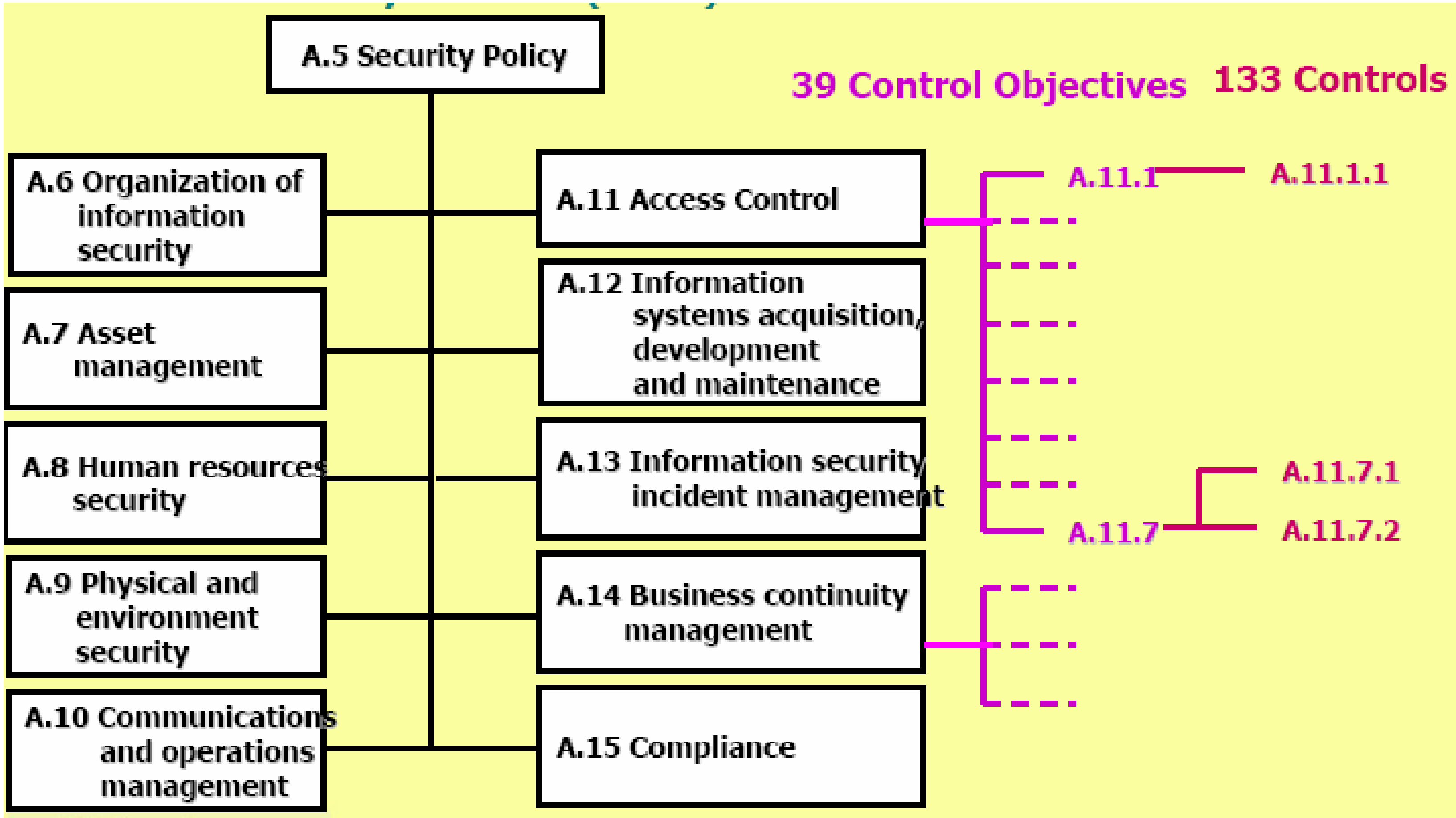
ISO 27000



A.5 Security Policy

39 Control Objectives

133 Controls

A.6 Organization of information security

A.7 Asset management

A.8 Human resources security

A.9 Physical and environment security

A.10 Communications and operations management

A.11 Access Control

A.12 Information systems acquisition, development and maintenance

A.13 Information security incident management

A.14 Business continuity management

A.15 Compliance

A.11.1

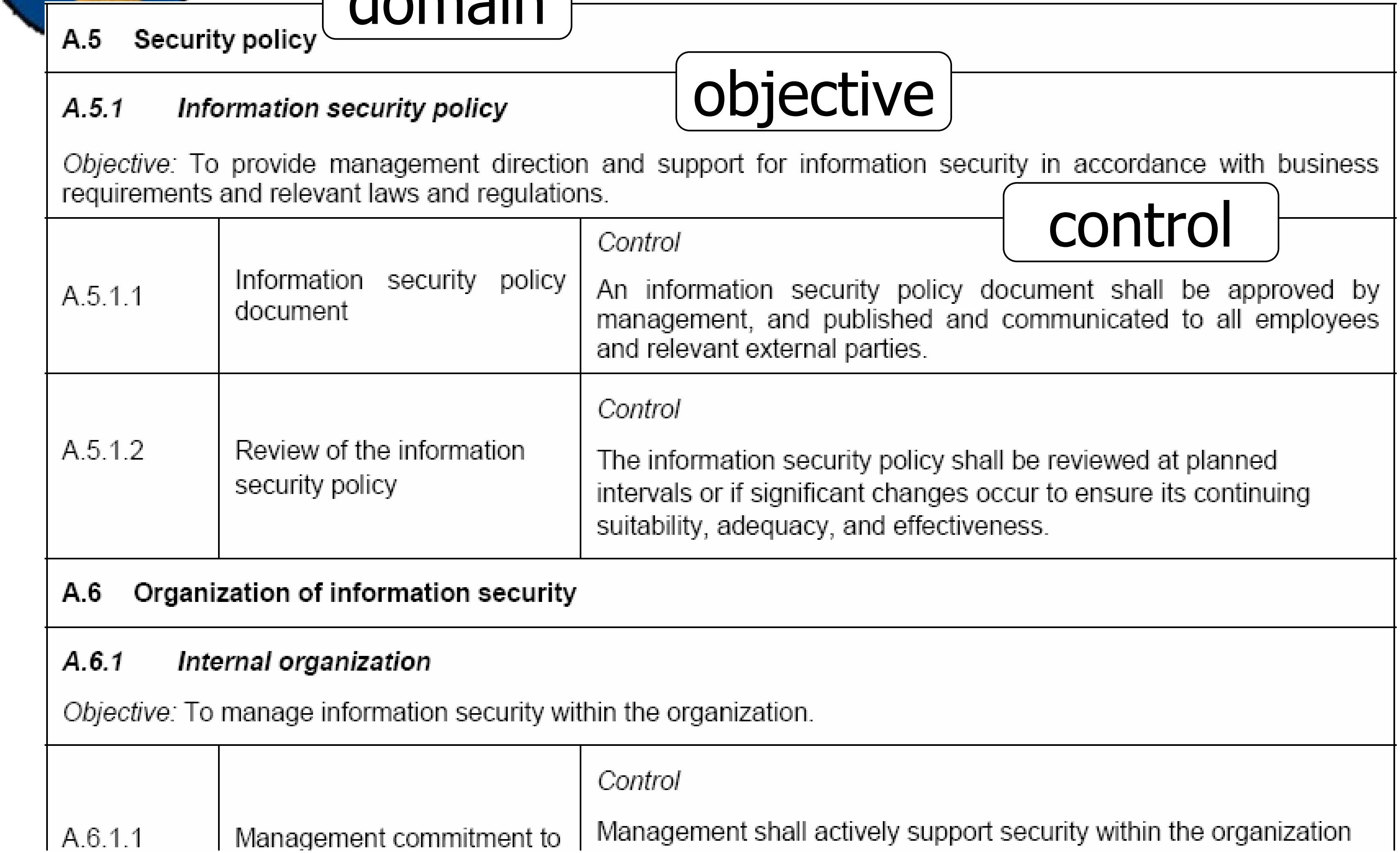
A.11.1.1

A.11.7

A.11.7.1

A.11.7.2

ISO 27000



domain

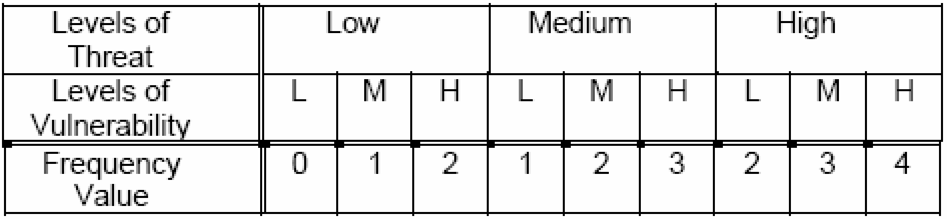
objective

control

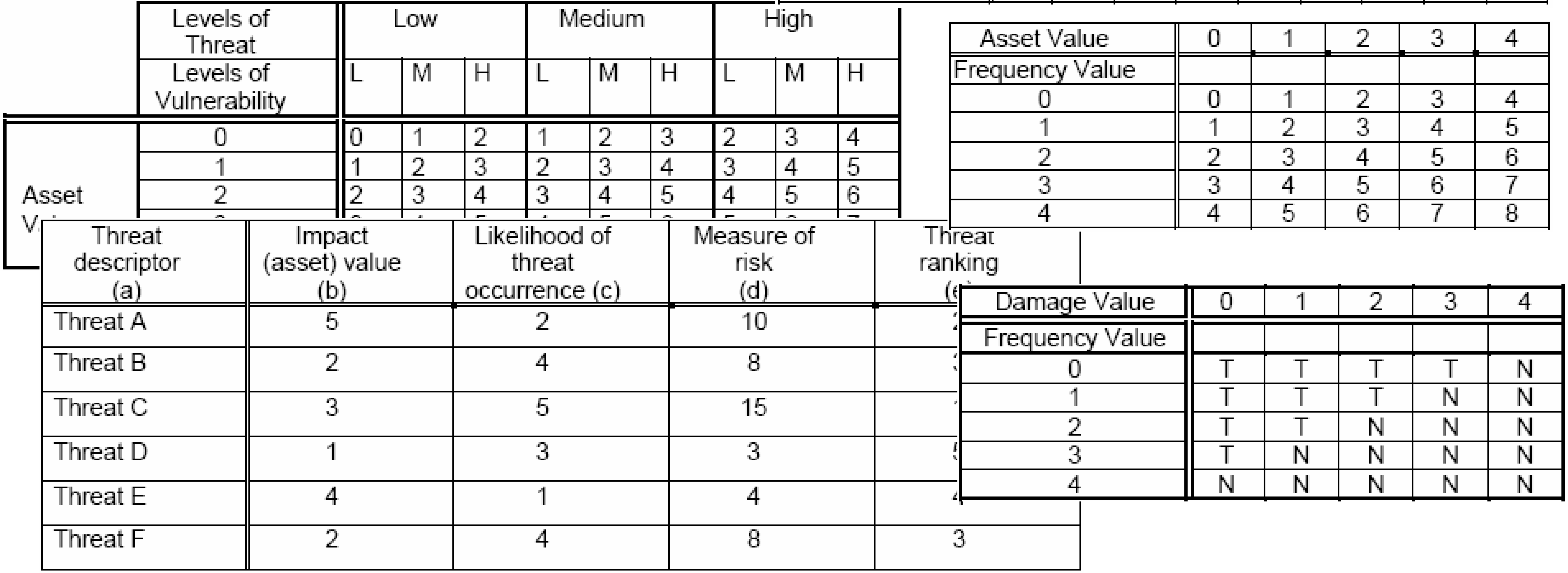
A.5 Security policy		
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization *Objective:* To manage information security within the organization.		
A.6.1.1	Management commitment to	*Control* Management shall actively support security within the organization

ตัวอย่างการประเมินความเสี่ยง

ลำดับความสำคัญขึ้นอยู่กับ
การคุกคาม, ช่องโหว่, มูลค่า



Levels of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Frequency Value	0	1	2	1	2	3	2	3	4



	Levels of Threat	Low			Medium			High		
	Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Asset V	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

Asset Value	0	1	2	3	4
Frequency Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Threat descriptor (a)	Impact (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Damage Value	0	1	2	3	4
Frequency Value					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

ISO 27000

A.6.1	Internal organization
A.6.1.1	Management commitment to information security
A.6.1.2	Information security coordination
A.6.1.3	Allocation of information security responsibilities
A.6.1.4	Authorization process for information processing facilities
A.6.1.5	Confidentiality agreements
A.6.1.6	Contact with authorities
A.6.1.7	Contact with special interest groups
A.6.1.8	Independent review of information security
A.6.2	External parties
A.6.2.1	Identification of risks related to external parties
A.6.2.2	Addressing security when dealing with customers
A.6.2.3	Addressing security in third party agreements

A.5	Security policy
A.5.1	Information security policy
A.5.1.1	Information security policy document
A.5.1.2	Review of the information security policy

A.7	Asset management
A.7.1	Responsibility for assets
A.7.1.1	Inventory of assets
A.7.1.2	Ownership of assets
A.7.1.3	Acceptable use of assets
A.7.2	Information classification
A.7.2.1	Classification guidelines
A.7.2.2	Information labeling and handling

ISO 27000

A.8	Human resources security
A.8.1	Prior to employment
A.8.1.1	Roles and responsibilities
A.8.1.2	Screening
A.8.1.3	Terms and conditions of employment
A.8.2	During employment
A.8.2.1	Management responsibilities
A.8.2.2	Information security awareness, education and training
A.8.2.3	Disciplinary process
A.8.3	Termination or change of employment
A.8.3.1	Termination responsibilities
A.8.3.2	Return of assets
A.8.3.3	Removal of access rights

A.9	Physical and environmental security
A.9.1	Secure areas
A.9.1.1	Physical security perimeter
A.9.1.2	Physical entry controls
A.9.1.3	Securing offices, rooms and facilities
A.9.1.4	Protecting against external and environmental threats
A.9.1.5	Working in secure areas
A.9.1.6	Public access, delivery and loading areas
A.9.2	Equipment security
A.9.2.1	Equipment siting and protection
A.9.2.2	Supporting utilities
A.9.2.3	Cabling security
A.9.2.4	Equipment maintenance
A.9.2.5	Security of equipment offpremises
A.9.2.6	Secure disposal or re-use of equipment
A.9.2.7	Removal of property

ISO 27000

A.10	Communications and operations management
A.10.1	Operational procedures and responsibilities
A.10.1.1	Documented operating procedures
A.10.1.2	Change management
A.10.1.3	Segregation of duties
A.10.1.4	Separation of development, test and operational facilities
A.10.2	Third party service delivery management
A.10.2.1	Service delivery
A.10.2.2	Monitoring and review of third party services
A.10.2.3	Managing changes to third party services
A.10.3	System planning and acceptance
A.10.3.1	Capacity management
A.10.3.2	System acceptance
A.10.4	Protection against malicious and mobile code
A.10.4.1	Controls against malicious code
A.10.4.2	Controls against mobile code

A.10.5	Back-up
A.10.5.1	Information back-up
A.10.6	Network security management
A.10.6.1	Network controls
A.10.6.2	Security of network services
A.10.7	Media handling
A.10.7.1	Management of removable media
A.10.7.2	Disposal of media
A.10.7.3	Information handling procedures
A.10.7.4	Security of system documentation
A.10.8	Exchange of information
A.10.8.1	Information exchange policies and procedures
A.10.8.2	Exchange agreements
A.10.8.3	Physical media in transit
A.10.8.4	Electronic messaging
A.10.8.5	Business information systems

ISO 27000

A.10.9	Electronic commerce services
A.10.9.1	Electronic commerce
A.10.9.2	On-line transactions
A.10.9.3	Publicly available information
A.10.10	Monitoring
A.10.10.1	Audit logging
A.10.10.2	Monitoring system use
A.10.10.3	Protection of log information
A.10.10.4	Administrator and operator logs
A.10.10.5	Fault logging
A.10.10.6	Clock synchronization

A.11	Access control
A.11.1	Business requirement for access control
A.11.1.1	Access control policy
A.11.2	User access management
A.11.2.1	User registration
A.11.2.2	Privilege management
A.11.2.3	User password management
A.11.2.4	Review of user access rights
A.11.3	User responsibilities
A.11.3.1	Password use
A.11.3.2	Unattended user equipment
A.11.3.3	Clear desk and clear screen policy
A.11.4	Network access control
A.11.4.1	Policy on use of network services
A.11.4.2	User authentication for external connections
A.11.4.3	Equipment identification in networks
A.11.4.4	Remote diagnostic and configuration port protection
A.11.4.5	Segregation in networks
A.11.4.6	Network connection control
A.11.4.7	Network routing control

ISO 27000

A.11.5	Operating system access control
A.11.5.1	Secure log-on procedures
A.11.5.2	User identification and authentication
A.11.5.3	Password management system
A.11.5.4	Use of system utilities
A.11.5.5	Session time-out
A.11.5.6	Limitation of connection time
A.11.6	Application and information access control
A.11.6.1	Information access restriction
A.11.6.2	Sensitive system isolation
A.11.7	Mobile computing and teleworking
A.11.7.1	Mobile computing and communications
A.11.7.2	Teleworking

A.12	Information systems acquisition, development and maintenance
A.12.1	Security requirements of information systems
A.12.1.1	Security requirements analysis and specification
A.12.2	Correct processing in applications
A.12.2.1	Input data validation
A.12.2.2	Control of internal processing
A.12.2.3	Message integrity
A.12.2.4	Output data validation
A.12.3	Cryptographic controls
A.12.3.1	Policy on the use of cryptographic controls
A.12.3.2	Key management

ISO 27000

A.12.4	Security of system files
A.12.4.1	Control of operational software
A.12.4.2	Protection of system test data
A.12.4.3	Access control to program source code
A.12.5	Security in development and support processes
A.12.5.1	Change control procedures
A.12.5.2	Technical review of applications after operating system changes
A.12.5.3	Restrictions on changes to software packages
A.12.5.4	Information leakage
A.12.5.5	Outsourced software development
A.12.6	Technical Vulnerability Management
A.12.6.1	Control of technical vulnerabilities

A.13	Information security incident management
A.13.1	Reporting information security events and weaknesses
A.13.1.1	Reporting information security events
A.13.1.2	Reporting security weaknesses
A.13.2	Management of information security incidents and improvements
A.13.2.1	Responsibilities and procedures
A.13.2.2	Learning from information security incidents
A.13.2.3	Collection of evidence
A.14	Business continuity management
A.14.1	Information security aspects of business continuity management
A.14.1.1	Including information security in the business continuity management process
A.14.1.2	Business continuity and risk assessment
A.14.1.3	Developing and implementing continuity plans including information security
A.14.1.4	Business continuity planning framework
A.14.1.5	Testing, maintaining and reassessing business continuity plans

ISO 27000

A.15	Compliance
A.15.1	Compliance with legal requirements
A.15.1.1	Identification of applicable legislation
A.15.1.2	Intellectual property rights (IPR)
A.15.1.3	Protection of organizational records
A.15.1.4	Data protection and privacy of personal information
A.15.1.5	Prevention of misuse of information processing facilities
A.15.1.6	Regulation of cryptographic controls
A.15.2	Compliance with security policies and standards, and technical compliance
A.15.2.1	Compliance with security policies and standards
A.15.2.2	Technical compliance checking
A.15.3	Information systems audit considerations
A.15.3.1	Information systems audit controls
A.15.3.2	Protection of information systems audit tools