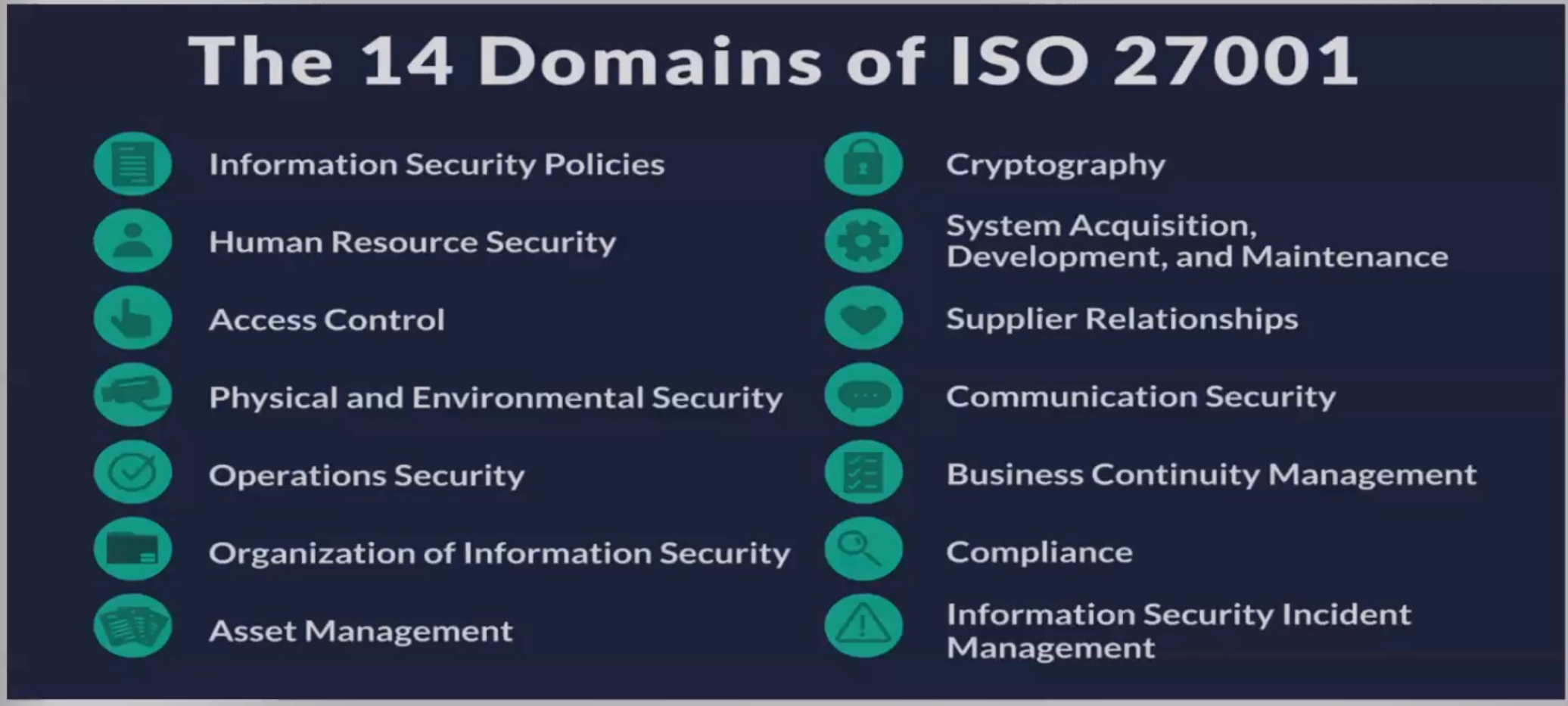
# Annex A – Continued



# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.1 Physical security perimeter

Control

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A.11.1.2 Physical entry controls

Control

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.3 Securing offices, rooms and facilities

Control

Physical security for offices, rooms and facilities shall be designed and applied.

A.11.1.4 Protecting against external and environmental threats

Control

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.1.5 Working in secure areas

Control

Procedures for working in secure areas shall be designed and applied.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organiza- tion's operations.

A.11.2.1 Equipment siting and protection

Control

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.11.2.2 Supporting utilities

Control

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.2.4 Equipment maintenance

Control

Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.11.2.5 Removal of assets

Control

Equipment, information or software shall not be taken off-site without prior authorization.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.6 Security of equipment and assets off-premises

Control

Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

A.11.2.7 Secure disposal or reuse of equipment

Control

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

# A.11 – Physical & Environmental Security

A.11 Physical and environmental security

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.8 Unattended user equipment

Control

Users shall ensure that unattended equipment has appropriate protection.

A.11.2.9 Clear desk and clear screen policy

Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

# A.12 –Operations Security

A.12 Operations security

A.12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

A.12.1.1 Documented operating procedures

Control

Operating procedures shall be documented and made available to all users who need them.

A.12.1.2 Change management

Control

Changes to the organization, business processes, information pro- cessing facilities and systems that affect information security shall be controlled.

# A.12 –Operations Security

A.12 Operations security

A.12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

A.12.1.3 Capacity management

Control

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required sys-tern performance.

A.12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments shall be sepa- rated to reduce the risks of unauthorized access or changes to the operational environment.

# A.12 –Operations Security

A.12 Operations security

A.12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

A.12.2.1 Controls against malware

Control

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.3 Backup

Objective: To protect against loss of data.

A.12.3.1 Information backup

Control

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

# A.12 –Operations Security

A.12 Operations security

A.12.4 Logging and monitoring

Objective: To record events and generate evidence.

A.12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information

Control

Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.4.3 Administrator and operator logs

Control

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

# A.12 –Operations Security

A.12 Operations security

A.12.4 Logging and monitoring

Objective: To record events and generate evidence.

A.12.4.4 Clock synchronization

Control

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

A.12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

A.12.5.1 Installation of software on operational systems

Control

Procedures shall be implemented to control the installation of soft-ware on operational systems.

# A.12 –Operations Security

A.12 Operations security

A.12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users shall be established and implemented.

# A.12 –Operations Security

A.12 Operations security

A.12.7 Information systems audit considerations

Objective: To minimize the impact of audit activities on operational systems.

A.12.7.1 Information systems audit controls

Control

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

# A.13 –Communications Security

A.13 Communications security

A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information pro- cessing facilities.

A.13.1.1 Network controls

Control

Networks shall be managed and controlled to protect information in systems and applications.

A.13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

# A.13 –Communications Security

A.13 Communications security

A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.3 Segregation in networks

Control

Groups of information services, users and information systems shall be segregated on networks.

A.13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

# A.13 –Communications Security

A.13 Communications security

A.13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.2 Agreements on information transfer

Control

Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 Electronic messaging

Control

Information involved in electronic messaging shall be appropriately protected.

A.13.2.4 Confidentiality or non-disclosure agreements

Control

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

# THANKS!