

DISCUSSION DOCUMENT

Information Security Policy in Practice

(การนำนโยบายความมั่นคงปลอดภัยสารสนเทศไปใช้ในองค์กร
อย่างมีประสิทธิภาพ)

Pathumwan Princess Hotel
Bangkok, Thailand
1 December 2014

Kitti Kosavisutte, Ph.D.
(kitti.kos@bbl.co.th)

Security Management

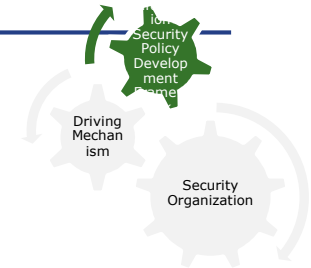


Key Components to Success



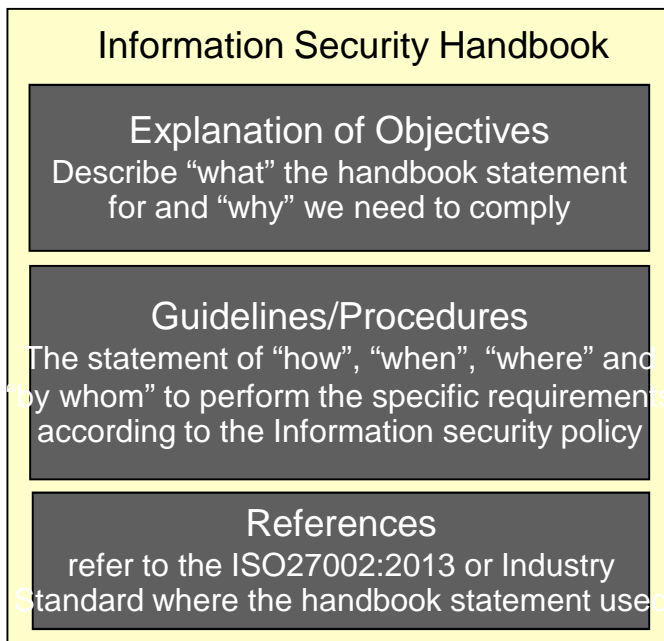
INFORMATION SECURITY POLICY FRAMEWORK DEVELOPMENT

Information Security Policy Development Framework



Governing Policy

Governing Policy: Management intention that states the “what” of a banking mandate with a degree of commitment



Information Security Handbook

Explanation of Objectives

Describe “what” the handbook statement for and “why” we need to comply

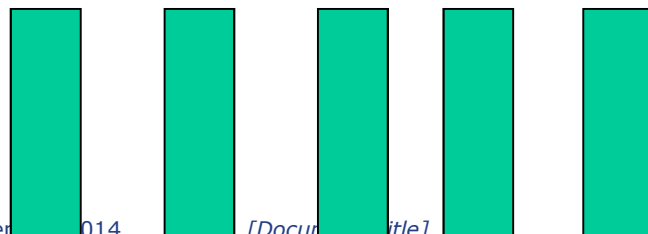
Guidelines/Procedures

The statement of “how”, “when”, “where” and “by whom” to perform the specific requirements according to the Information security policy

References

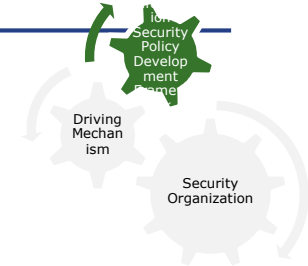
refer to the ISO27002:2013 or Industry Standard where the handbook statement used

Handbook: Requirements and guidance that State “why”, “how”, “when”, “where” and “by whom” of a banking mandate



Standard and Operational Procedure: step-by-step procedure of performing based on handbook

Governing Policy Document Structure



สารบัญ (Table of Contents)

1. บทนำ (Introduction)	5
1.1 บทย่อ (Overview).....	5
1.2 ขอบเขตและจุดมุ่งหมายของนโยบายการรักษาความปลอดภัยข้อมูล (Scope and Purpose of the Information Security Policy)	5
2. วัตถุประสงค์ในการรักษาความปลอดภัย (Security Objectives)	5
3. โครงสร้างและองค์ประกอบพื้นฐานในการรักษาความปลอดภัย (Security Organization/Infrastructure)	5
3.1 ความรับผิดชอบ (Responsibilities).....	5
ประธานบริหาร (BBL President).....	5
ผู้อำนวยการด้านสารสนเทศ (BBL CIO).....	5
ผู้รับผิดชอบงานรักษาความปลอดภัย (BBL Security Management).....	5
ผู้บริหารของธนาคาร (BBL Management).....	5
เจ้าหน้าที่ด้านเทคนิค (Technical Staff).....	5
พนักงานและบุคคลภายนอกที่ปฏิบัติงานในธนาคาร (Employees and non-employees).....	5
3.2 นโยบายการรักษาความปลอดภัย (Security Policies).....	5
3.3 การขอผ่อนผันการปฏิบัติตามนโยบาย (Policy Waiver).....	5
4. การบริหารจัดการความเสี่ยงด้านความปลอดภัยข้อมูล (Information Security Risk Management)	17
4.1 การบริหารความเสี่ยง (Risk Management).....	17

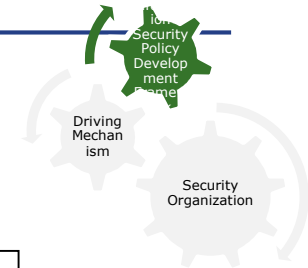
Role & Responsibility

Policy Statements

C Information Security Policy Waiver	49
Version History	50
Contact for Enquiries	50
Document Information	50
Purpose of Document	50
Intended Audience for this Document	50
Information Security Policy Waiver Fill-in Guidance	52
D Information Security Policy Feedback	54
Version History	55
Contact for Enquiries	55

Policy Feedback: suggested corrections or updates with change control process for improving the usefulness of the document

Sample of Information Security Policy



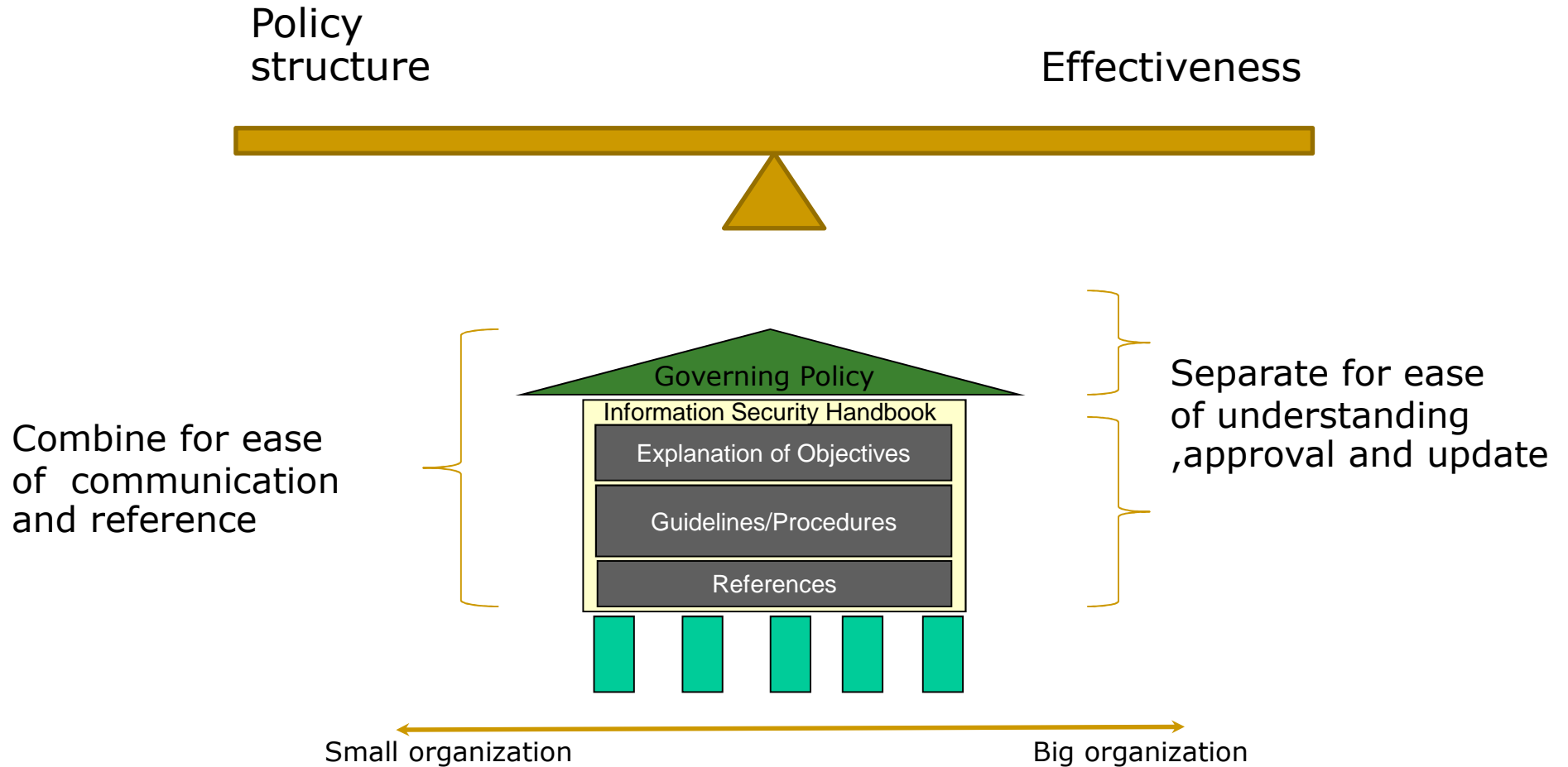
Management Intention
Degree of commitment

7. Hardware Security

7.1 Hardware Security

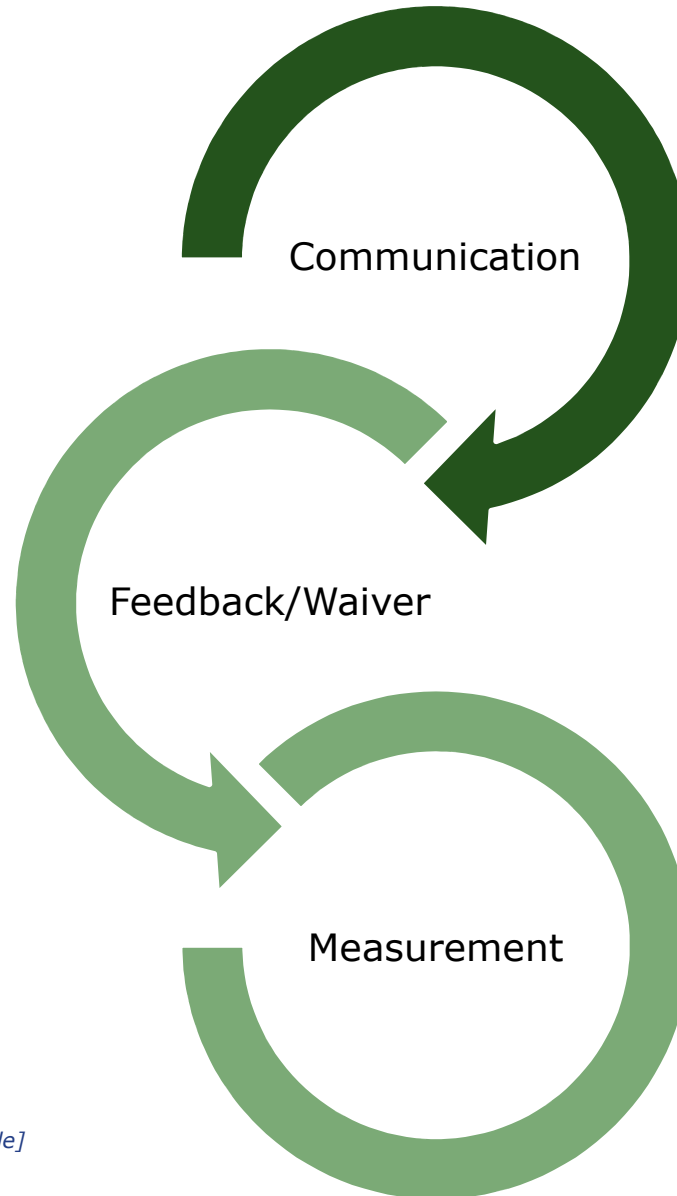
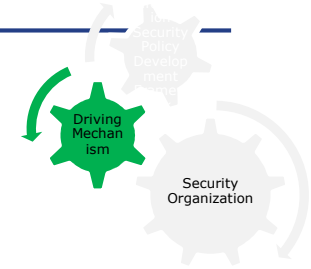
Implement hardware products with dependable, appropriate security controls and features and preserve the integrity of the security features provided through the system software. Equipment should be correctly installed, configured, and maintained to ensure its continued availability and integrity.

Balance

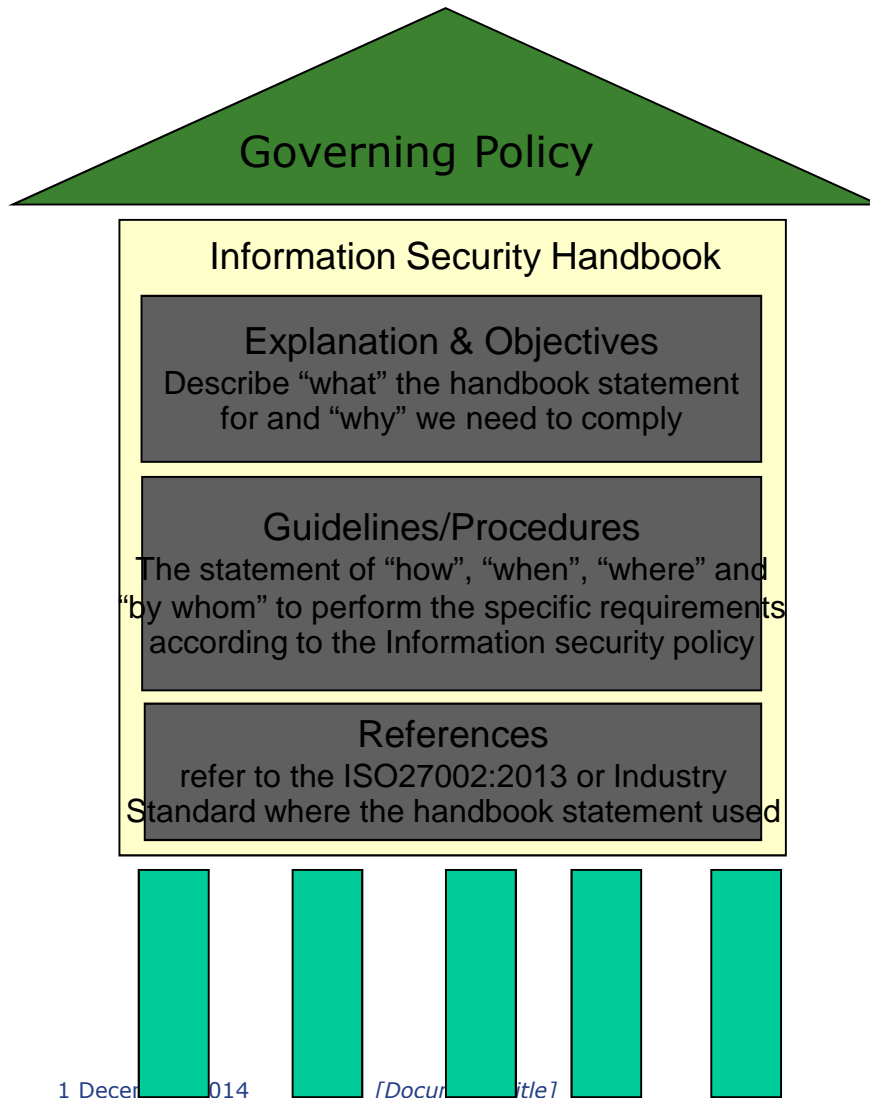
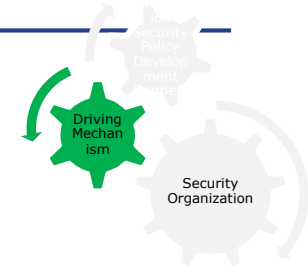


INFORMATION SECURITY POLICY DRIVING MECHANISM

Information Security Policy Driving Mechanism



Information Security Policy Implementation Plan



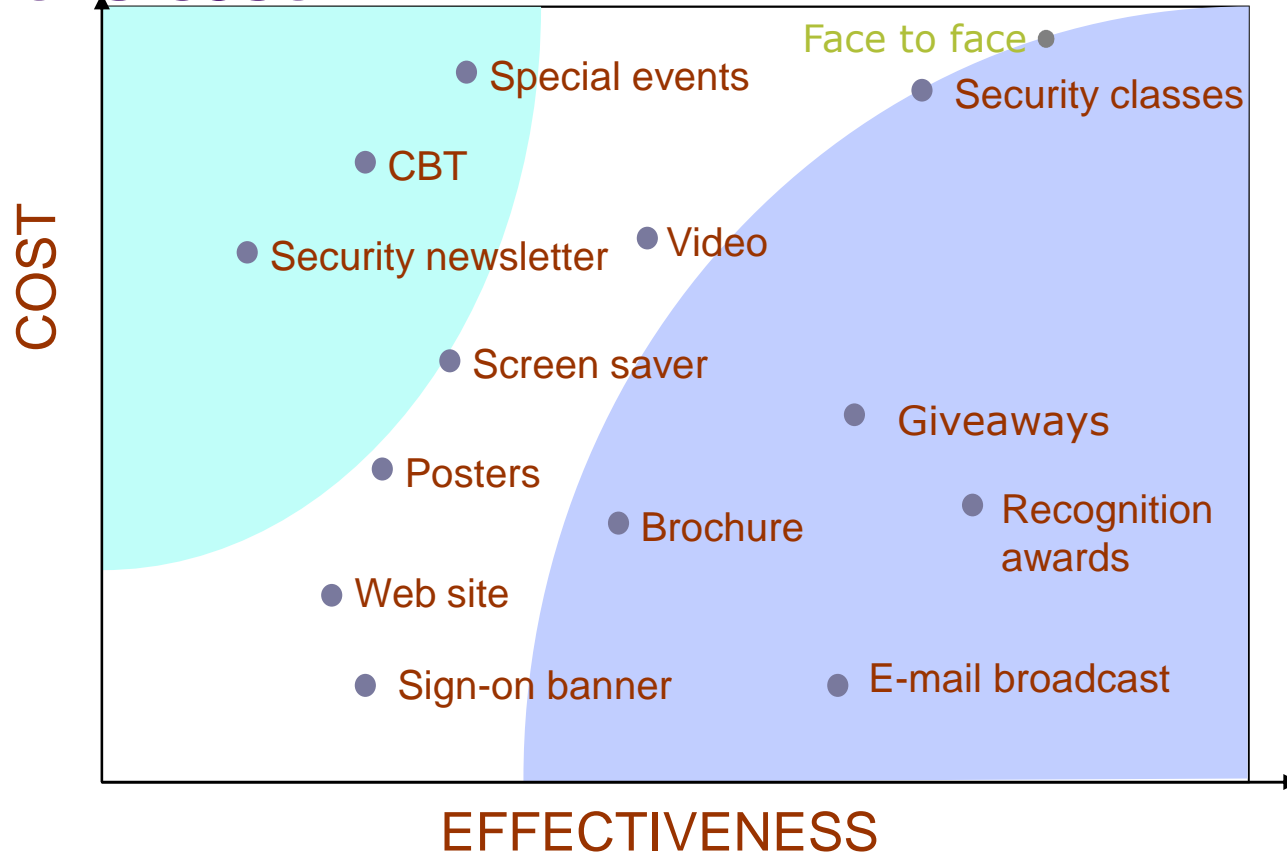
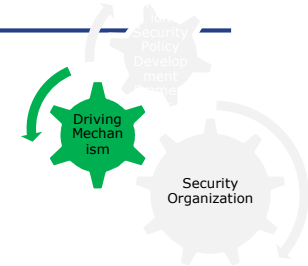
Via Communication Plan

Employee, outsource, vendor, consultant

Communication Plan

- Awareness Training Program
- Recognition Award
- Poster
- Security Day
- Face-to-face Meeting
- Email
- Log-on Screen
- Intranet
- Newsletter/Brochure

However, the plan needs to balance the effectiveness of different channels with the cost



Not recommended



Recommended

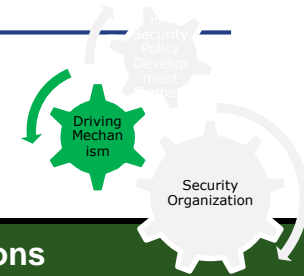


Highly recommended

Note: CBT = Computer Based Training

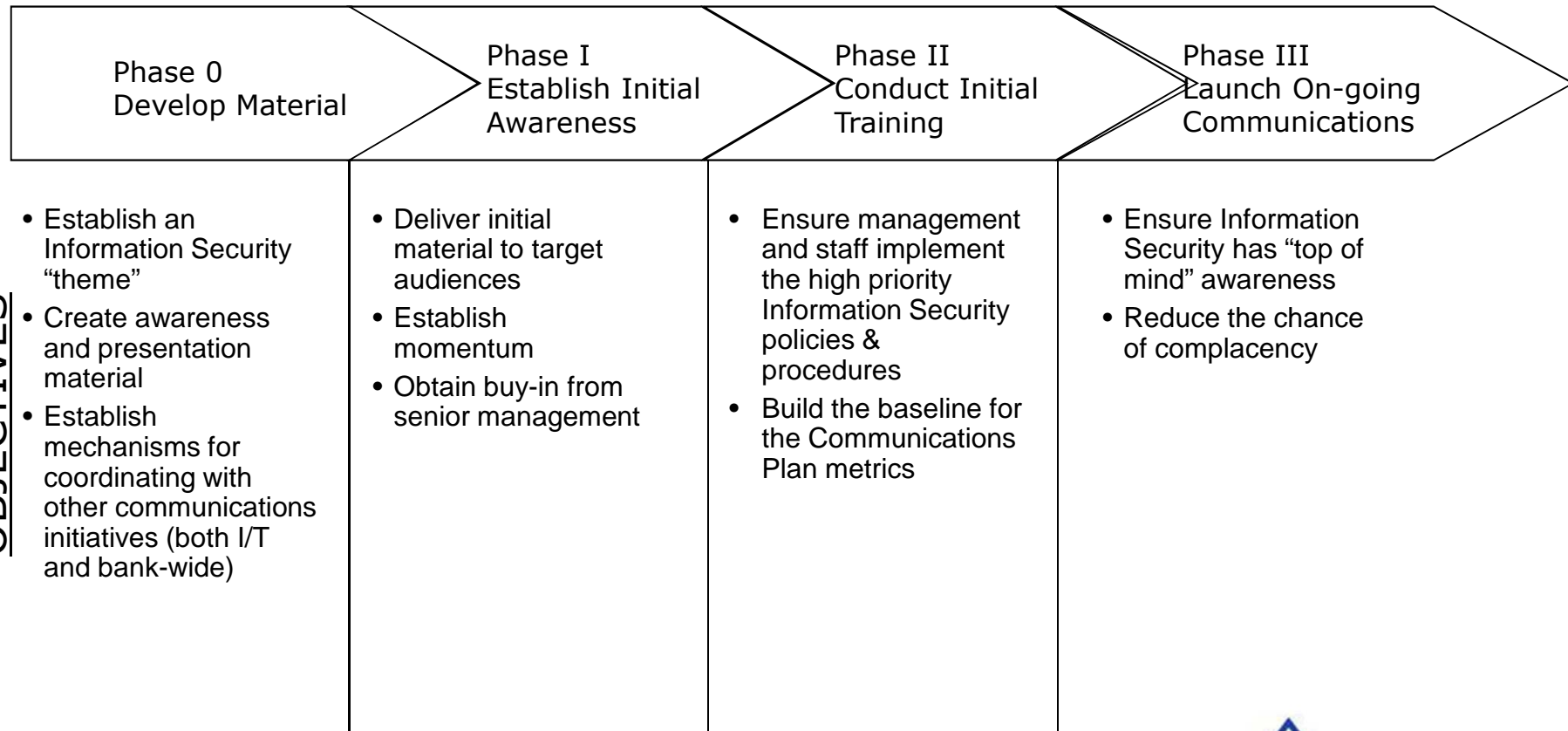
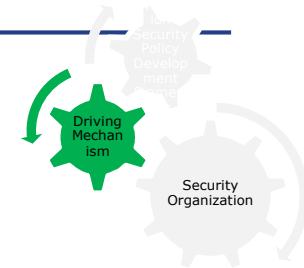
Source: University of Arizona Communications Program Assessment;
US Department of Defense Information Assurance presentation

The plan will need to incorporate a broad set of “communications channels” to deliver the messages



Channel	Primary Uses	Implications
Face-to-face Meetings	<ul style="list-style-type: none"> ▶ Initial awareness of Information Security and responsibilities 	<ul style="list-style-type: none"> ▶ Requires time investment by Security Management ▶ Presentation material needs to be integrated into employee orientation
E-mail	<ul style="list-style-type: none"> ▶ Communications of urgent new / emerging threats ▶ Informing staff of contests / awards 	<ul style="list-style-type: none"> ▶ Need to ensure up-to-date emails of all staff ▶ Will need to coordinate with splash screens
Training Programs (both general and Security-specific)	<ul style="list-style-type: none"> ▶ Overall awareness of Information Security ▶ Initial familiarity with Information Security policies, procedures & guidelines 	<ul style="list-style-type: none"> ▶ Security Management participation in new employee orientation programs ▶ Integration with other induction programs
Videos	<ul style="list-style-type: none"> ▶ Reach remote audiences with both awareness and training content 	<ul style="list-style-type: none"> ▶ Need to have resources available for video creation & editing
Memos / Handbooks	<ul style="list-style-type: none"> ▶ Specific information on implementing Information Security ▶ Answers to Information Security questions 	<ul style="list-style-type: none"> ▶ On-going feedback from management and staff to ensure clarity & completeness
Splash Screens / Log-on Screens	<ul style="list-style-type: none"> ▶ Reminder of importance of Information Security ▶ “Message of the day” for Information Security 	<ul style="list-style-type: none"> ▶ Staff to develop fresh messages ▶ Implementation resources to change screens on a frequent basis
Reminder artifacts (e.g., posters, coffee cups)	<ul style="list-style-type: none"> ▶ General reminders of importance of Information Security 	<ul style="list-style-type: none"> ▶ Refresh content from time-to-time to avoid becoming “part of the background”
Intranet	<ul style="list-style-type: none"> ▶ On-line policies, procedures & guidelines ▶ Delivery of on-line security quizzes / contests 	<ul style="list-style-type: none"> ▶ Ensure integration between on-line and paper versions of documentation ▶ Need to resource on-going content development
Newsletters	<ul style="list-style-type: none"> ▶ Communications of changes to policies or procedures ▶ Communications of general threats & vulnerabilities 	<ul style="list-style-type: none"> ▶ Need on-going support for developing content ▶ May need to be integrated into overall I/T or Security communications

However, the communications plan will ensure consistent messages, irrespective of channel



Example posters

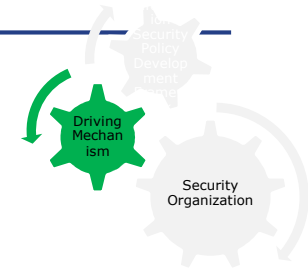
• **ข้อควรปฏิบัติ 10 ประการ** •
ในการรักษาความปลอดภัยข้อมูล

- 1. จัดเก็บและทำลายเอกสารสำคัญอย่างปลอดภัย
- 2. ปฏิบัติตามกฎหมายเข้าใช้ห้องมั่นคงและศูนย์ข้อมูลอย่างเคร่งครัด
- 3. ตัดบัตรพนักงานตลอดเวลาที่ปฏิบัติงานอยู่ในธนาคาร
- 4. ตั้งรหัสผ่านให้ตายาก และไม่บอกให้ผู้อื่นรู้
- 5. ไม่ส่งอีเมลที่ไม่เหมาะสม
- 6. ปฏิบัติตามข้อตกลงในการใช้อินเทอร์เน็ตอย่างสม่ำเสมอ
- 7. ล็อกคอมพิวเตอร์ทุกครั้งที่ถูกจากโต๊ะ
- 8. ไม่ติดตั้งซอฟต์แวร์โดยไม่ได้รับอนุญาต
- 9. ขออนุมัติทุกครั้งก่อนนำคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์เชื่อมต่อกับระบบของธนาคาร
- 10. หากพบเหตุการณ์ผิดปกติด้านความปลอดภัยข้อมูล โปรดแจ้ง Service Desk 0-2685-7007

อ่านรายละเอียดเพิ่มเติมได้ที่ <http://oportal/sites/sm>

 Bangkok Bank
ธนาคารกรุงเทพ

Governing Policy Document Structure



สารบัญ (Table of Contents)

1. บทนำ (Introduction)	5
1.1 บทย่อ (Overview).....	5
1.2 ขอบเขตและจุดมุ่งหมายของนโยบายการรักษาความปลอดภัยข้อมูล (Scope and Purpose of the Information Security Policy)	5
2. วัตถุประสงค์ในการรักษาความปลอดภัย (Security Objectives)	5
3. โครงสร้างและองค์ประกอบพื้นฐานในการรักษาความปลอดภัย (Security Organization/Infrastructure)	5
3.1 ความรับผิดชอบ (Responsibilities).....	5
ประธานบริหาร (BBL President).....	5
ผู้อำนวยการด้านสารสนเทศ (BBL CIO).....	5
ผู้รับผิดชอบงานรักษาความปลอดภัย (BBL Security Management).....	5
ผู้บริหารของธนาคาร (BBL Management).....	5
เจ้าหน้าที่ด้านเทคนิค (Technical Staff).....	5
พนักงานและบุคคลภายนอกที่ปฏิบัติงานในธนาคาร (Employees and non-employees).....	5
3.2 นโยบายการรักษาความปลอดภัย (Security Policies).....	5
3.3 การขอผ่อนผันการปฏิบัติตามนโยบาย (Policy Waiver).....	5
4. การบริหารจัดการความเสี่ยงด้านความปลอดภัยข้อมูล (Information Security Risk Management)	17
4.1 การบริหารความเสี่ยง (Risk Management).....	17

Role & Responsibility

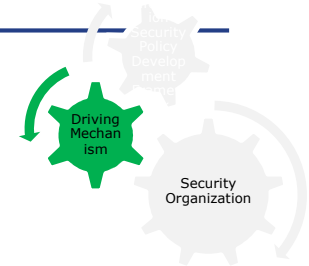
Policy Statements

Policy Waiver: Justification for non-compliance or deviation from Information Security Policy. Formalize

C Information Security Policy Waiver	49
Version History	50
Contact for Enquiries	50
Document Information	50
Purpose of Document	50
Intended Audience for this Document	50
Information Security Policy Waiver Fill-in Guidance	52
D Information Security Policy Feedback	54
Version History	55
Contact for Enquiries	55

Policy Feedback: suggested corrections or updates with change control process for improving the usefulness of the document

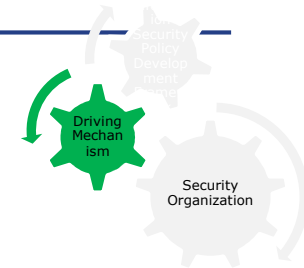
Measurement

















Criteria for determining overall readiness to implement Information Security Policy in includes:

- **Principle** – International Standard/ Practice and in-house developed methodologies adopted as guidelines
- **Practice** – Current operations
- **Process** – Identified process in each area of operation
- **People** – Working Units who responsible for the processes
- **Technology** – Tools or systems to support the implementation

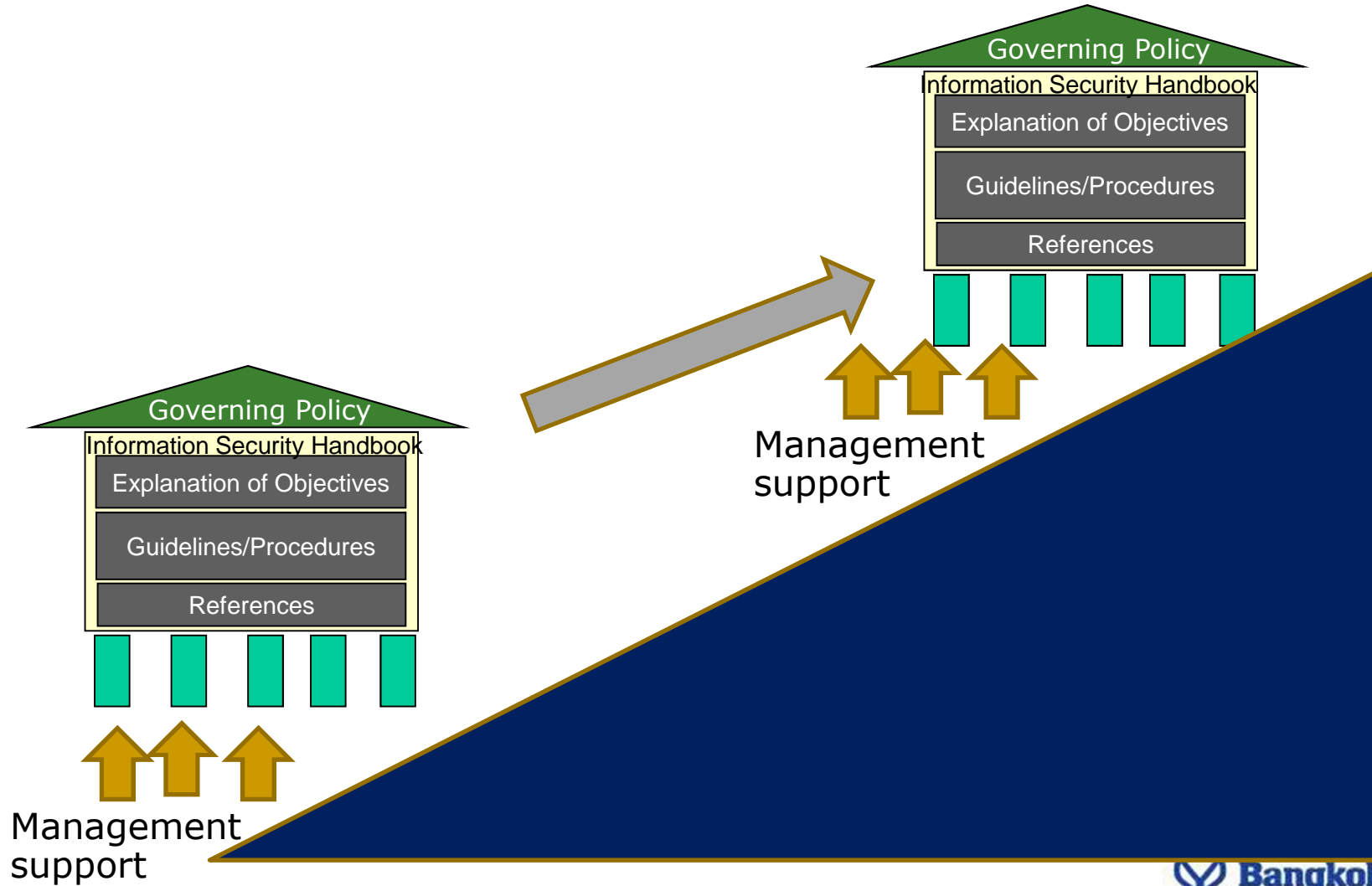
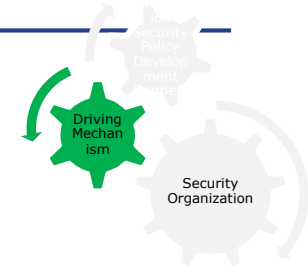
Overall Readiness - Sample



Information Security Policy Readiness	Readiness
5. Information Security Management Components	 3
6. Information Systems Acquisition, Development, and Maintenance	 4
7. Hardware Security	 2
8. Software Security	 4
9. Access Control	 4
10. Communications Security	 3
11. Physical Security	 4
12. Personnel Security	 3
13. Information Asset Security	 4
14. Business Continuity	 4
15. Segregation of Duties	 5

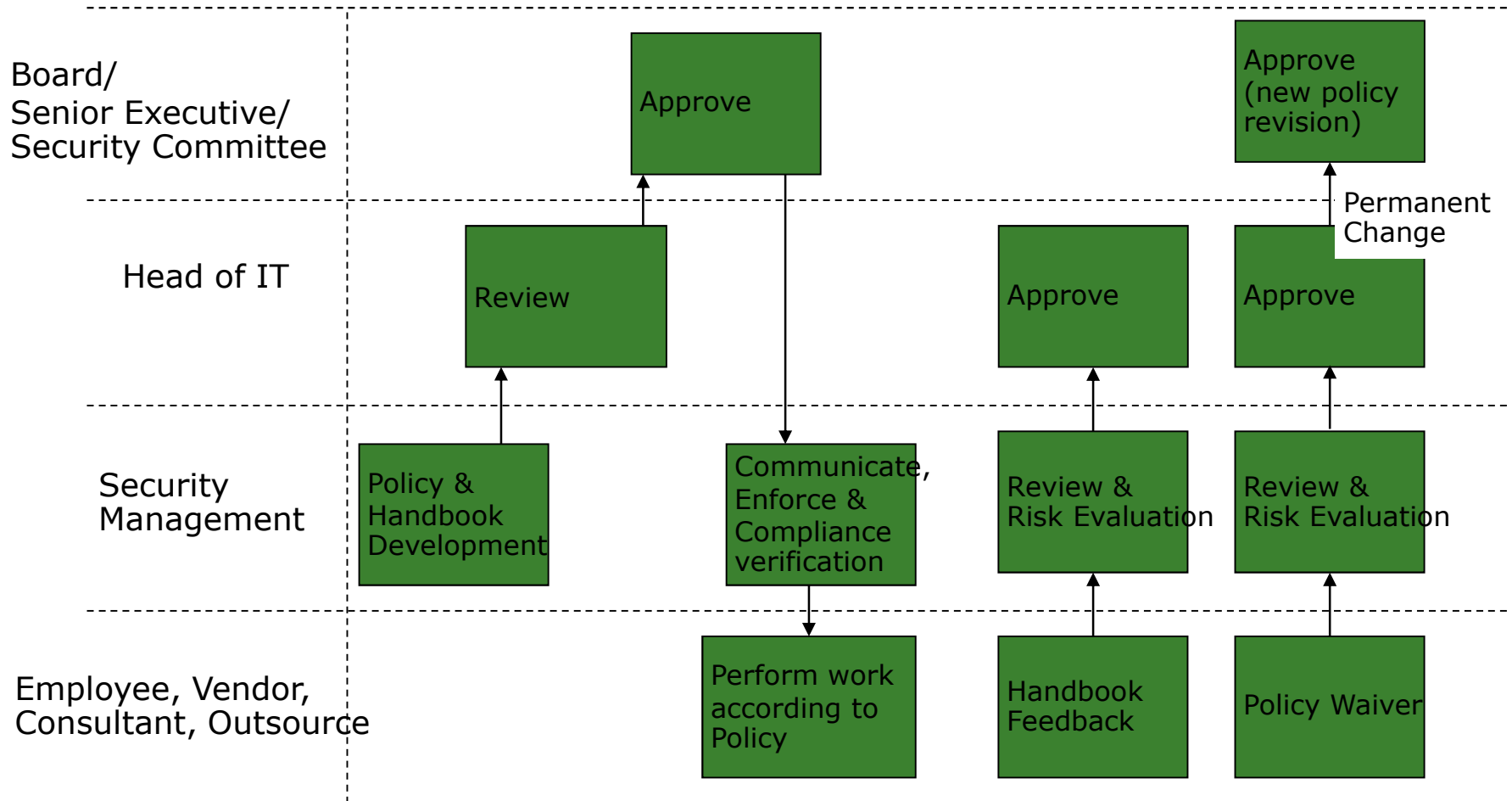
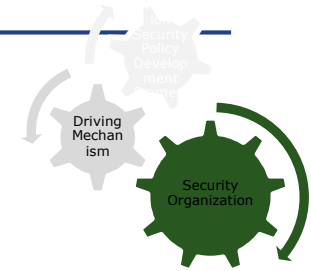
-  = Very High
-  = High
-  = Medium
-  = Low
-  = Very low

Information Security Policy Improvement



INFORMATION SECURITY ORGANIZATION

Responsibility for Information Security Policy Execution



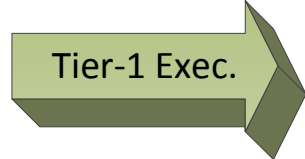
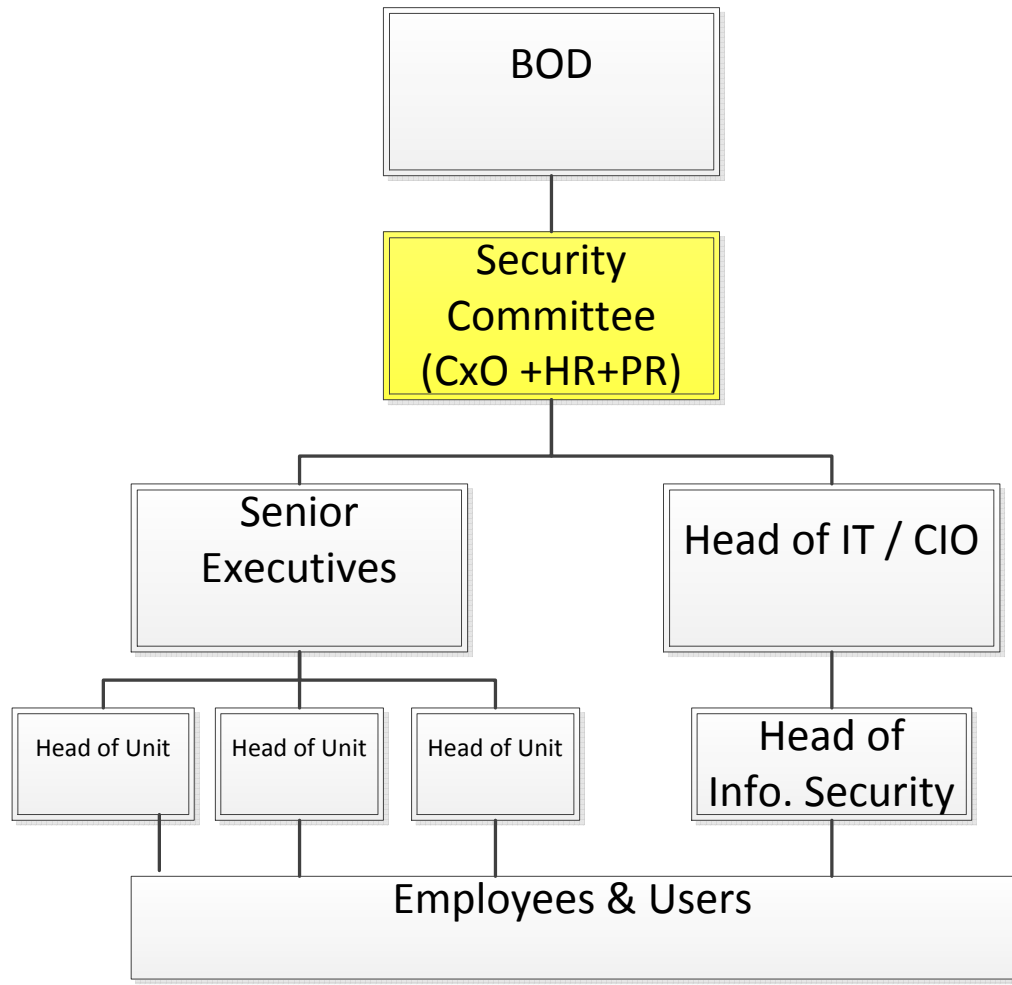
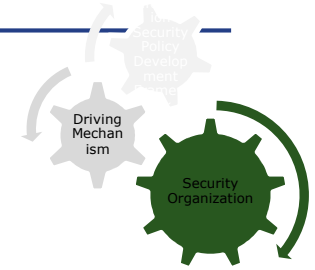
Policy Development (handbook will be approved by Head of IT)

Feedback

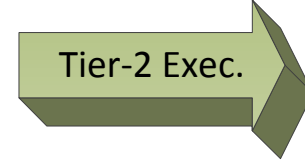
Waiver



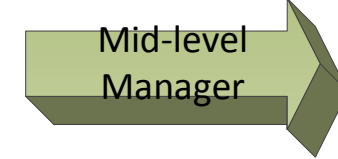
Information Security Organization



Oversee the effectiveness

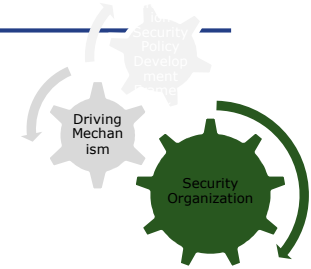


Oversee the development and implementation of policies



Implementing & assessing the risks

Security Committee Responsibilities



The Security Committee is responsible for:

- ensuring that the Head of Information Technology reports annually on the effectiveness of the information security management program and on remedial actions where required
- ensuring that senior management provide information security for operations and information technology (IT) resources under their control
- ensuring that organization has trained personnel to support compliance with the information security management program
- delegating to the Head of Information Technology the authority to ensure compliance with the information security management program

CASE STUDY FOR DISCUSSION

THANK YOU