

Setting the Scene

ST2610

Security Policy & Incident Management (SPIM)

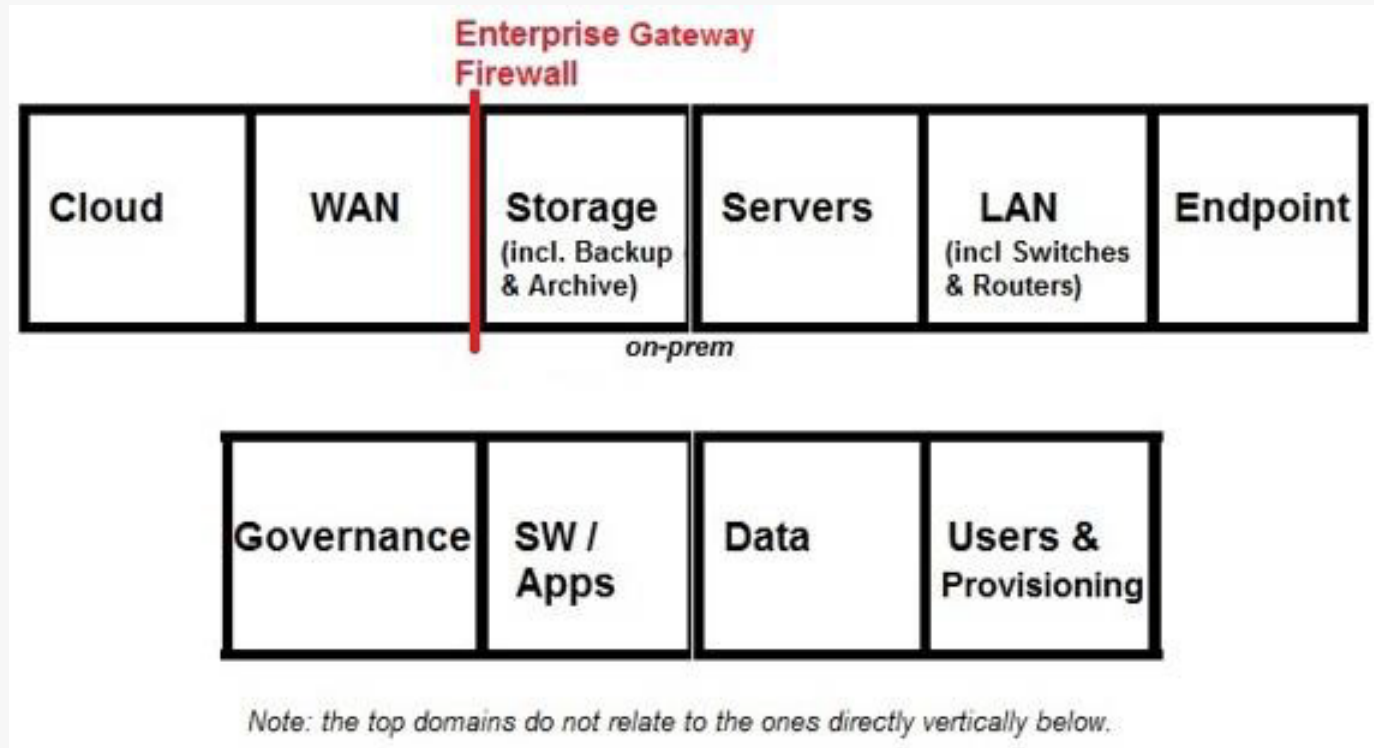
“Hi there, Cybersecurity Manager”

- Boss: “My company needs cybersecurity.”
- Boss: “Now, secure my enterprise.”

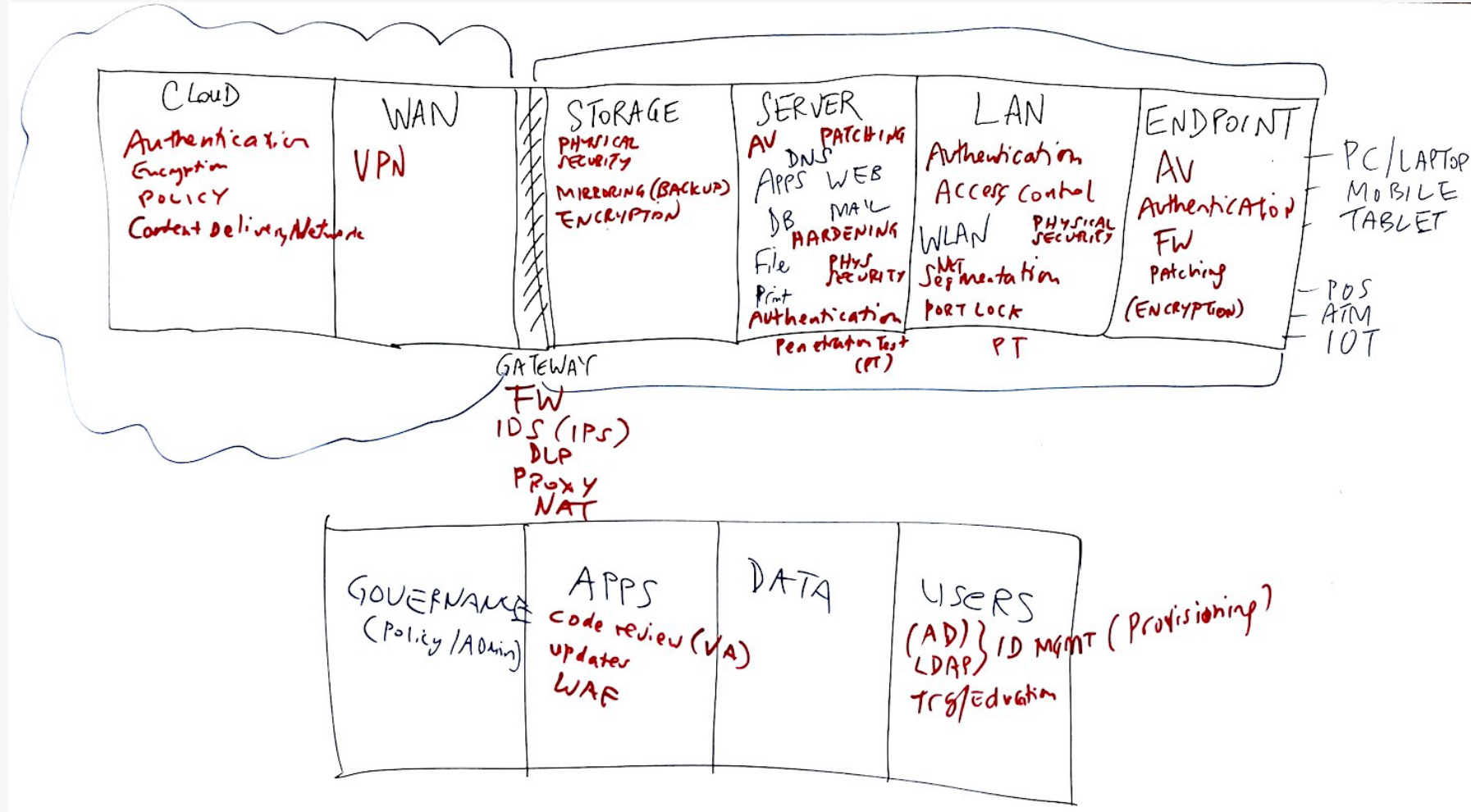


Class Activity Discuss how would you approach this problem.

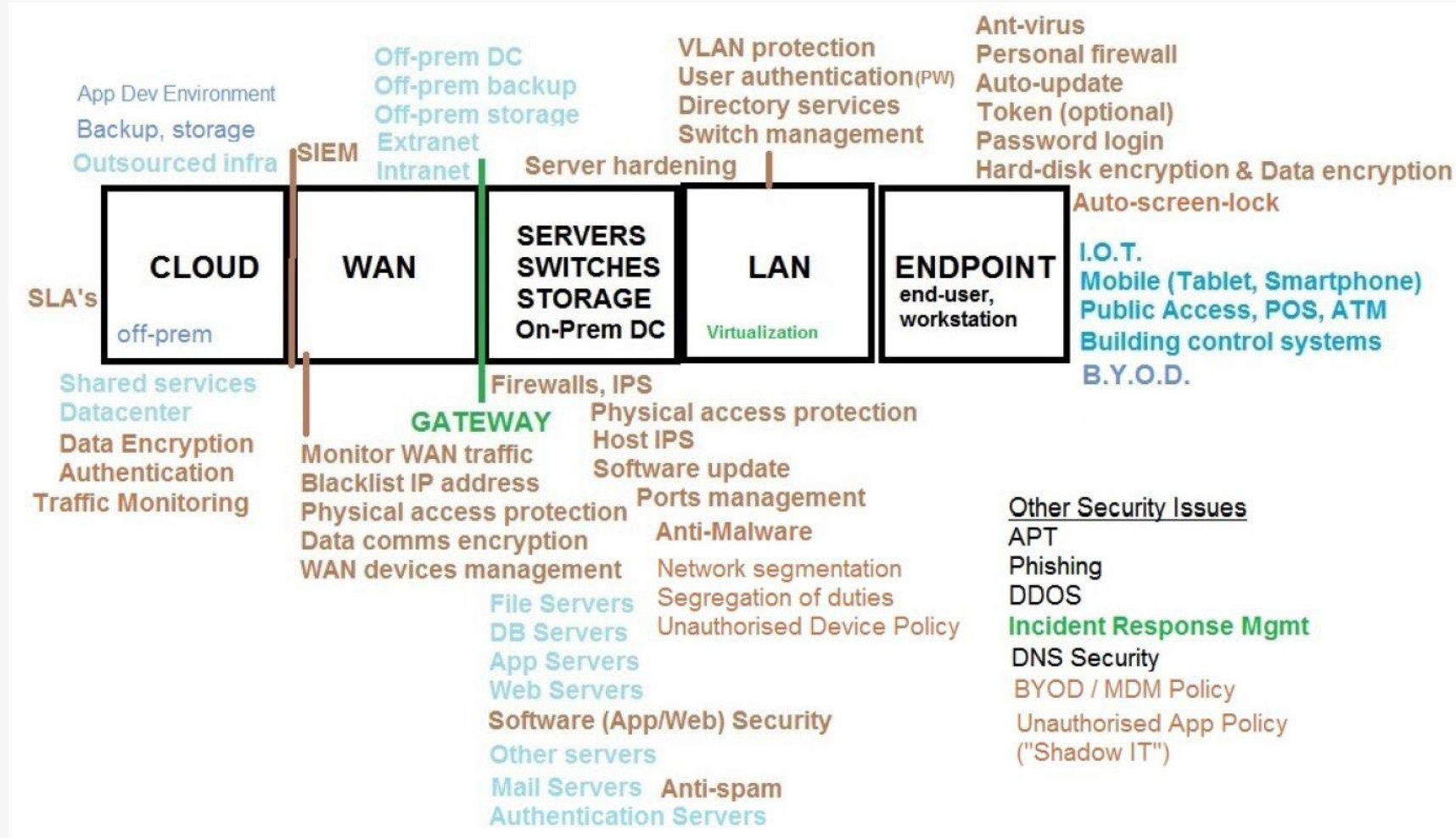
Enterprise IT Infrastructure | an e.g.



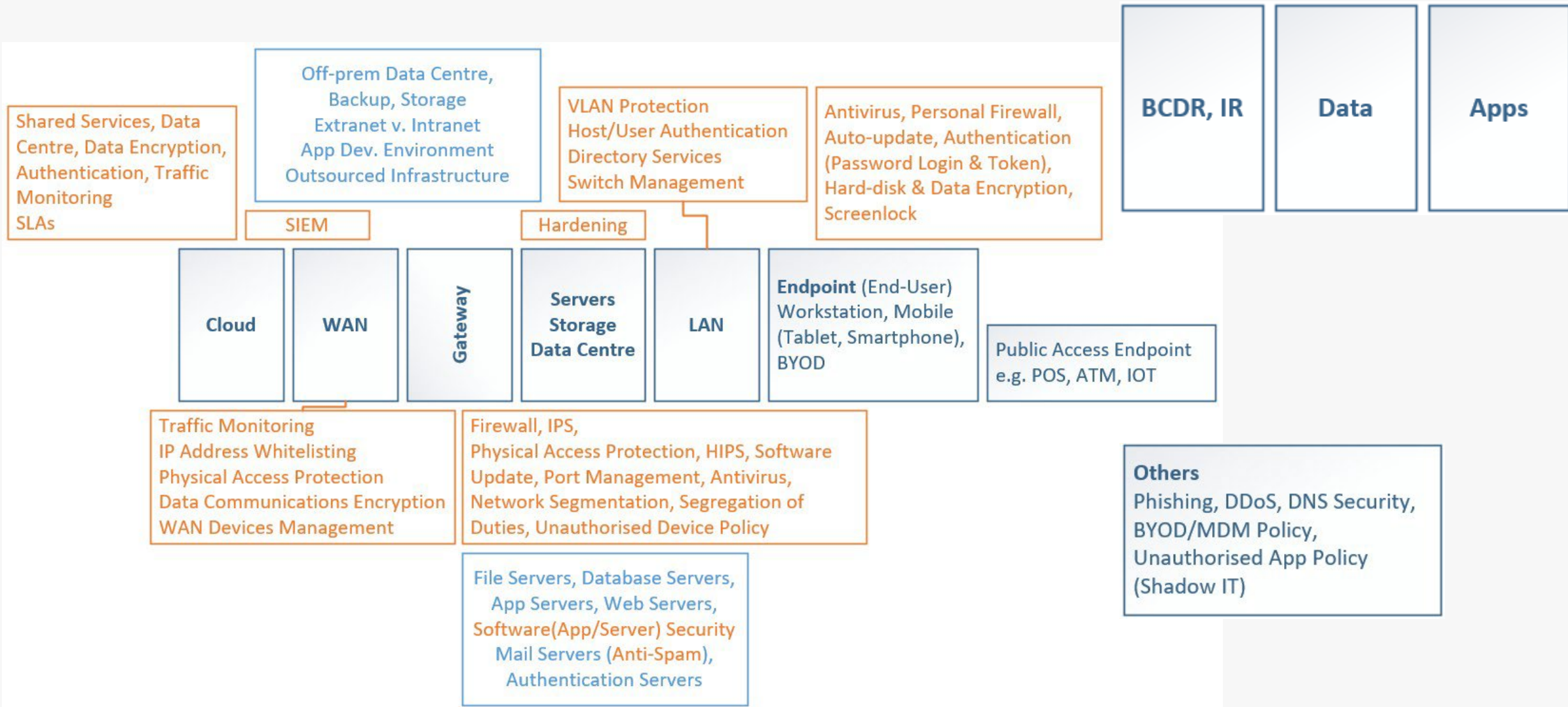
Enterprise IT Infrastructure | an e.g.



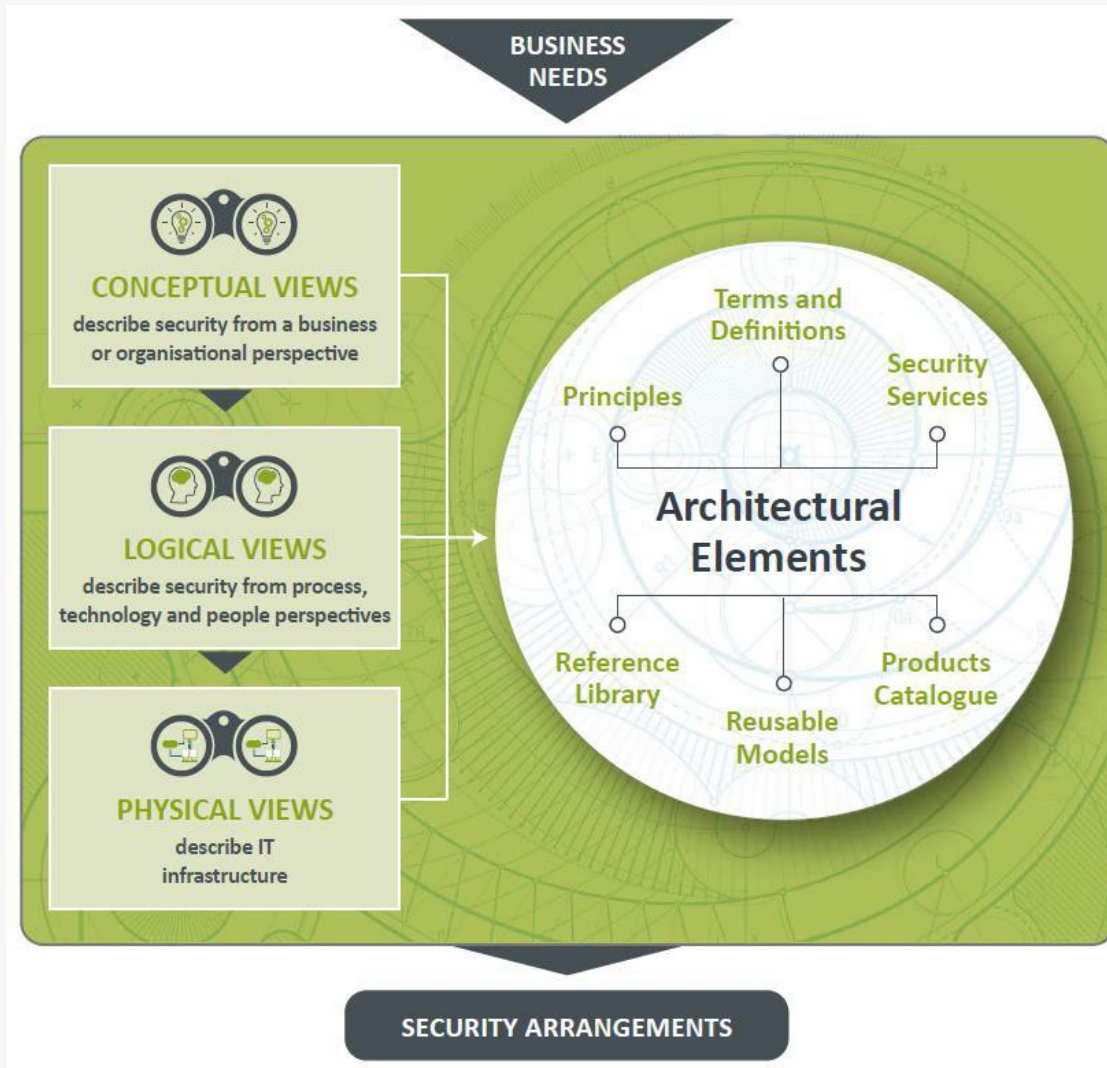
Enterprise IT Infrastructure | an e.g.



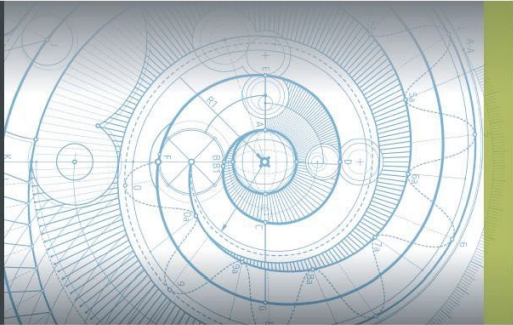
Enterprise IT Infrastructure | an e.g.



Business & Security Architecture



ISF Information Security Forum



SECURITY ARCHITECTURE

Navigating complexity

Global information security spending across all market segments reached approximately US\$75 billion last year, and is projected to grow nearly 8% by 2019.¹ To safeguard a return on this investment, many organisations are turning to security architecture.

Advocates claim many benefits, including cost efficiencies, improved alignment between business and IT, process refinements, enhanced capacity for change, and a basis upon which information risk management practices can be improved.

Detractors on the other hand, claim that security architecture can take too long, cost too much, frustrate senior managers, and limit flexibility and innovation.

Given this contradiction, how can organisations unlock and realise the potential value of security architecture?

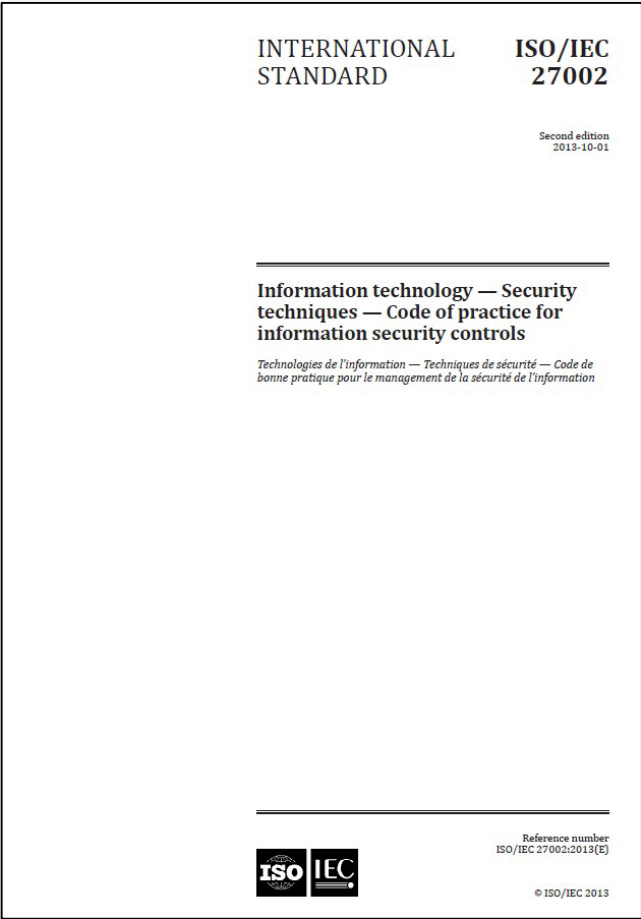
The ISF report *Security Architecture: Navigating complexity* answers this important question. It demystifies security architecture and conveys six lessons uncovered by ISF research. It provides a flexible approach for developing and using security architecture that can be tailored to suit the diverse needs of organisations.

Organisations that better understand security architecture are using it to navigate the complexity inherent in today's interconnected world. These organisations are unlocking value and providing a sound basis for protecting their business against ever-more sophisticated cyber security threats.

Business & Security Architecture



ISO/IEC 27002:2013



Contents	Page
Foreword	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this standard	1
4.1 Clauses	1
4.2 Control categories	1
5 Information security policies	2
5.1 Management direction for information security	2
6 Organization of information security	4
6.1 Internal organization	4
6.2 Mobile devices and teleworking	6
7 Human resource security	9
7.1 Prior to employment	9
7.2 During employment	10
7.3 Termination and change of employment	13
8 Asset management	13
8.1 Responsibility for assets	13
8.2 Information classification	15
8.3 Media handling	17
9 Access control	19
9.1 Business requirements of access control	19
9.2 User access management	21
9.3 User responsibilities	24
9.4 System and application access control	25
10 Cryptography	28
10.1 Cryptographic controls	28
11 Physical and environmental security	30
11.1 Secure areas	30
11.2 Equipment	33
12 Operations security	38
12.1 Operational procedures and responsibilities	38
12.2 Protection from malware	41
12.3 Backup	42
12.4 Logging and monitoring	43
12.5 Control of operational software	45
12.6 Technical vulnerability management	46
12.7 Information systems audit considerations	48
13 Communications security	49
13.1 Network security management	49
13.2 Information transfer	50
14 System acquisition, development and maintenance	54
14.1 Security requirements of information systems	54
14.2 Security in development and support processes	57
14.3 Test data	62
15 Supplier relationships	62
15.1 Information security in supplier relationships	62
© ISO/IEC 2013 - All rights reserved	III

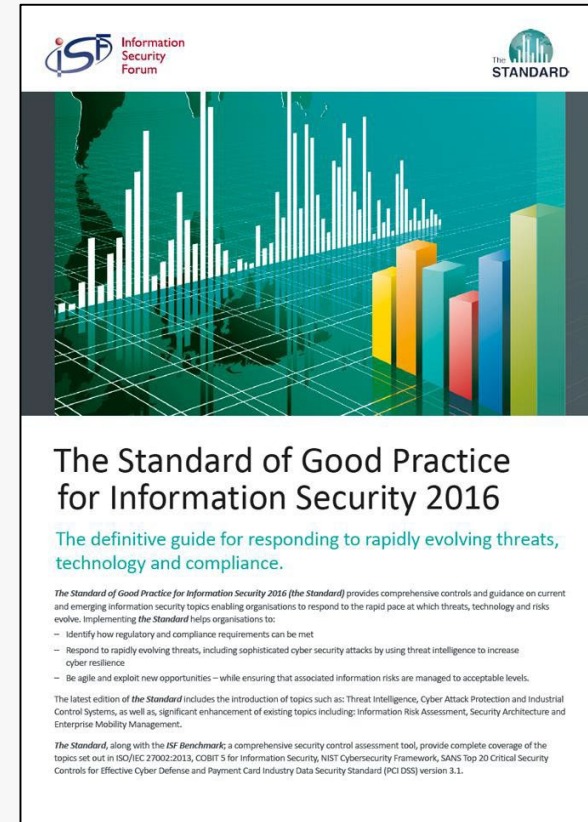
ISO/IEC 27002:2013(E)	
15.2 Supplier service delivery management	66
16 Information security incident management	67
16.1 Management of information security incidents and improvements	67
17 Information security aspects of business continuity management	71
17.1 Information security continuity	71
17.2 Redundancies	73
18 Compliance	74
18.1 Compliance with legal and contractual requirements	74
18.2 Information security reviews	77
Bibliography	79

CIS Critical Security Controls



Standard of Good Practice (SOGP)

- Security Governance
- Information Risk Assessment
- Security Management
- People Management
- Information Management
- Physical Asset Management
- System Development
- Business Application Management
- System Access
- System Management
- Networks and Communications
- Supply Chain Management
- Technical Security Management
- Threat and Incident Management
- Business Continuity
- Security Monitoring & Improvement

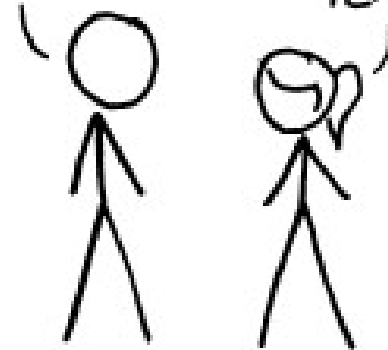


HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

How Much Is Enough?

- **Governance, Risk, Compliance (GRC)**

- Compliance must never be the 1st consideration

- **Enterprise Risk Management (ERM)**

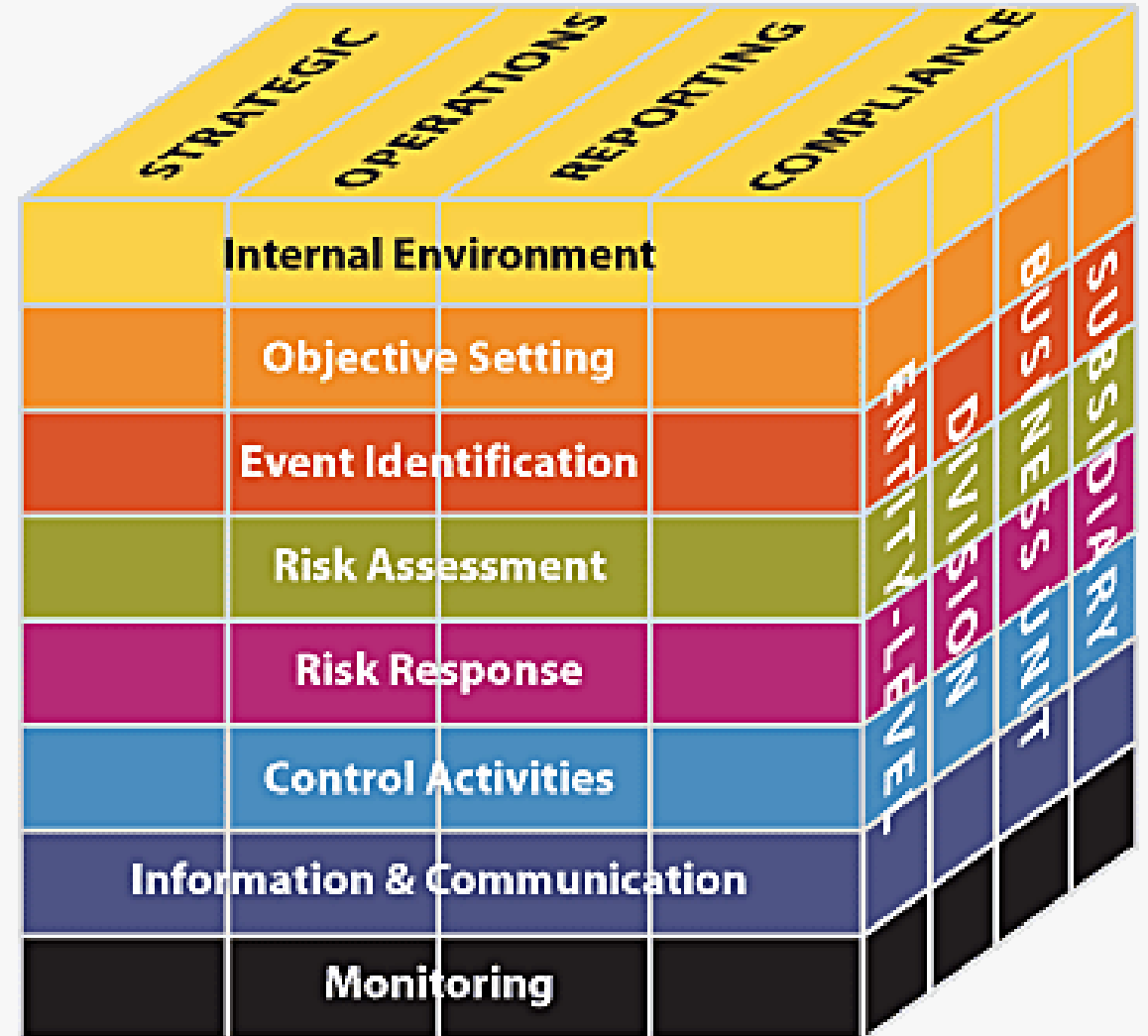
- Top management recognise that cybersecurity issues can impact business operations.
 - “A **process**, effected by an entity’s board of directors, management and other personnel, applied in **strategy-setting** and **across the enterprise**, designed to **identify potential events** that may affect the entity, and **manage the risk** to be within its **risk appetite**, to provide **reasonable assurance** regarding the achievement of entity objectives.”

Committee of Sponsoring Organisations (COSO)

ERM Integrated Framework

The COSO Cube

- To help assist with the implementation of ERM process
- Each of these components are considered at multiple levels of the organisation, rather than a single function, unit or department



ERM Integrated Framework (cont'd)

The COSO Cube

What It Is

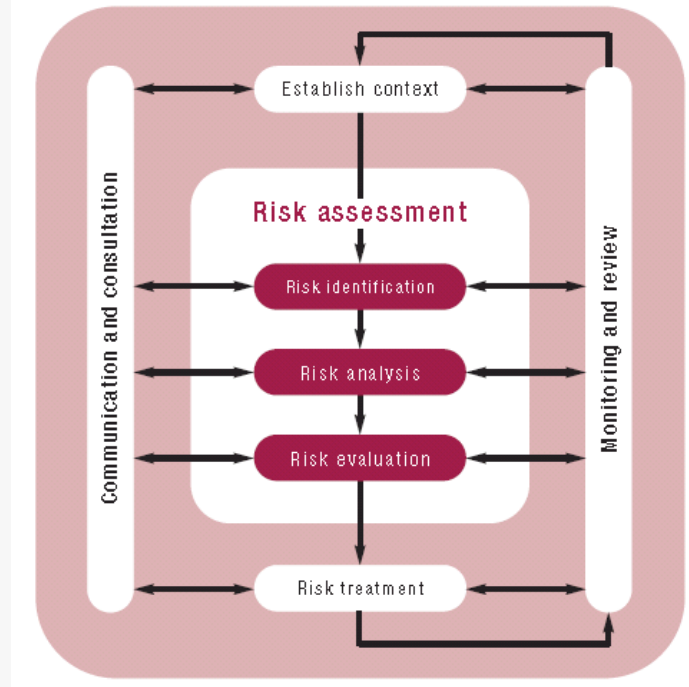
- Provides a comprehensive and systematic approach to a more proactive and holistic risk management
- Provides a common lexicon of risk terminology, and provides direction and guidance for implementing ERM
- Requires that organisations examine their complete portfolio of risks, consider how those risks interrelate, and that management develops an appropriate risk mitigation approach to address these risks in a manner that is consistent with the organisation's strategy and risk appetite

What It Is Not

- A silver bullet to prevent risks from occurring
- A methodology or a checklist of items that need to be completed that guarantee results
- The only way organisation can take a more proactive approach to managing risk

ISO 31000 – Risk Management

- Provides a universally recognised paradigm for practitioners and companies employing risk management processes across different industries, subject matters and regions.
- “A **process** that provides **confidence** that planned objectives will be achieved within an **acceptable degree of residual risk**.”

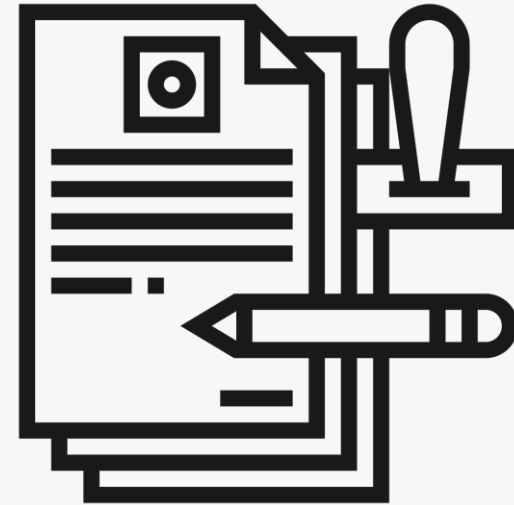


Wicked Problem

- Cybersecurity can be thought of as a wicked problem
- Wicked Problem
 - Problems that are **difficult to define**, and have other **complicating characteristics** that inhabit overarching insights and silver bullet solutions.
 - A wicked problem is a problem that is **difficult or impossible to solve** because of **incomplete, contradictory, and changing requirements** that are often difficult to recognise. The use of the term “wicked” here has come to denote **resistance to resolution**, rather than evil. Moreover, because of **complex interdependencies**, the **effort to solve one aspect of a wicked problem may reveal or create other problems**.

Key Cybersecurity Management Instrument

– **Policy**



Lesson 1

Introduction to Policy

Module 4

Security Policy & Incident Management (SPIM)

Examples of Policies

- Information Classification Security Policy
- Acceptable Use Policy (AUP)
- Network Security Policy
- Wireless Security Policy
- Remote Access Policy
- Software Security Policy
- Web Security Policy
- Extranet Policy
- Access Control Policy
- Authentication Policy
- Email Security Policy
- Security Awareness Policy
- Incident Management Policy
- Business Continuity and Disaster Contingency Policy

Compliance Hierarchy & Other Considerations

– Compliance Hierarchy

1. Common Law
2. Law of the Land
3. Protocol
- 4. Policy**
5. Procedure
6. Process
7. Blueprint
8. Framework & Methodology
9. Guideline & Best Practices
10. Plan
11. Standards
12. Principles

– Other Considerations

- Rules & Regulations
- Directive / Directions
- Circular
- Notice
- Instructions
- Policy

- Audit & Compliance

No. 1 – 3 are beyond organisational control

No. 5 – 12 are not mandatory

Fire-Fighting Protocol

If there is a fire in a data-centre, Network Operations Centre (NOC) or computer centre, which would be the preferred first-resort fire-fighting solution built into the facility?

- a. Water sprinkler system
- b. Halon gas / powder system
- c. High-pressure extractor system (sucks the flames and fumes out of the building)

Fire-Fighting Protocol (cont'd)

In view of a data protection and asset (systems, equipment) protection policy, and the conventional thinking of 10 years ago, (a) water sprinkler system will damage the equipment, cause electric shocks, bring systems down and corruption or loss of data.

(c) High-pressure extractor is unlikely due to cost-of-installation issues, and its efficacy is questionable.

Hence, (b) halon gas / powder system is the most suitable answer because halon can put out the fire but without the risks that the water option brings.

Fire-Fighting Protocol (cont'd)

But today, the consideration would be different.

(b) halon gas / powder system is effective and well-associated with computer centres, but is harmful to personnel therein.

(c) High-pressure extractor is also known to be harmful to personnel therein, as the flames are hot and dangerous fumes are being sucked away at high speed and pressure.

Hence, (a) water sprinkler system is the best answer, in view of least likelihood of endangering personnel therein. i.e., we will accept the risks to damage and loss from the water regarding the assets.

Fire-Fighting Protocol (cont'd)

In today's modern data-centres, NOC and computer centres, we expect an active and automated (hot) backup and high-availability (HA), disaster recovery (DR) and business continuity (BC) services or facility are in place elsewhere so that in case of a fire here, the services can be quickly restored or continued with minimal disruption, the data will be safe, and the lost assets can be replaced if it can't be salvaged, serviced or required.

The protocol element here is the prioritisation of the preservation of human lives, over the policy or desire to minimise data loss and financial loss due to service disruption or damage of equipment.

Policy | A Management Instrument

- Focuses on the **why** and **what** to do, and **doing the right things**
 - Rather than **how** to do, and **doing things right**
- Document
 - Formal Structure / Manner, not email
 - Can be Electronic Format e.g. .doc, .ppt, .html, etc.

Policy – Definitions

- A **course or principle of actions** adopted or proposed by an organisation or individual.
- A set of ideas or a plan of what to do in a **particular situations** that **has been agreed to** officially by a group of people, a business organisation, a government, or a political party.

Cambridge English Dictionary

- A set of policies are principles, rules and guidelines formulated or adopted by an organisation to **reach its long-term goals** and typically **published** in a booklet or other form that is **widely accessible**.

Business Dictionary

- A plan or course of action, as of a government, political group, business or other organisation, intended to **influence and determine, decisions, actions**, and other matters.

American Heritage Dictionary

(Cyber)/Information Security Policy

- A set of mechanisms by which an organisation's information systems security **objectives** can be **defined** and **attained**.
- Practically speaking ... A **published document** (or set of documents) in which the organisation's **philosophy, strategy, policies and practices** with regard to **confidentiality, integrity and availability** of **information and information systems** are **laid out**.
- Information Security Policy Document
 - A document that states how an organisation plans to protect the organisation's assets
 - High-level statements that provide guidance to workers

(Cyber)/Information Security Policy

(cont'd)

- A formal, belief and **high-level statement** or plan that **embraces** an organisation's general beliefs, goals, objectives and acceptable procedures for a **specific subject area**.

SANS Institute

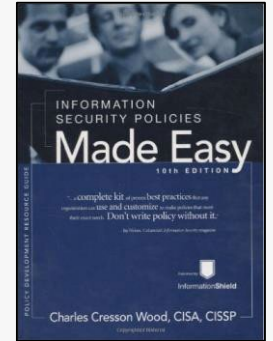
- A policy sets out an organisation's **aims, principles and approach**. It **specifies what is required** to be achieved or delivered **without prescribing** how it is to be carried out. A policy can be fulfilled by one or several processes working in unison. Policy requirements are typically expressed in **simple single statement** format or limited to short paragraphs comprising of a few statements.

Business Continuity Management (BCM) Institute

"If you can't explain it simply, you don't understand it well enough."
Albert Einstein

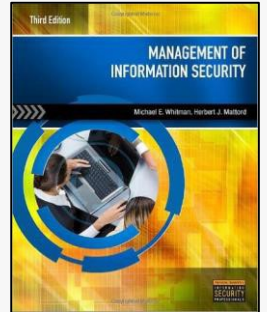
Need for Policy

- “... Policies are important **reference documents** for internal audits and for the resolution of legal disputes about management’s **due diligence** [and] policy documents can act as a **clear statement of management’s intent** ...”



Need for Policy (cont'd)

- “However, **policy isn’t just a management tool to meet legal requirements**. It’s necessary to **protect the organisation** and the jobs of its employees.
- Consider this scenario: An employee behaves inappropriately in the workplace, perhaps by viewing unsuitable web pages or reading another employee’s email. Another employee is aggrieved by this behaviour and sues the company. The company does not have policy that prohibits the behaviour, so any direct action against the offending employee risks further litigation. The lawsuit is settled in the disgruntled employee’s favour, and the resulting judgement puts the organisation into bankruptcy. Once the organisation goes out of business, the rest of the employees lose their job – all because the company did not have effective policies in place that would have enabled it to terminate the misbehaving employee.”



Policy Breakdown / Compliance Paradox

- Spirit of the Law v. Letter of the Law
- When a situation occurs and the policy does not know how to deal with it or ends up with inefficiency and causing other problems.
- e.g.
 - Marina Bay Sands (MBS) Casino \$100 entry charge v. Broken down lift
 - Car exiting car park, and not having enough value in the cash card
 - School's No Hair-Dye-Colour Policy
v. Chinese girl with natural brown hair forced to dye to black
 - Restaurants' No-Outside-Food Policy v. Broken Rice Cooker
 - Complicated Password Policy

Non-Compliance

- Not the same as Policy Breakdown / Compliance Paradox

- Rule by Exception

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle.”
Sun Tzu, The Art of War

- Revisit your policies if there are too many exceptions

Soft Components of a Policy

- Philosophy
 - Organisation's **approach** towards information security, the framework, the guiding **principles** of the information security strategy. The security philosophy is a big umbrella under which all other security mechanisms should fall. It will explain to future generations **why you did what you did**.
- Strategy
 - **Plan** or the **project plan of the security philosophy**. A measurable plan detailing **how** the organisation **intends to achieve the objectives** that are laid out, either implicitly or explicitly, within the framework of the philosophy.
- Policies
 - Simply **rules**. They are the dos and don'ts of information security, again, within the framework of the philosophy.
- Practices
 - **The how** of the organisation's policy. They are a practical guide regarding what to do, and how to do it.

Recap: Practically speaking ... A published document (or set of documents) in which the organisation's philosophy, strategy, policies and practices with regard to confidentiality, integrity and availability of information and information systems are laid out.

3 Important Attributes of a Policy

- Must be **Implementable & Enforceable** (i.e. doable)
 - If not, users will
 - Not take the policy seriously
 - Try to bypass or cheat
 - Do other things to just comply
- Must be **Concise & Easy to Understand**
 - For maximum coverage or ability to comply
 - If not, users may
 - Misinterpret
 - Not take the policy seriously
- Must **Balance Security with Productivity**
 - If not, users will
 - Try to bypass or cheat
 - Do other things to just comply

Seemingly Harmless but Unreasonable Clause

- Massachusetts's Office of Consumer Affairs & Business Regulation
 - 201 CMR 17.00 – Regulations on the Protection of Personal Information
- §17.05(5) – Requires **encryption** of personal identifiable data on laptops
- §17.02 – Definition of Encryption
 - “The transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning **cannot** be assigned without the use of a confidential process or key ...”
 - A breakable algorithm does not satisfy the ‘cannot’ requirements
 - Unreasonableness – Few (if available) algorithms are literally impossible to break forever

Benefits of Policies

- Management's Involvement
 - Development of a policy includes the ancillary benefit of making upper management aware of and involved in information security. This should make it a higher organisational priority, which can only increase the level of security throughout the company.
- Exemplify an organisation's commitment to security
- Provide paper trail to prove due diligence

– **5 Practical Benefits of Security Policies**

- They form a benchmark for progress measurement
- They help ensure consistency
- They serve as a guide to information security
- They define acceptable use
- They give security staff the backing of management

2nd Nature to Risk Management

- An integrated documented management system needs to be an integral part of the organisations' day-to-day operations
 - i.e. the business's 2nd nature focused on risk management
- When the management system becomes 2nd nature within the business activities, it minimises the frequency of dealing with “surprises”

Inadequate Documentation

- US' Code of Federal Regulation (CFR)
- 17 CFR §248.30 Procedures to safeguard customer records and information; disposal of consumer report information
 - (a) Every broker, dealer and investment company, and every investment adviser registered with the Commission **must adopt written policies and procedures** that address **administrative, technical, and physical safeguards** for the **protection of customer records and information**. These written policies and procedures must be reasonably designed to:
 - (1) Insure the security and confidentiality of customer records and information;
 - (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
 - (3) Protect against unauthorised access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Inadequate Documentation (cont'd)

- 2010, the **Financial Industry Regulatory Authority (FINRA)** fined **D.A. Davidson & Co.** US\$375,000 after a hacker stole personal data of 192,000 Davidson customers.
- Key Reason – Davidson's security documentation was incomplete
 - "... failed to ... establish and maintain a system, including written supervisory procedures, reasonably designed to achieve compliance with 17 CFR §248.30 ..."
- Davidson ...
 - Have a security programme
 - Cybersecurity mechanisms are in place
 - Regularly review logs
 - Engage with security auditors and consultant, and had implemented majority of their recommendations
 - Responded well when the incident happened
 - Prevention and mitigation steps, incident management, contacting law enforcement, hiring experts, etc.
- Still ... the other reasons
 - IDS had not been implemented
 - Failed to encrypt a database containing non-public customer information
 - Failed to require a password to access a database containing non-public customer information

4 Key Components of a Security Policy & Manual Framework

1. Policy
 - What behaviour are we trying to govern?
2. Standards
 - Specifies minimum requirements in a policy
 - What are the responsibilities that each individual must meet for compliance?
3. Guidelines
 - Suggestions for best ways to accomplish a task
 - Help to conform to a standard
 - What are the general technical requirements for individuals or devices to be compliance with the policy?
4. Procedures
 - A method by which a policy is accomplished
 - Instructions to carry out a policy
 - Focus on actions and steps
 - What are the general technical requirements for individuals or devices to be compliance with the policy?



Password Policy | an e.g.

1. Policy

- All users must have a unique username and password that conforms to the secure password standard
- Users shall not share their passwords

2. Standard

- Passwords should meet the following standards:
 - Minimum of 8 alphanumeric characters
 - Changed every 90 days

3. Guideline

- A good way to create a strong password is to think of a phrase like “My favourite town is Yishun”.

4. Procedure

- To change passwords, press the Ctrl, Alt and Delete keys together
- Click on “Change Password”

Process v. Procedure

- Process

- A **set of activities** or **tasks** with **defined outcomes, deliverables** and **evaluation criteria** to **fulfil the requirements** of a certain policy or part of it thereof. It can also include determining and establishing the requirements to fulfil a certain policy first before undertaking the set of activities or tasks.

- Procedure

- A **sequence of small tasks** or **detailed steps** taken to accomplish a certain process or a particular goal.

Requirement Levels Lexicon

Ref: RFC 2119

- **Must, Required** or **Shall** – An absolute requirement of the specification.
- **Must Not** or **Shall Not** – An absolute prohibition of the specification.
- **Should** or **Recommend** – There may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **Should Not** or **Not Recommended** – There may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighted before implementing any behavior described with this label.
- **May** or **Optional** – An item is truly optional.

Policy Headers / Template | Logistics

1. Owner * IMPORTANT
 - Originating Owner, Issuer, Writer, Department, including Contact Information
 - Define Contacts and Authority Responsibilities
 - Can be a Person, a Department, or Organisation
2. Date of Issue * IMPORTANT
 - May contain Original Date of Issuance, but Latest Date of Policy Document Must be Clear
 - Effective Date of Implementation
3. Version No. & Revision History * IMPORTANT

Policy Headers / Template | The Policy

4. Objective / Overview

- Reasons why the policy is needed or what it seeks to govern or enforce
- Why are we implanting this policy? | The Purpose
- What behaviour are we trying to govern? | The Goal
- What conflict or problem does the policy intent to resolve?
- What is the overall benefit?

5. Scope

- Defines what target matters, audience, areas and/or circumstances covered in the policy
- Who must observe the policy | Audience
- Who must understand the policy in order to perform their job?
- Which technologies or groups are included to the policy?

6. Policy Statements

- Forms the bulk of the policy
- Focuses on the specifics of how the policy will be implemented | The Rule
- A systematic list of all the rules and actions to be taken to control the risk associated with an organisation's identified risks

Policy Headers / Template | Interpretation

7. References

- Corresponding standards documentation
- Links to guidelines that relate to the policy statement

8. Glossary

- Defines acronyms and technical terms that enable the reader to better understand the policy

Policy Headers / Template | Enforcement

9. Enforcement

- Identifies the penalties for violating the policy

10. Exception | Linked with 'Scope'

- Defines what target matters, audience, areas and/or circumstances are exempted from the policy

11. Violation Handling

- Defines what consequences will a violator or violation of the policy may face

Structuring a Policy

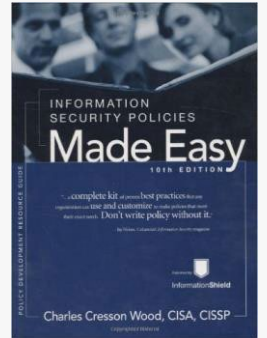
- Simple & Practical
- Lightweight
- Easy to Manage & Maintain
- Easy to Access by People Seeking Specific Information

Recap: 3 Important Attributes of a Policy...

(1) Implementable & Enforceable; (2) Concise & Easy to Understand; (3) Balance Security with Productivity.

Writing a Policy

- Policies e.g.
 - Available on PolyMall
- How to Write an Information Security Policy in 5 Minutes
 - <https://www.youtube.com/watch?v=PIRaC78n9f0>



Policy – Sanity Check

- Does the policy have a clearly defined scope?
 - Is it clear to which system and which people the policy is applicable?
- Is the policy comprehensive in terms of the defined scope it means to address?
 - Are all systems and issues sufficiently covered?
- Does the policy clearly define responsibilities?
 - Is it clear to the end-user, the line manager and the various administrators exactly what his or her responsibilities are?
 - Is it clear who is responsible for various aspects of security?
- Is the policy enforceable?
 - Can it be applied in a concrete manner so that the compliance is measurable?
- Is the policy adaptable?
 - Can it be easily changed to address new risks, threats and technologies?
- Is the policy having its desired effects?
- Is the policy universally known and understood within the organisation?
 - Is the policy well distributed?
 - Is there an awareness programme of the policy?
 - Is the content understood?
- Does the policy comply with law and with duties to 3rd parties?
 - Is the organisation fulfilling its statutory obligations?

Common Cybersecurity Management Problem

- Wrong Scope
- Tackling / Solving the Wrong Problem

Cybersecurity Practice

- The value of information and/or services, and the organisation's commitment to cybersecurity / information security
- The designation of authority to Cybersecurity / Information Security Officer and security-related personnel in the organisation as is appropriate
- The principle of accountability that states clearly that administrators and users will be held accountable for behaviour that impacts the security of the organisation's cyberspace and/or information
- The principle of individual responsibility of all system users for the security of information resources
- The organisation's approach to cybersecurity / information security reviews
 - e.g. How often? Who will perform them? etc.

