

THE 14 CONTROL SETS OF ISO 27001:2013 (ANNEX A)

ISO 27001 is the international standard for effective information security management, offering a comprehensive approach to protecting an organisation's information from a wide range of threats and vulnerabilities.

The standard includes a set of 114 controls that are designed to mitigate information security risks. These controls are divided into 14 different categories, which are summarised below:



A.5 INFORMATION AND SECURITY **POLICIES** Information security policies need to be

approved from the top of the organisation and communicated clearly to all employees.



A.6 ORGANISATION OF INFORMATION SECURITY

A management framework supports all of the organisation's information security initiatives.





Employees and contractors should be aware of

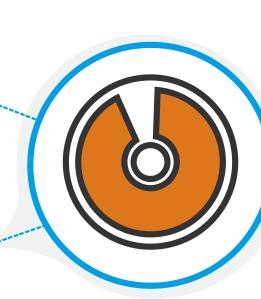
A.7 HUMAN RESOURCE SECURITY

their role in safeguarding the organisation's information.



Organisations need to identify their assets and determine the appropriate level of protection required for each.

A.8 ASSET MANAGEMENT





Access control should be implemented (with

A.9 ACCESS CONTROL

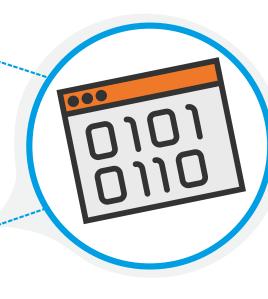
privileges frequently reviewed), and all users should be accountable for safeguarding their passwords.



Cryptography should be used effectively

A.10 CRYPTOGRAPHY

to protect the confidentiality, authenticity, and integrity of information.



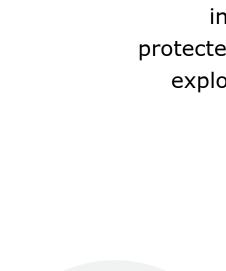


ENVIRONMENTAL SECURITY Appropriate measures must be taken to prevent unauthorised access to the

A.11 PHYSICAL AND

organisation's information.





information processing facilities are protected from malware, loss of data, and

exploitation of technical vulnerabilities.

security into the development lifecycle of

information systems and protect data

throughout the testing process.



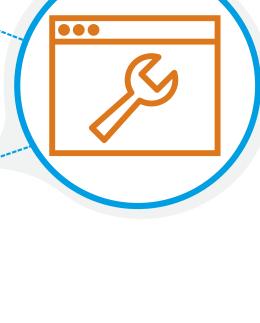


of any information transferred, both internally and externally.

A.13 COMMUNICATIONS

SECURITY

Organisations need to maintain the security



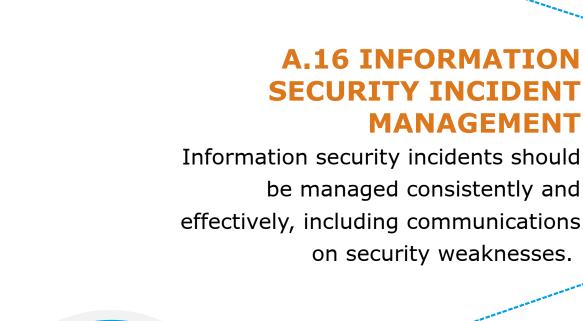


A.15 SUPPLIER

RELATIONSHIPS

A.16 INFORMATION SECURITY INCIDENT

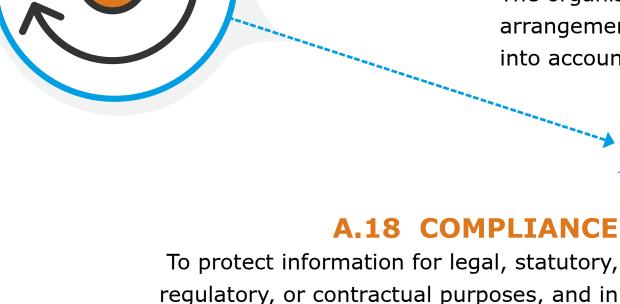
Assets need to be protected while remaining accessible to suppliers.



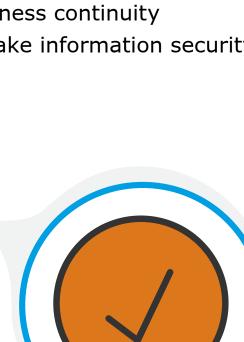
MANAGEMENT

be managed consistently and effectively, including communications on security weaknesses.





into account.



A.18 COMPLIANCE

regulatory, or contractual purposes, and in accordance with organisational requirements.



Implement an ISO 27001-compliant ISMS at a fraction of the cost

Achieve ISO 27001 compliance with our affordable DIY packages that include everything from copies of the standards, implementation guides, documentation toolkits, risk assessment software, training courses and qualifications and consultancy.



Let's get your ISO 27001