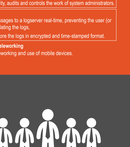
HOW BALABIT HELPS TO COMPLY WITH ISO 27001?

A.5 Information security policies

A.5.1 Management direction for information security
To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.



A.6 Organization of information security

A.6.1 Internal organization
To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Shell Control Box
- Creates a separate auditor layer above privileged users, segregates the role of IT maintenance and security, audits and controls the work of system administrators.

syslog-ng
- Securely transfer log messages to a logserver real-time, preventing the user (or an attacker) from manipulating the logs.
- on the logserver, it can store the logs in encrypted and time-stamped format.

A.6.2 Mobile devices and teleworking
To ensure the security of teleworking and use of mobile devices.

A.7 Human resource security

A.7.1 Prior to employment
To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7.2 During employment
To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

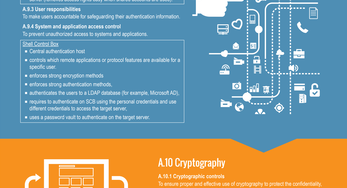
A.7.3 Termination and change of employment
To protect the organization's interests as part of the process of changing or terminating employment.

A.8 Asset management

A.8.1 Responsibility for assets
To identify organizational assets and define appropriate protection responsibilities.

A.8.2 Information classification
To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

A.8.3 Media handling
To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.



A.9 Access control

A.9.1 Business requirements of access control
To limit access to information and information processing facilities.

Shell Control Box
- Granularly controls access to servers, applications and protocol features, based on the identity of the user, or group-membership.

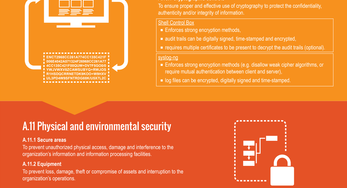
A.9.2 User access management
To ensure authorized user access and to prevent unauthorized access to systems and services.

Shell Control Box
- Controls remote access from a central location.
- enforces strong authentication and authorization.
- provides customized access control to audited systems.
- supports scenarios when the user does not know the credential of the server (removes access rights-way when shared accounts are used).

A.9.3 User responsibilities
To make users accountable for safeguarding their authentication information.

A.9.4 System and application access control
To prevent unauthorized access to systems and applications.

Shell Control Box
- Central authentication host
- controls which remote applications or protocol features are available for a specific user
- enforces strong encryption methods
- enforces strong authentication methods,
- authenticates the users to a LDAP database (for example, Microsoft AD),
- requires to authenticate on SCB using the personal credentials and use different credentials to access the target server,
- uses a password vault to authenticate on the target server.



A.10 Cryptography

A.10.1 Cryptographic controls
To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

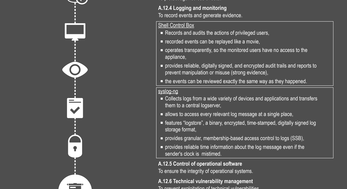
Shell Control Box
- Enforces strong encryption methods.
- audit trails can be digitally signed, time-stamped and encrypted,
- requires multiple certificates to be present to decrypt the audit trails (optional).

syslog-ng
- Enforces strong encryption methods (e.g. disallow weak cipher algorithms, or require mutual authentication between client and server).
- log files can be encrypted, digitally signed and time-stamped.

A.11 Physical and environmental security

A.11.1 Secure areas
To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.2 Equipment
To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.



A.12 Operations security

A.12.1 Operational procedures and responsibilities
To ensure correct and secure operations of information processing facilities.

Shell Control Box
- Complements change management policies and controls remote management of IT processing facilities,
- changes can be audited, and be part of the change documentation,
- audit trails can be used in forensic or general review to verify that a particular configuration change was actually performed.

syslog-ng
- Detects if its configuration changed and sends log message about it.

A.12.2 Protection from malware
To ensure that information and information processing facilities are protected against malware.

A.12.3 Backup
To protect against loss of data.

A.12.4 Logging and monitoring
To record events and generate evidence.

Shell Control Box
- Records and audits the actions of privileged users,
- recorded events can be replayed like a movie,
- operates transparently, so the monitored users have no access to the appliance,
- provides reliable, digitally signed, and encrypted audit trails and reports to prevent repudiation or misuse (strong evidence),
- the events can be reviewed exactly the same way as they happened.

syslog-ng
- Collects logs from a wide variety of devices and applications and transfers them to a central logserver,
- allows to access every relevant log message at a single place,
- features "logstore", a binary, encrypted, time-stamped, digitally signed log storage format,
- provides granular, membership-based access control to logs (SSB),
- provides reliable time information about the log message even if the sender's clock is mistimed.

A.12.5 Control of operational software
To ensure the integrity of operational systems.

A.12.6 Technical vulnerability management
To prevent exploitation of technical vulnerabilities.

A.12.7 Information systems audit considerations
To minimize the impact of audit activities on operational systems.

A.13 Communications security

A.13.1 Network security management
To ensure the protection of information in networks and its supporting information processing facilities.

Shell Control Box
- Controls, monitors, and audits the encrypted channels used in remote access,
- enforces strong authentication and authorization methods, incl. gateway authentication, two-factor authentication, and 4-eyes authorization,
- monitors the terminal connections used to access networking devices, such as switches,
- collects configuration changes of Cisco routers,
- prevents the network admins from executing unwanted commands.

syslog-ng
- TLS can be used to encrypt the communication between the clients and the log server,
- TLS-encryption also prevents third-parties from modifying the communication,
- The communication between the client and the server can be mutually authenticated using X.509 certificates.

A.13.2 Information transfer
To maintain the security of information transferred within an organization and with any external entity.

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems
To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.2 Security in development and support processes
To ensure that information security is designed and implemented within the development lifecycle of information systems.

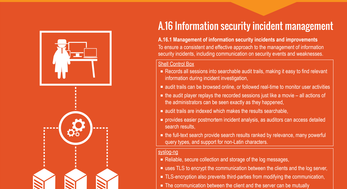
A.14.3 Test data
To ensure the protection of data used for testing.

A.15 Supplier relationships

A.15.1 Information security in supplier relationships
To ensure protection of the organization's assets that is accessible by suppliers.

A.15.2 Supplier service delivery management
To maintain an agreed level of information security and service delivery in line with supplier agreements.

Shell Control Box
- Oversees IT services managed by third parties,
- provides detailed audit trails and reports to review the actions of the third parties,
- offers granular access control to limit the access of the third party to the absolutely necessary.



A.16 Information security incident management

A.16.1 Management of information security incidents and improvements
To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Shell Control Box
- Records all sessions into searchable audit trails, making it easy to find relevant information during incident investigation,
- audit trails can be browsed online, or followed real-time to monitor user activities
- the audit player replays the recorded sessions just like a movie – all actions of the administrators can be seen exactly as they happened,
- audit trails are indexed which makes the results searchable,
- provides easier postmortem incident analysis, as auditors can access detailed search results,
- the full-text search provide search results ranked by relevance, many powerful query types, and support for non-Latin characters.

syslog-ng
- Reliable, secure collection and storage of the log messages,
- uses TLS to encrypt the communication between the clients and the log server,
- TLS-encryption also prevents third-parties from modifying the communication,
- The communication between the client and the server can be mutually authenticated using X.509 certificates,
- log messages can be encrypted using public-key encryption,
- requests time-stamps for the stored data from an external Timestamping Authority (TSA) to include reliable dates in the log files.

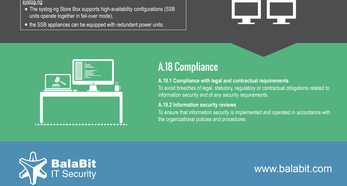
A.17 Information security aspects of business continuity management

A.17.1 Information security continuity
Information security continuity shall be embedded in the organization's business continuity management systems.

A.17.2 Redundancies
To ensure availability of information processing facilities.

Shell Control Box
- Supports high-availability configurations (two SCB units operate together in fail-over mode).
- the appliances can be equipped with redundant power units.

syslog-ng
- The syslog-ng Store Box supports high-availability configurations (SSB units operate together in fail-over mode).
- the SSB appliances can be equipped with redundant power units.



A.18 Compliance

A.18.1 Compliance with legal and contractual requirements
To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.2 Information security reviews
To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

BalaBit IT Security

www.balabit.com