLE Security Management of IS

#	Category	Principles
1	Security Foundation	i. Establish a sound security policy as the **foundation** for design ii. Treat security as an integral part of the overall system design iii. Clearly delineate the physical and logical security boundaries governed by associated security policies. iv. Ensure that developers are trained on how to develop secure software.
2	Risk-Based	i. Reduce risk to an acceptable level ii. Assume that external systems are insecure. iii. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness. iv. Implement tailored system security measures to meet organizational security goals. v. Protect information while being processed, in transit, and in storage. vi. Consider custom products to achieve adequate security. vii. Protect against all likely classes of attacks.

System Design Process and LIFE-CYCLE Security Management of IS

#	Category	Principles
3	Ease of Use	i. Where possible, base security on open standards for portability and interoperability ii. Use common language in developing security requirements iii. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process. iv. Strive for operational ease of use
4	Increase Resilience	i. Implement layered security (Ensure no single point of vulnerability) ii. Design and operate an IT system to limit damage and to be resilient in response iii. Provide assurance that the system is, and continues to be, resilient in the face of expected threats iv. Limit or contain vulnerabilities v. Isolate public access systems from mission critical resources (e.g., data, processes, etc.) vi. Use boundary mechanisms to separate computing systems and network infrastructures vii. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations viii. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability

System Design Process and LIFE-CYCLE Security Management of IS

#	Category	Principles
5	Reduce Vulnerabilities	i. Strive for simplicity ii. Minimize the system elements to be trusted iii. Implement least privilege iv. Do not implement unnecessary security mechanisms v. Ensure proper security in the shutdown or disposal of a system Identify and prevent common errors and vulnerabilities
6	Design with Network in Mind	i. Implement security through a combination of measures distributed physically and logically ii. Formulate security measures to address multiple overlapping information domains iii. Authenticate users and processes to ensure appropriate access control decisions both within and across domains iv. Use unique identities to ensure accountability

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
1	**Initiation**	i. Establish a sound security policy as the **foundation** for design ii. Treat security as an integral part of the overall system design iii. Clearly delineate the physical and logical security boundaries governed by associated security policies. iv. Ensure that developers are trained in how to develop secure software. v. Reduce risk to an acceptable level vi. Assume that external systems are insecure. vii. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness viii. Use common language in developing security requirements

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
2	**Development or Acquisition**	i. Treat security as an integral part of the overall system design ii. Clearly delineate the physical and logical security boundaries governed by associated security policies. iii. Ensure that developers are trained in how to develop secure software iv. Reduce risk to an acceptable level v. Assume that external systems are insecure. vi. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness. vii. Implement tailored system security measures to meet organizational security goals. viii. Protect information while being processed, in transit, and in storage. ix. Consider custom products to achieve adequate security. x. Protect against all likely classes of attacks. xi. Where possible, base security on open standards for portability and interoperability xii. Use common language in developing security requirements xiii. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process. xiv. Strive for operational ease of use

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
2	**Development or Acquisition**	xv. Implement layered security (Ensure no single point of vulnerability) xvi.Design and operate an IT system to limit damage and to be resilient in response xvii.Provide assurance that the system is, and continues to be, resilient in the face of expected threats xviii.Limit or contain vulnerabilities xix.Isolate public access systems from mission critical resources (e.g., data, processes, etc.) xx. Use boundary mechanisms to separate computing systems and network infrastructures xxi.Design and implement audit mechanisms to detect unauthorized use and to support incident investigations xxii.Strive for simplicity xxiii.Minimize the system elements to be trusted xxiv.Do not implement unnecessary security mechanisms xxv.Identify and prevent common errors and vulnerabilities xxvi.Implement security through a combination of measures distributed physically and logically xxvii.Formulate security measures to address multiple overlapping information

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
3	**Implementation**	i. Treat security as an integral part of the overall system design ii. Reduce risk to an acceptable level iii. Assume that external systems are insecure. iv. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations v. Do not implement unnecessary security mechanisms. vi. Identify and prevent common errors and vulnerabilities.

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
4	**Operations and maintenance**	i. Treat security as an integral part of the overall system design ii. Reduce risk to an acceptable level iii. Assume that external systems are insecure. iv. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness v. Use common language in developing security requirements vi. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process. vii. Strive for operational ease of use viii. Implement layered security (Ensure no single point of vulnerability) ix. Design and operate an IT system to limit damage and to be resilient in response x. Provide assurance that the system is, and continues to be, resilient in the face of expected threats. xi. Use boundary mechanisms to separate computing systems and network infrastructures.

Mapping Security Principles onto life-cycle security Phases

#	Life-cycle Phase	Security Engineering Principles
4	**Operations and maintenance**	xii. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability. xiii. Strive for simplicity. xiv. Minimize the system elements to be trusted xv. Implement least privilege xvi. Authenticate users and processes to ensure appropriate access control decisions both within and across domains xvii.Use unique identities to ensure accountability.
5	**Disposal**	i. Establish a sound security policy as the “foundation” for design ii. Reduce risk to an acceptable level. iii. Ensure proper security in the shutdown or disposal of a system (consider type of media, sensitivity of data, EoL value of data and applicable infosec frameworks and legal requirements)

Disposal/Destruction Techniques

Clearing – remove data in a manner that end users cannot easily recover it

Digital Shredding/Wiping –overwrites data with other characters

Degaussing – uses strong magnetic fields to rearrange the structure of the HDD so that it can no longer be used

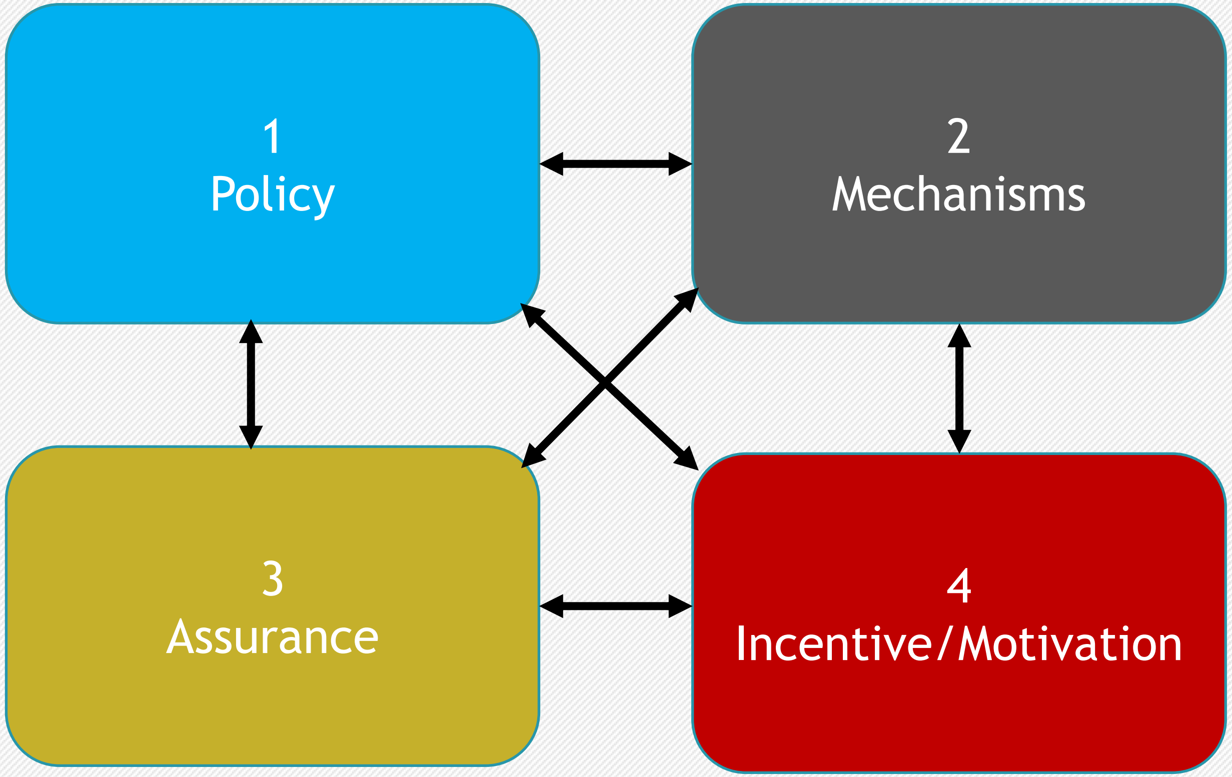
Physical destruction – hydraulic or mechanical crushing in a manner that data can never be used or reconstructed.

Security Engineering Framework

Good security engineering requires the interaction of these four components working together

High-level statements that identifies the organisations intentions on what needs to be achieved

Defines what needs to be done to implement the policy: ciphers, access controls, hardware tamper-resistance and other machinery



1
Policy

2
Mechanisms

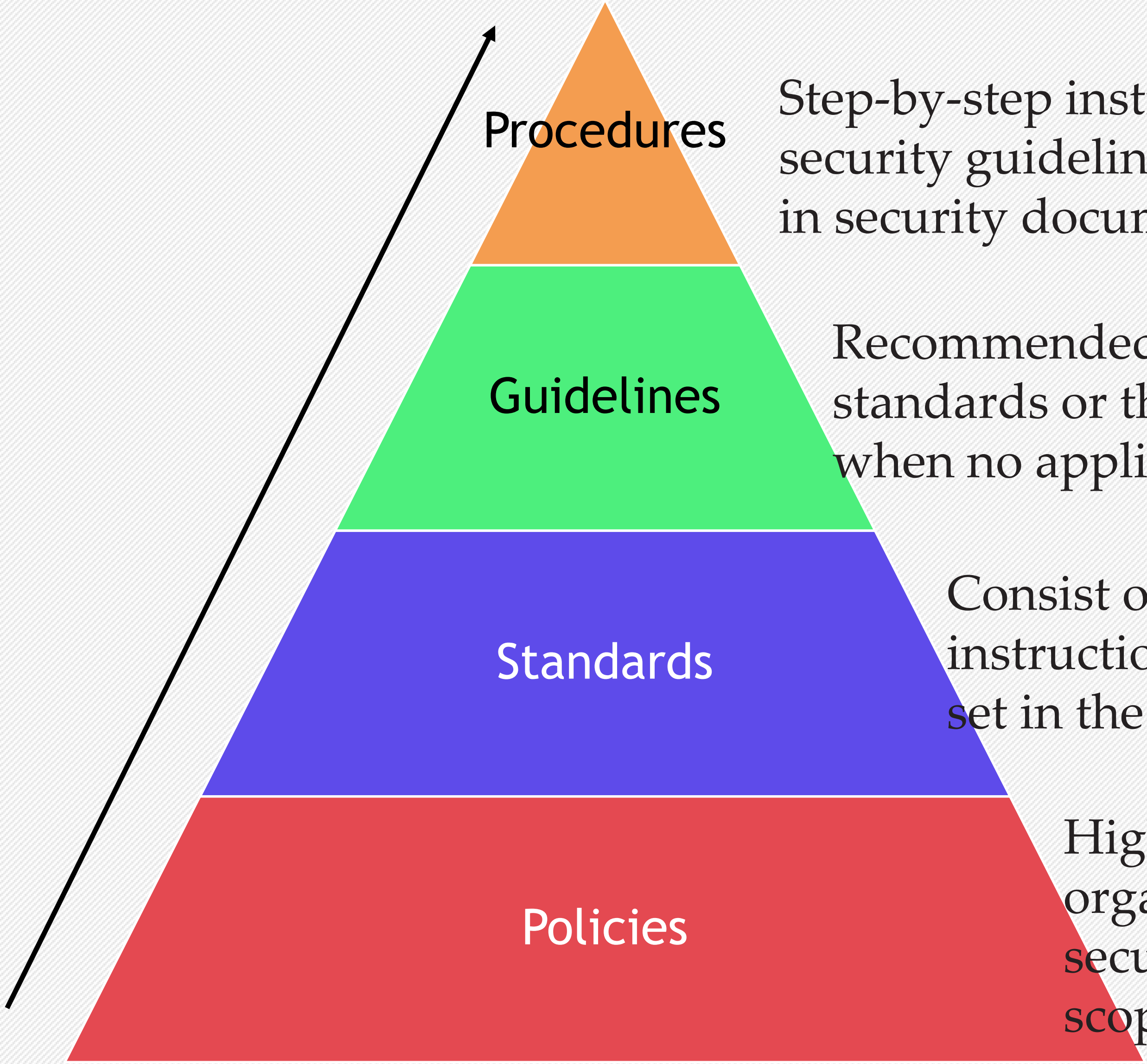
3
Assurance

4
Incentive/Motivation

The amount of reliance you can place on each particular mechanism

the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy

Security policies



Step-by-step instructions on task required to implement the security guidelines, standards and policies. The lowest level in security documentation.

Recommended, non-mandatory controls that supports standards or that provide a reference for decision making when no applicable standard exists.

Consist of specific/obligatory low-level controls, rules, instructions and/or actions required to realise the goals set in the security policy

High-level statements that identifies the organisations intentions or vision concerning the security of its digital assets. It further defines goals, scope and responsibilities.

Four Types of Policies

Programme-level policy

Usually issued by top management of the organisation, contains:

- **Purpose** - defines the **goals** of the security programme e.g CIA, reduction in error, data loss, data corruption; management structure for the management and coordination of resources for the programme.
- **Scope** - specifies the resources covered (facilities, hardware, software), information and personnel.
- **Responsibilities** - addresses the responsibilities of officers and departments/functions throughout the organisation.
- **Compliance** - provides a sanction grid for employees that may violate the policy. As a high level document, it does not provide the details of the sanction grid.

Programme-framework policy

Provides organization-wide direction for broad areas of programme implementation such as:

- **Acceptable use rules** for e-mail, Internet, cell-phones and other wireless devices
- Business continuity planning (BCP) framework
- Physical security requirements framework for data centres
- Application development security framework

Issue-specific policy

- Identifies and defines specific areas of concern and state an organization's position or posture on the issue.
- May come from the head of the organisation, the chief information officer (CIO) or chief information security officer (CISO) depending on kind of issue in question.
- Focus on issues of current relevance to an organisation
- May change frequently due to changes in technology.
- Example of issues that an issue-specifc policy may address include: Email acceptable use, Internet acceptable use, Laptop security policy, Wireless security policy

System-specific policy

System specific policy does the following:

- State security objectives of a specific system
- Define how the system should be operated to achieve the security objectives
- Specify how the protections and features of the technology will be used to support or enforce the security objectives. Examples includes:

✓ Who is allowed to read or modify data in the system?

✓ Under what conditions can data be read or modified?

✓ Are users allowed to connect the computer system from home or on the road?

Issues Specific Security Policies

SN	Policy	Description
1	Acceptable use	Defines the set of rules and restrictions on how users will behave with respect to organisation’s digital assets. It also spells out the consequences for violation.
2	Account management	Defines how administrators manage users’ identity of the enterprise systems: that is; how user identity is created, altered or deleted on the organisation’s system
3	Password	Set rules and restrictions on how users generate and maintain account credentials, such as: minimum number of characters, level of password complexity, frequency of password changed
4	Data ownership	Outlines accountability in terms of information ownership but stating personnel that are responsible for keeping a set of information secure and accessible to authorised users.
5	Data classification	Outlines how organisation defines the different levels of data sensitivity. This is based on which data will generate the most risk when it is leaked, lost or tempered with.
6	Data retention	Outlines when and how organisations should keep or purge data from their systems. This is important when organisations holds PII or PHI
7	Communication	Defines the rules that governs how members of a team should communicate with each other or with external parties. Set boundaries on what should be discussed and provide clear path for escalation

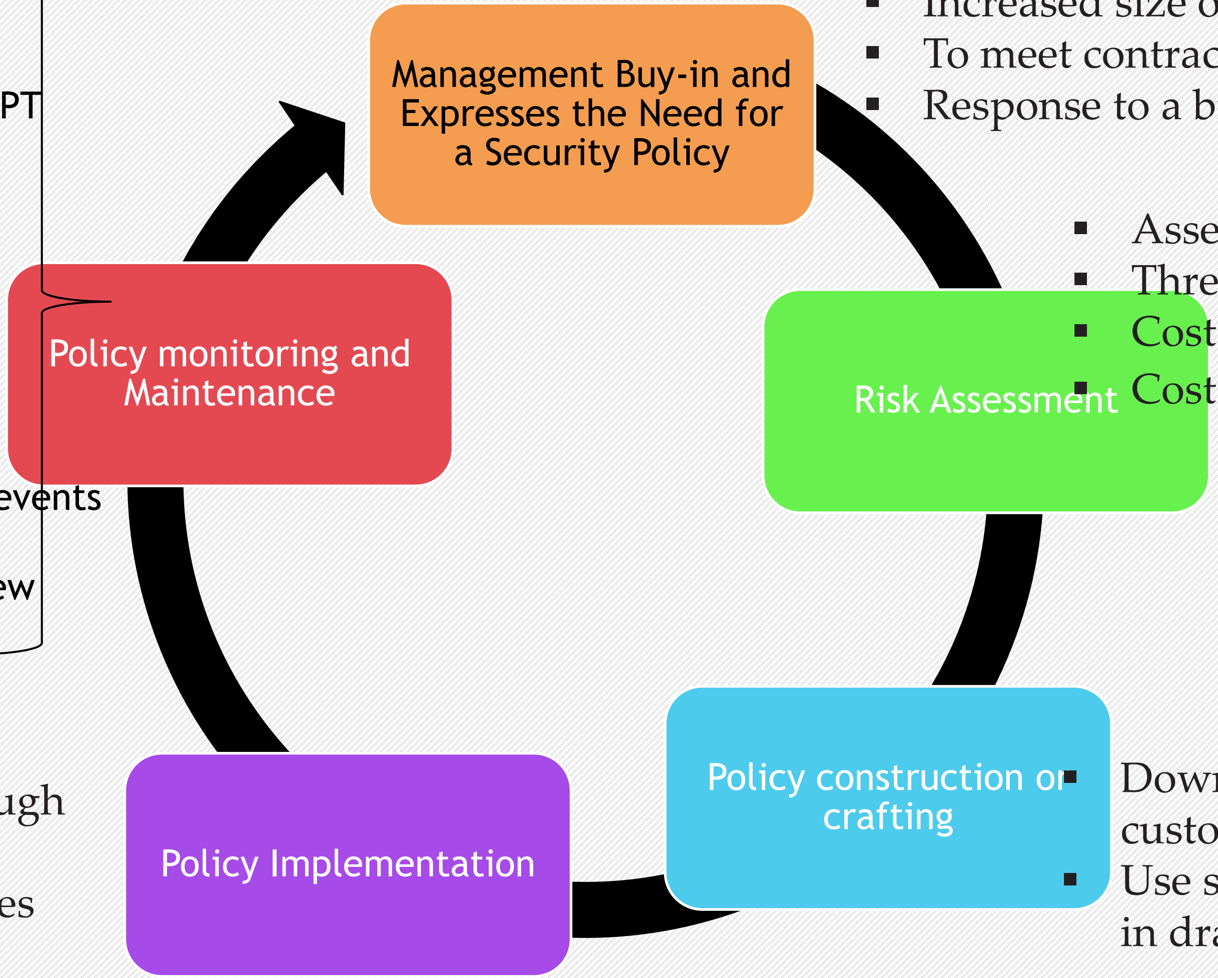
Security Policy Development Life-cycle

Monitoring - to enforce the policy

- Measure users' behaviour
- Perform system audits
- Perform intrusion detection and PT
- User activity audit trail
- Audit policy compliance

Maintenance- Review the following:

- Reports of security incidents
- Security and tech infrastructure
- Business strategies
- Trends analysis and unexpected events
- Legal requirements
- Compile requests for policy review
- Repeat policy life-cycle


Management Buy-in and Expresses the Need for a Security Policy
Risk Assessment
Policy construction or crafting
Policy Implementation
Policy monitoring and Maintenance

- Compliance reasons
- Increased size of organisation
- To meet contractual obligations
- Response to a breach, etc

- Assets identification
- Threats and vulnerability Identification
- Cost of protection
- Cost Benefit Analysis

- Download existing template and customize
- Use security consulting company to aid in drafting a security policy document.

- Define security controls through procedures and guidelines
- Define security responsibilities
- Test security controls
- Implement security control
- Implement security policy training

Content of a Security Policy

Although, information security policy contents varies across organisations, the following generic themes should be considered for addressing the over all risk of the organisation:

- Scope of the security policy
- How information is classified
- Goals for the secure handling of information
- Relationship between other management policies and the security policy
- Reference to supporting documents and other policies
- Specific instructions to handling security issues
- Assignment of specific responsibilities to persons or groups – accountability
- Known consequences to security breach or non-compliance
- Effective and expiration dates

Best Practices to be Incorporated in the Security Policy

The following best practices should be defined in the security policy

SN	Best Practice	Description
1	Separation of concerns	Duties and responsibilities should be separated among individuals in the organisation to avoid abuse. E.g design and development should not be with one person. The roles of backup operator, restore operator and auditor should be assigned to different persons
2	Job rotation	No one person should be allowed to stay on s critical job role for too long. This helps spread vital institutional knowledge among trusted employees and avoid abuses. For instance, firewall administrator and access control specialists job can be rotated
3	Mandatory vacations	This provides the organisation an opportunity to review employers activities. It states that an employee proceeds on at least a 5-days in a row vacation. This enables the audit and security teams review his/her activities.
4	Least privilege	Users should only the system access that is necessary for them to perform their duties. This access includes facilities, hardware, software and information.
5	Incident response	Defines monitoring, response and reporting requirements necessary for incidents that involve security breach or suspected breach. This policy ensures that users are trained to identify incidents and the right reporting hierarchy for all classes of incidents.
6	Forensic tasks	This policy defines who should be notified when forensics are required, conditions upon which they are required, template for contacting those responsible for the forensics,

Best Practices to be Incorporated in the Security Policy – cont’d

SN	Best Practice	Description
7	Employment and termination procedure	Define on-boarding and off-boarding procedure when an employment begins and terminates. On-boarding involves acquainting new employees with security policies. Off-boarding involves ensuring employee relinquish systems access, data and physical equipment. The policy should specify when to enforce non-disclosure agreement.
8	Continuous monitoring	This policy outlines the tools and mechanisms to continuously monitor the systems for changes that have potentials to increase the risk of the system. It defines what events and environment to be monitored based on the knowledge of what is considered abnormal.
9	Training and awareness	This policy is made to ensure comprehensive education of users to protect the system from user-based attacks through social engineering, educate them about the policies and procedures required to operate safely. Onscreen messaging at log-on, pamphlets,
10	Auditing requirements and frequency	Defines the kind of audits, who performs them and the frequency of their performance as well as delineating the authorities for remediating issues raised by the auditors.
11	Information classification	Policy should define which information should be mapped into the various information classification categorisation: public, private, restricted and confidential. Organisations may create their own categorization schemes.

Security Standards and Frameworks

security standards and frameworks are designed to help organisations define their cybersecurity goals and provide a road map on how to achieve these goals. The table below briefly discusses some of these standards and frameworks. Note that standards, frameworks and best practices are optional for organisation to follow.

SN	Standard/framework	Description
1	NIST cybersecurity framework	Developed by the National Institute for Standards and Technology (NIST). The framework seeks to adopt common language for best practices in the cybersecurity realm to enable organisations can apply its guidance in their specific environments. It is made of the **core**, **profile** and the **tiers**
2	RMF	Risk management framework (RMF) developed by the NIST and used by US DoD develops the processes for integrating information assurance and risk management strategies into the systems development life-cycle (SDLC)
3	COBIT	Control Objectives for Information and related Technologies, developed by ISACA provides a framework for IT management and governance. It based on five principles: meeting stakeholders needs; covering the organisation end-to-end; applying single, integrated framework; enabling a holistic approach; and separating governance from management
4	ITAF	The Information Technology Assurance Framework (ITAF), published by ISACA provides guidelines for the roles and responsibilities of auditors and guidance for the overall audit process.

Security Standards and Frameworks

security standards and frameworks are designed to help organisations define their cybersecurity goals and provide a road map on how to achieve these goals. The table below briefly discusses some of these standards and frameworks.

SN	Standard/framework	Description
5	ISO/IEC/27000 Series	Developed by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is a large family of ICT security standards. 27000 –IT security and vocabulary; 27001 - information assurance principles and processes; 27033 – network security; 27044 – data storage security.
6	Standard of Good Practice for Information Security	Created by Information Security Forum (ISF) help business understand and address evolving security issues in compliance, threat and risk management.
7	CIS Control	Centre for Internet Security (CIS) list 18 Critical Security Controls. E.g data protection, malware defence, access control management, etc
8	RFC 2196	Also called Site Security Handbook. This Request for Comments (RFC) provides guidance for securing sites that have Internet-connected systems. It provides best practices for policy writing, network and systems security, incident response.

Privacy Laws and Regulations – Local Laws

While standards, frameworks and good practices are optional for organisations to follow, laws and regulations within the jurisdiction which organisations operate must be followed. These laws and regulations have impact on the risk assessments of such organisations.

#	Law/ Regulation	Description
1	Cybercrime Act 2015	The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also ensures the Protection of critical national information infrastructure (CNII), and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.
2	Credit Reporting Act 2017	The Credit Reporting Act 2017 in the financial services sector, promotes access to credit information. Amongst other things, it protects the confidentiality right of data subjects, including the right to consent and right to accurate personal information.
3	National Health Act 2014	The National Health Act 2014 requires health services providers to keep records of patients' personal information by storing every user's health record safely and in strict confidentiality

Privacy Laws and Regulations – Local Laws – cont’d

#	Law/ Regulation	Description
4	NIMC Act 2007	No person or body corporate shall have access to the data or information contained in the database with respect to registered individual entry except with the authorization of the commission which will be based on the consent of the individual or on account of national security, prevention or detection of crime section 26(1-3)
2	FIRS Act 2007	A person in possession of or control, of any document; information, return of assessment list or copy of such list relating to the income or profits or losses of any person, who at any time communicates or attempts to communicate such information or anything contained in such document, return, list or copy to any person-section 50(2)
3	Constitution of the FRN 1999	The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected- section 37

Privacy Laws and Regulations – Local Regulations

#	Law/ Regulation	Description
1	Nigerian Data Protection Regulation (NDPR), 2019	Nigerian Data Protection Regulation, 2019 (NDPR) which was issued by the National Information Technology Development Agency (NITDA). The Nigerian Data Protection Regulation 2019 was made by virtue of the National Information Technology Development Agency Act 2007. While the NDPR is very similar to the EU-GDPR, it is not a law emanating from a legislative process.
2	The Consumer Code of Practice Regulation (CCPR), 2018	The Consumer Code of Practice Regulation (CCPR) was issued by the Nigerian Communications Commission (NCC) in 2018. The CCPR provides that all licensees, that is, the telecoms service providers who are data controllers over the data provided them by subscribers or customers must take reasonable steps to protect customer information against 'improper or accidental disclosure' and must ensure that such information is securely stored. It also provides that customer information must 'not be transferred to any party except as otherwise permitted or required by other applicable laws or regulation.
3		