

IT Security Procedures

ดร. ธนัญชัย ตริภาค

หลักการสำคัญของ Security คืออะไร ??

Hardware

Software



Tools

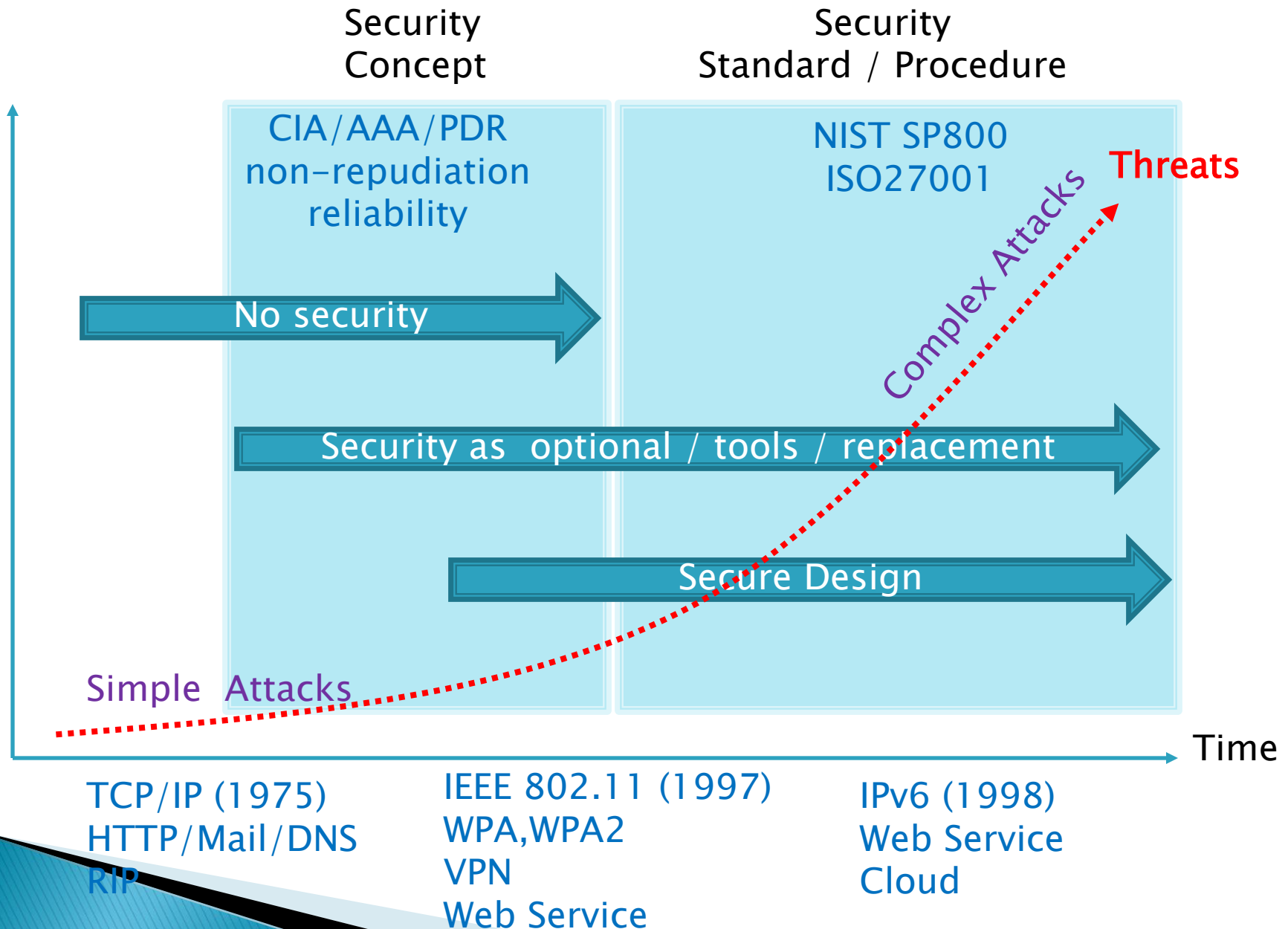
Process

ให้นักศึกษารวบรวม กิจกรรม / โครงการ ทั้งหมด ที่ทำให้ระบบสารสนเทศมีความปลอดภัย

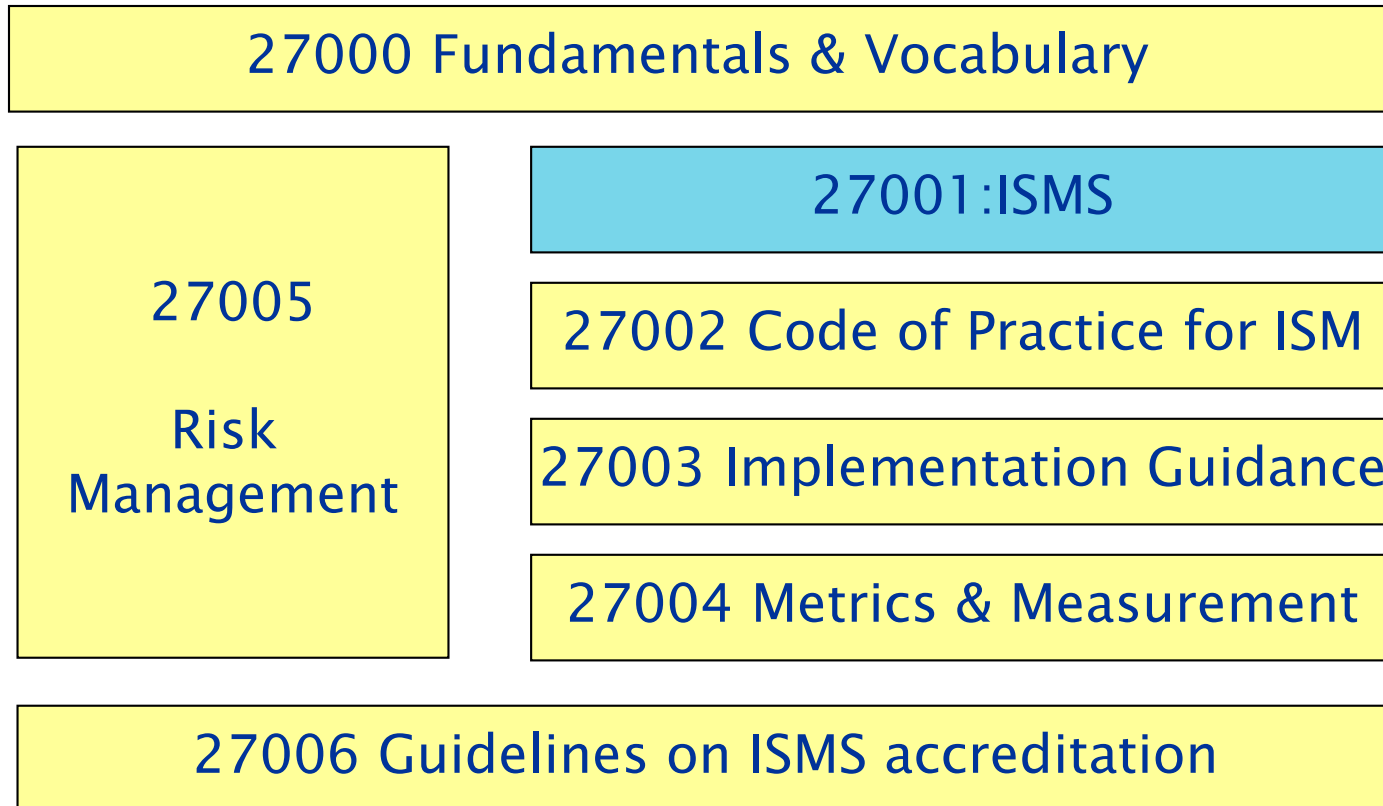
ทำทั้งหมดแล้ว
มั่นใจกี่ %



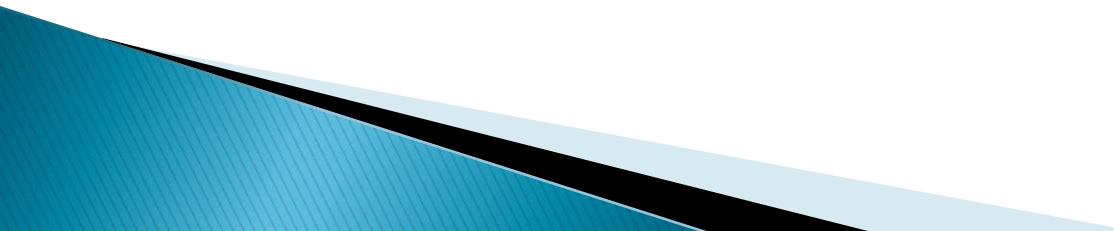
ทำครั้งเดียว
ทำสม่ำเสมอทุกปี
ทำ N ปีต่อครั้ง



Structure of 27000 series



รายละเอียดสำคัญ ของ ISO27000:2005 (Annex A)

1. Security policy (5)
 2. Organization of information security (6)
 3. Asset management(7)
 4. Human resources security (8)
 5. Physical and environmental security (9)
 6. Communications and operations management (10)
 7. Access control (11)
 8. Information systems acquisition, development and maintenance (12)
 9. Information security incident management (13)
 10. Business continuity management (14)
 11. Compliance (15)
- 

1. Security Policy


- ▶ Objective:
 - Information security policy.
- ▶ Covers:
 - Information security policy document
 - Review of Informational Security Policy

2. Organization of information security

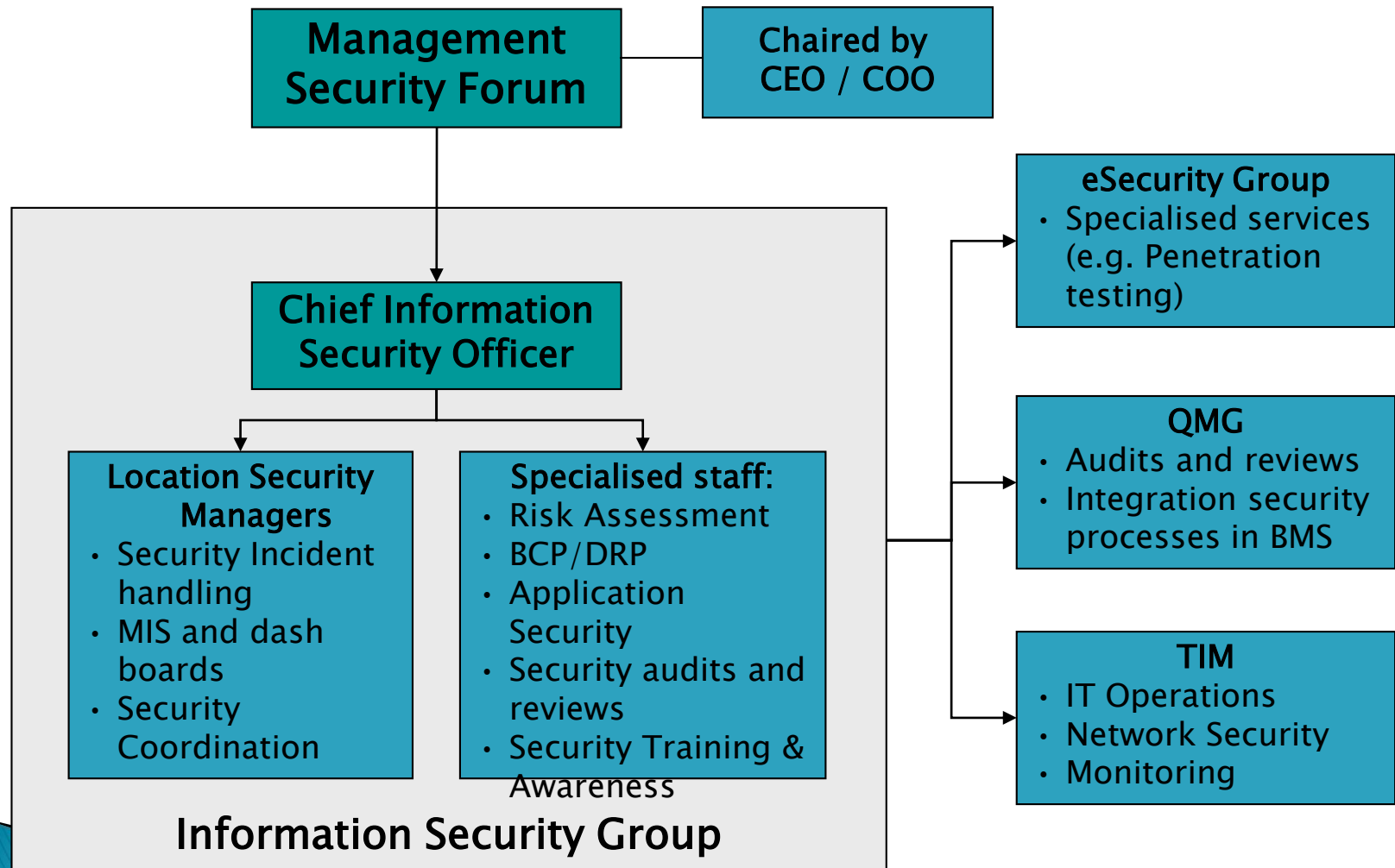
▶ Objective:

- Internal Organization
- External Parties

▶ Covers:

- Management commitment to information security
 - Information security coordination
 - Allocation of information security responsibilities
 - Authorization process for information processing facilities
 - Confidentiality agreements
 - Contact with authorities
 - Contact with special interest groups
 - Independent review of information security
 - Identification of risks related to external parties
 - Addressing security when dealing with customers
 - Addressing Security in third party agreements
- 

2. Organization of information security – Example



3. Asset Management

- ▶ Objective:
 - Responsibility for assets
 - Information classification
- ▶ Covers:
 - Inventory of assets
 - Ownership of assets
 - Acceptable use of assets
 - Classification guidelines
 - Information labelling and handling




4. Human Resource Security

▶ Objective:

- Prior to employment
- During employment
- Termination or change of employment

▶ Covers:


- Roles and responsibilities
 - Screening
 - Terms and conditions of employment
 - Management responsibilities
 - Information security awareness, education and training
 - Disciplinary process
 - Termination responsibilities
 - Return of assets
 - Removal of access rights
- 

5. Physical and Environmental Security

▶ Objective:

- Secure Areas
- Equipment Security

▶ Covers:

- Physical Security Perimeter
 - Physical entry Controls
 - Securing Offices, rooms and facilities
 - Protecting against external and environmental threats
 - Working in Secure Areas
 - Public access delivery and loading areas
 - Cabling Security
 - Equipment Maintenance
 - Securing of equipment off-premises
 - Secure disposal or re-use of equipment
 - Removal of property
- 

6. Communications & Operations Management


▶ Objective:

- Operational Procedures and responsibilities
- Third party service delivery management
- System planning and acceptance
- Protection against malicious and mobile code
- Backup
- Network Security Management
- Media handling
- Exchange of Information
- Electronic Commerce Services
- Monitoring

▶ Covers:

- Documented Operating procedures
 - Change management
 - Segregation of duties
- 

6. Communications & Operations Management (contd..)

- Separation of development, test and operational facilities
 - Service delivery
 - Monitoring and review of third party services
 - Managing changes to third party services
 - Capacity Management
 - System acceptance
 - Controls against malicious code
 - Controls against mobile code
 - Information backup
 - Network Controls
 - Security of network services
 - Management of removable media
 - Disposal of Media
 - Information handling procedures
 - Security of system documentation
 - Information exchange policies and procedures
 - Exchange agreements
- 

6. Communications & Operations Management (contd..)

- Exchange agreements
- Electronic Messaging
- Business information systems
- Electronic Commerce
- On-Line Transactions
- Publicly available information
- Audit logging
- Monitoring system use
- Protection of log information
- Administrator and operator logs
- Fault logging
- Clock synchronisation

7. Access Controls


▶ Objective:

- Business Requirement for Access Control
- User Access Management
- User Responsibilities
- Network Access Control
- Operating system access control
- Application and Information Access Control
- Mobile Computing and teleworking

▶ Covers:

- Access Control Policy
- User Registration
- Privilege Management
- User Password Management
- Review of user access rights
- Password use

7. Access Controls (contd..)

- Unattended user equipment
 - Clear desk and clear screen policy
 - Policy on use of network services
 - User authentication for external connections
 - Equipment identification in networks
 - Remote diagnostic and configuration port protection
 - Segregation in networks
 - Network connection control
 - Network routing control
 - Secure log-on procedures
 - User identification and authentication
 - Password management system
 - Use of system utilities
 - Session time-out
 - Limitation of connection time
 - Information access restriction
 - Sensitive system isolation
 - Mobile computing and communications
 - Teleworking
- 

8. Information systems acquisition, development and maintenance

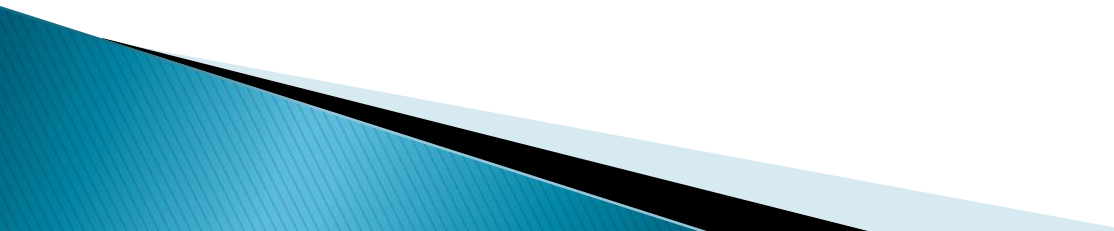
► Objective:

- Security requirements of information systems
- Correct processing in applications
- Cryptographic controls
- Security of system files
- Security in development and support processes
- Technical Vulnerability Management

► Covers:

- Security requirements analysis and specification
- Input data validation
- Control of internal processing
- Message integrity
- Output data validation
- Policy on use of cryptographic controls
- Key management
- Control of operational software
- Protection of system test data

8. Information systems acquisition, development and maintenance (contd)

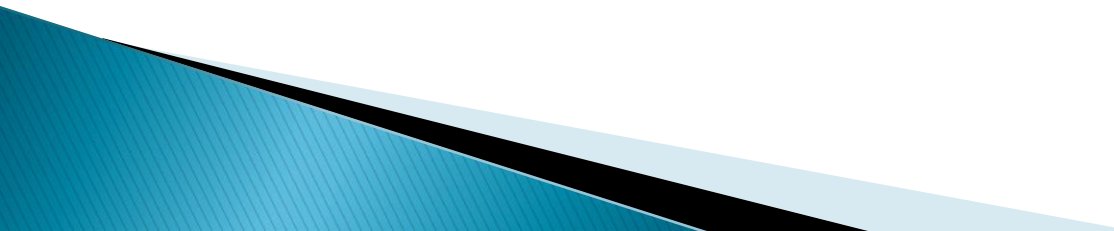
- Access Control to program source code
 - Change control procedures
 - Technical review of applications after operating system changes
 - Restriction on changes to software packages
 - Information leakage
 - Outsourced software development
 - Control of technical vulnerabilities
- 

9. Information Security Incident Management

▶ Objective:

- Reporting information security events and weaknesses
- Management of information security incidents and improvements

▶ Covers:

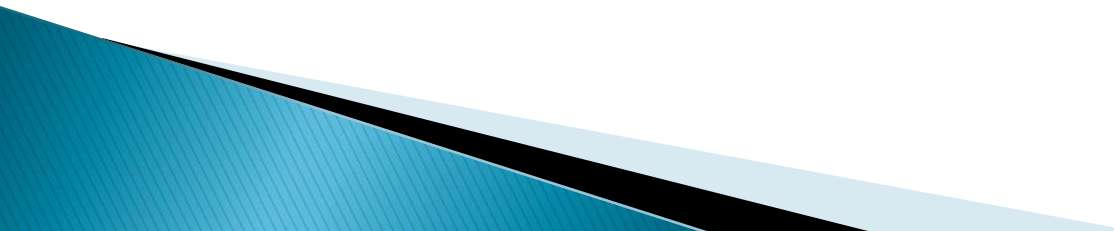
- Reporting information security events
 - Reporting security weaknesses
 - Responsibilities and procedures
 - Learning from information security incidents
 - Collection of evidence
- 

10. Business Continuity Management

▶ Objective:

- Information security aspects of business continuity management

▶ Covers:

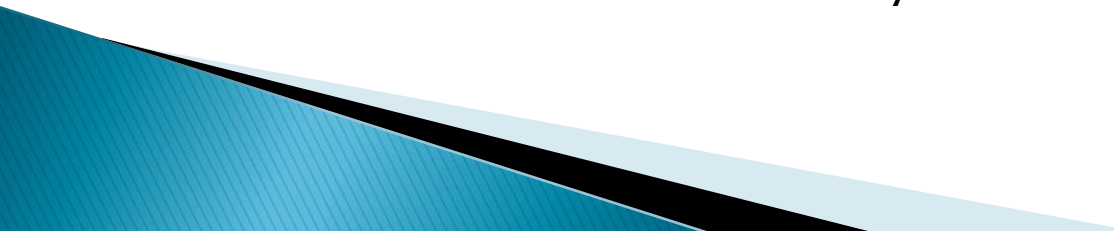
- Including information security in the business continuity management process
 - Business continuity and risk assessment
 - Developing and implementing continuity plans including information security
 - Business continuity planning framework
 - Testing, maintaining and re-assessing business continuity plans
- 

11. Compliance

▶ Objective

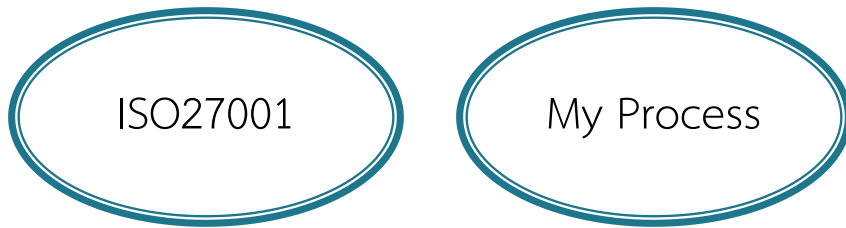
- Compliance with legal requirements
- Compliance with security policies and standards, and technical compliance
- Information Systems audit considerations

▶ Covers:

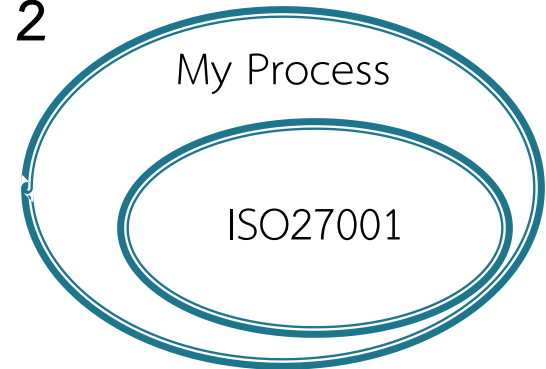
- Identification of applicable legislation
 - Intellectual property rights (IPR)
 - Protection of organizational records
 - Data protection and privacy of personal information
 - Prevention of misuse of information processing facilities
 - Regulation of cryptographic controls
 - Compliance with security policies and standards
 - Technical compliance checking
 - Information systems audit controls
 - Protection of information system audit tools
- 

เปรียบเทียบการทำงานที่นักศึกษากำหนด กับ ISO27001 แล้ว เป็นแบบไหน ???

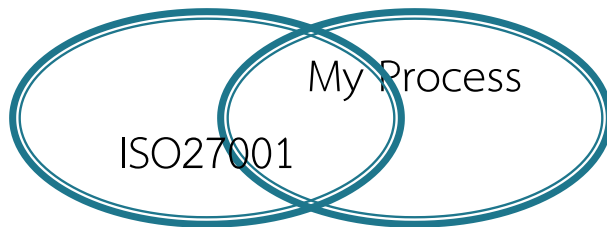
1



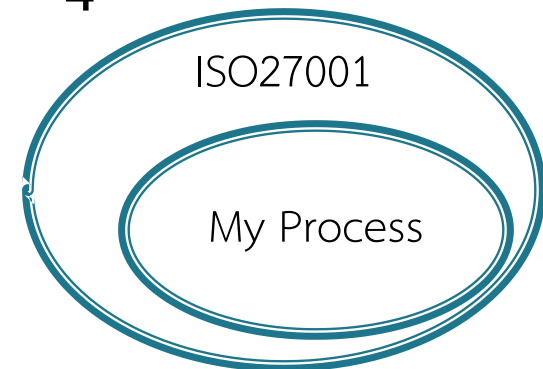
2



3



4



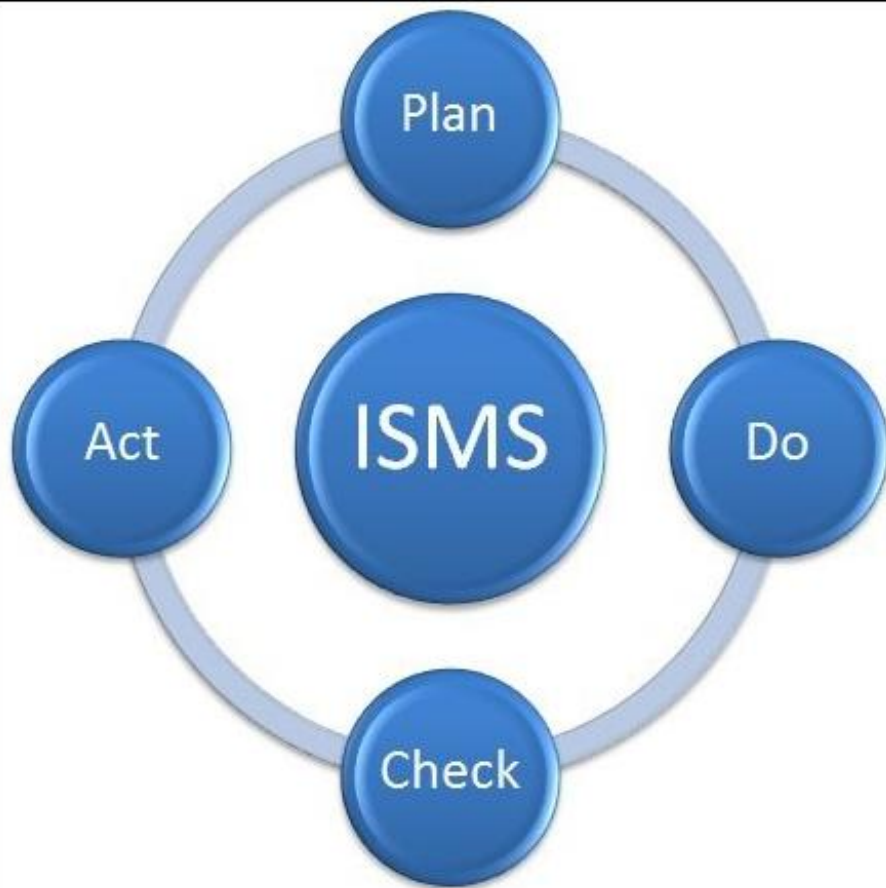
นักศึกษาคิดว่าถ้าดำเนินการตาม ISO27001 แล้วจะมีความ
มั่นใจในความปลอดภัยกี่ %



อะไรคือความเสี่ยงที่ยังหลงเหลืออยู่ของการใช้ ISO27001



ISO27001 FB's Profile Picture



ISO27001

June 28, 2011 · ✱

Like · Comment · Share



Write a comment...

สรุป / ผลลัพธ์ที่ได้