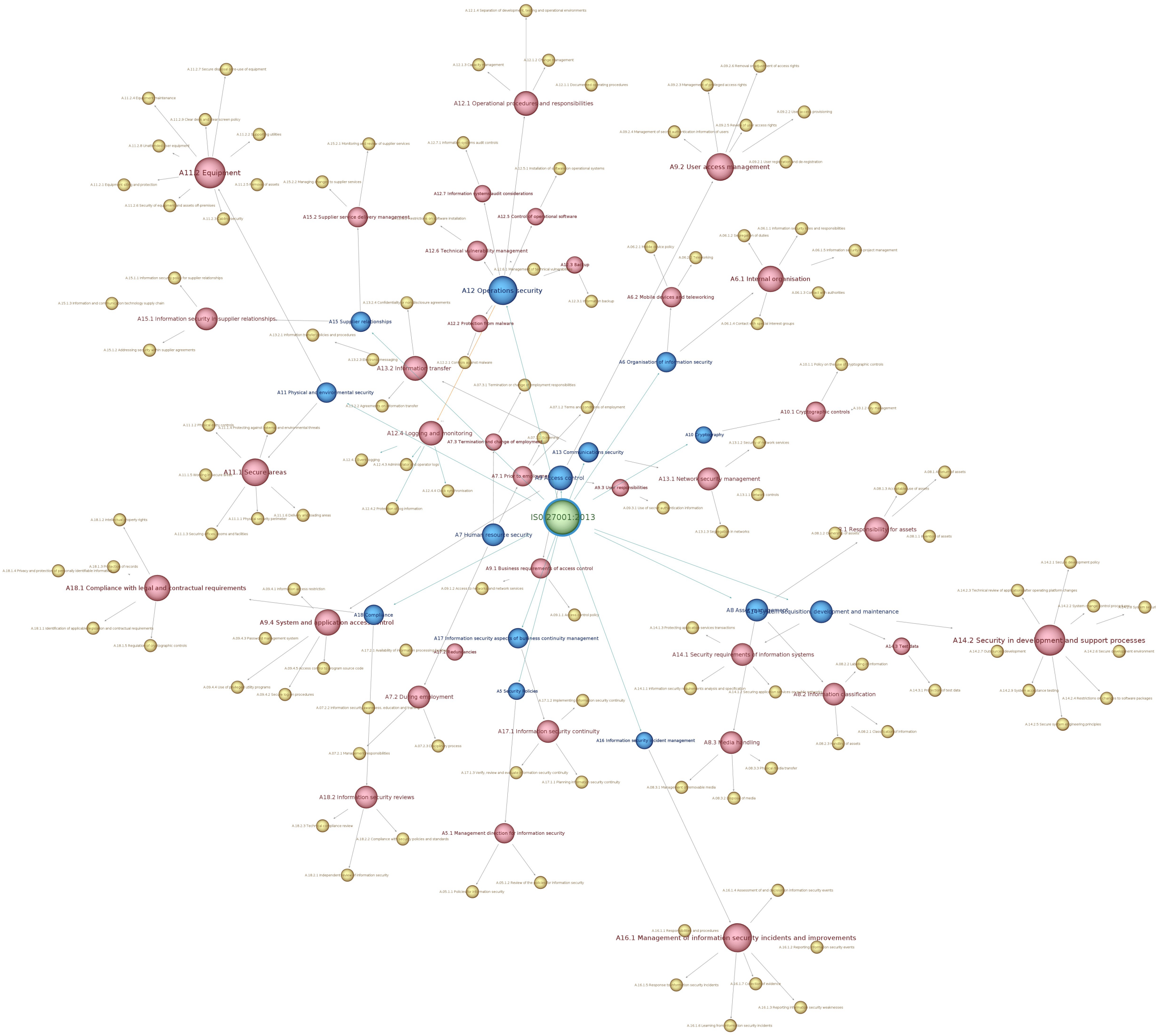

A.12.1.4 Separation of development, testing and operational environments
A.12.1.3 Capacity management
A.12.1.2 Change management
A.12.1.1 Documented operating procedures
A12.1 Operational procedures and responsibilities
A.11.2.7 Secure disposal or re-use of equipment
A.11.2.4 Equipment maintenance
A.11.2.9 Clear desk and clear screen policy
A.11.2.2 Supporting utilities
A.11.2.8 Unattended user equipment
A11.2 Equipment
A.11.2.1 Equipment siting and protection
A.11.2.5 Removal of assets
A.11.2.6 Security of equipment and assets off-premises
A.11.2.3 Cabling security
A.15.2.1 Monitoring and review of supplier services
A.15.2.2 Managing changes to supplier services
A15.2 Supplier service delivery management
A.12.6.2 Restrictions on software installation
A.12.7.1 Information systems audit controls
A12.7 Information systems audit considerations
A.12.5.1 Installation of software on operational systems
A12.5 Control of operational software
A12.6 Technical vulnerability management
A.12.6.1 Management of technical vulnerabilities
A12.3 Backup
A.12.3.1 Information backup
A12 Operations security
A12.2 Protection from malware
A.12.2.1 Controls against malware
A.09.2.6 Removal or adjustment of access rights
A.09.2.3 Management of privileged access rights
A.09.2.2 User access provisioning
A.09.2.5 Review of user access rights
A.09.2.4 Management of secret authentication information of users
A.09.2.1 User registration and de-registration
A9.2 User access management
A.06.1.1 Information security roles and responsibilities
A.06.1.2 Segregation of duties
A.06.1.5 Information security in project management
A.06.2.1 Mobile device policy
A.06.2.2 Teleworking
A6.1 Internal organisation
A.06.1.3 Contact with authorities
A6.2 Mobile devices and teleworking
A.06.1.4 Contact with special interest groups
A6 Organisation of information security
A.15.1.1 Information security policy for supplier relationships
A.15.1.3 Information and communication technology supply chain
A15.1 Information security in supplier relationships
A.15.1.2 Addressing security within supplier agreements
A.13.2.4 Confidentiality or non-disclosure agreements
A15 Supplier relationships
A.13.2.1 Information transfer policies and procedures
A.13.2.3 Electronic messaging
A13.2 Information transfer
A.07.3.1 Termination or change of employment responsibilities
A11 Physical and environmental security
A.13.2.2 Agreements on information transfer
A.07.1.2 Terms and conditions of employment
A.10.1.1 Policy on the use of cryptographic controls
A10.1 Cryptographic controls
A.10.1.2 Key management
A.11.1.2 Physical entry controls
A.11.1.4 Protecting against external and environmental threats
A12.4 Logging and monitoring
A7.3 Termination and change of employment
A.07.1.1 Screening
A10 Cryptography
A.13.1.2 Security of network services
A13 Communications security
A.12.4.1 Event logging
A.12.4.3 Administrator and operator logs
A.11.1.5 Working in secure areas
A11.1 Secure areas
A7.1 Prior to employment
A9 Access control
A13.1 Network security management
A.08.1.4 Return of assets
A9.3 User responsibilities
A.12.4.4 Clock synchronisation
A.13.1.1 Network controls
A.08.1.3 Acceptable use of assets
A.09.3.1 Use of secret authentication information
A.12.4.2 Protection of log information
A.11.1.6 Delivery and loading areas
A.11.1.1 Physical security perimeter
ISO 27001:2013
A.18.1.2 Intellectual property rights
A.11.1.3 Securing offices, rooms and facilities
A.13.1.3 Segregation in networks
A.08.1.2 Ownership of assets
A8.1 Responsibility for assets
A.08.1.1 Inventory of assets
A7 Human resource security
A.18.1.3 Protection of records
A.18.1.4 Privacy and protection of personally identifiable information
A9.1 Business requirements of access control
A.14.2.1 Secure development policy
A18.1 Compliance with legal and contractual requirements
A.09.4.1 Information access restriction
A.09.1.2 Access to networks and network services
A.14.2.3 Technical review of applications after operating platform changes
A.14.2.2 System change control procedures
A.14.2.8 System security testing
A8 Asset management
A14 System acquisition, development and maintenance
A18 Compliance
A.09.1.1 Access control policy
A9.4 System and application access control
A.18.1.1 Identification of applicable legislation and contractual requirements
A.14.1.3 Protecting application services transactions
A14.2 Security in development and support processes
A.09.4.3 Password management system
A17 Information security aspects of business continuity management
A.18.1.5 Regulation of cryptographic controls
A.17.2.1 Availability of information processing facilities
A17.2 Redundancies
A14.1 Security requirements of information systems
A14.3 Test data
A.14.2.7 Outsourced development
A.14.2.6 Secure development environment
A.09.4.5 Access control to program source code
A.08.2.2 Labelling of information
A.09.4.4 Use of privileged utility programs
A.09.4.2 Secure log-on procedures
A.14.1.1 Information security requirements analysis and specification
A.14.1.2 Securing application services on public networks
A5 Security Policies
A.14.3.1 Protection of test data
A.14.2.9 System acceptance testing
A8.2 Information classification
A.14.2.4 Restrictions on changes to software packages
A7.2 During employment
A.07.2.2 Information security awareness, education and training
A.17.1.2 Implementing information security continuity
A.14.2.5 Secure system engineering principles
A17.1 Information security continuity
A.08.2.1 Classification of information
A16 Information security incident management
A8.3 Media handling
A.08.2.3 Handling of assets
A.07.2.3 Disciplinary process
A.07.2.1 Management responsibilities
A.08.3.3 Physical media transfer
A.17.1.3 Verify, review and evaluate information security continuity
A.17.1.1 Planning information security continuity
A.08.3.1 Management of removable media
A18.2 Information security reviews
A.08.3.2 Disposal of media
A.18.2.3 Technical compliance review
A5.1 Management direction for information security
A.18.2.2 Compliance with security policies and standards
A.18.2.1 Independent review of information security
A.05.1.2 Review of the policies for information security
A.05.1.1 Policies for information security
A.16.1.4 Assessment of and decision on information security events
A.16.1.1 Responsibilities and procedures
A16.1 Management of information security incidents and improvements
A.16.1.2 Reporting information security events
A.16.1.5 Response to information security incidents
A.16.1.7 Collection of evidence
A.16.1.3 Reporting information security weaknesses
A.16.1.6 Learning from information security incidents

1. Top 10 Entities

Total number of entities	164
Total number of entities	163

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	ISO27001.AFAM	A5 Security Policies	1
2	ISO27001.AOBJ	A5.1 Management direction for information security	1
3	ISO27001.ACTRL	A.05.1.1 Policies for information security	1
4	ISO27001.ACTRL	A.05.1.2 Review of the policies for information security	1
5	ISO27001.AOBJ	A6.1 Internal organisation	1
6	ISO27001.AFAM	A6 Organisation of information security	1
7	ISO27001.ACTRL	A.06.1.1 Information security roles and responsibilities	1
8	ISO27001.ACTRL	A.06.1.2 Segregation of duties	1
9	ISO27001.ACTRL	A.06.1.3 Contact with authorities	1
10	ISO27001.ACTRL	A.06.1.4 Contact with special interest groups	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	ISO27001.A	IS0 27001:2013	14
2	ISO27001.AOBJ	A11.2 Equipment	9
3	ISO27001.AOBJ	A14.2 Security in development and support processes	9
4	ISO27001.AFAM	A12 Operations security	7
5	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements	7
6	ISO27001.AOBJ	A9.2 User access management	6
7	ISO27001.AOBJ	A11.1 Secure areas	6
8	ISO27001.AOBJ	A6.1 Internal organisation	5
9	ISO27001.AOBJ	A9.4 System and application access control	5
10	ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements	5

Ranked by Total Links

Rank	Type	Value	Total links
1	ISO27001.A	IS0 27001:2013	14
2	ISO27001.AOBJ	A11.2 Equipment	10
3	ISO27001.AOBJ	A14.2 Security in development and support processes	10
4	ISO27001.AFAM	A12 Operations security	8
5	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements	8
6	ISO27001.AOBJ	A9.2 User access management	7
7	ISO27001.AOBJ	A11.1 Secure areas	7
8	ISO27001.AOBJ	A6.1 Internal organisation	6
9	ISO27001.AOBJ	A9.4 System and application access control	6
10	ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements	6

2. Entities by Type

ISO27001.ACTRLs (114)	
A.05.1.1 Policies for information security	A.05.1.2 Review of the policies for information security
A.06.1.1 Information security roles and responsibilities	A.06.1.2 Segregation of duties
A.06.1.3 Contact with authorities	A.06.1.4 Contact with special interest groups
A.06.1.5 Information security in project management	A.06.2.1 Mobile device policy
A.06.2.2 Teleworking	A.07.1.1 Screening
A.07.1.2 Terms and conditions of employment	A.07.2.1 Management responsibilities
A.07.2.2 Information security awareness, education and training	A.07.2.3 Disciplinary process
A.07.3.1 Termination or change of employment responsibilities	A.08.1.1 Inventory of assets
A.08.1.2 Ownership of assets	A.08.1.3 Acceptable use of assets
A.08.1.4 Return of assets	A.08.2.1 Classification of information
A.08.2.2 Labelling of information	A.08.2.3 Handling of assets
A.08.3.1 Management of removable media	A.08.3.2 Disposal of media
A.08.3.3 Physical media transfer	A.09.1.1 Access control policy
A.09.1.2 Access to networks and network services	A.09.2.1 User registration and de-registration
A.09.2.2 User access provisioning	A.09.2.3 Management of privileged access rights
A.09.2.4 Management of secret authentication information of users	A.09.2.5 Review of user access rights
A.09.2.6 Removal or adjustment of access rights	A.09.3.1 Use of secret authentication information
A.09.4.1 Information access restriction	A.09.4.2 Secure log-on procedures
A.09.4.3 Password management system	A.09.4.4 Use of privileged utility programs
A.09.4.5 Access control to program source code	A.10.1.1 Policy on the use of cryptographic controls
A.10.1.2 Key management	A.11.1.1 Physical security perimeter
A.11.1.2 Physical entry controls	A.11.1.3 Securing offices, rooms and facilities
A.11.1.4 Protecting against external and environmental threats	A.11.1.5 Working in secure areas
A.11.1.6 Delivery and loading areas	A.11.2.1 Equipment siting and protection
A.11.2.2 Supporting utilities	A.11.2.3 Cabling security
A.11.2.4 Equipment maintenance	A.11.2.5 Removal of assets
A.11.2.6 Security of equipment and assets off-premises	A.11.2.7 Secure disposal or re-use of equipment
A.11.2.8 Unattended user equipment	A.11.2.9 Clear desk and clear screen policy
A.12.1.1 Documented operating procedures	A.12.1.2 Change management
A.12.1.3 Capacity management	A.12.1.4 Separation of development, testing and operational environments
A.12.2.1 Controls against malware	A.12.3.1 Information backup
A.12.4.1 Event logging	A.12.4.2 Protection of log information
A.12.4.3 Administrator and operator logs	A.12.4.4 Clock synchronisation
A.12.5.1 Installation of software on operational systems	A.12.6.1 Management of technical vulnerabilities
A.12.6.2 Restrictions on software installation	A.12.7.1 Information systems audit controls
A.13.1.1 Network controls	A.13.1.2 Security of network services
A.13.1.3 Segregation in networks	A.13.2.1 Information transfer policies and procedures
A.13.2.2 Agreements on information transfer	A.13.2.3 Electronic messaging
A.13.2.4 Confidentiality or non-disclosure agreements	A.14.1.1 Information security requirements analysis and specification
A.14.1.2 Securing application services on public networks	A.14.1.3 Protecting application services transactions
A.14.2.1 Secure development policy	A.14.2.2 System change control procedures

- A.14.2.3 Technical review of applications after operating platform changes
- A.14.2.4 Restrictions on changes to software packages
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.7 Outsourced development
- A.14.2.8 System security testing
- A.14.2.9 System acceptance testing
- A.14.3.1 Protection of test data
- A.15.1.1 Information security policy for supplier relationships
- A.15.1.2 Addressing security within supplier agreements
- A.15.1.3 Information and communication technology supply chain
- A.15.2.1 Monitoring and review of supplier services
- A.15.2.2 Managing changes to supplier services
- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weaknesses
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence
- A.17.1.1 Planning information security continuity
- A.17.1.2 Implementing information security continuity
- A.17.1.3 Verify, review and evaluate information security continuity
- A.17.2.1 Availability of information processing facilities
- A.18.1.1 Identification of applicable legislation and contractual requirements
- A.18.1.2 Intellectual property rights
- A.18.1.3 Protection of records
- A.18.1.4 Privacy and protection of personally identifiable information
- A.18.1.5 Regulation of cryptographic controls
- A.18.2.1 Independent review of information security
- A.18.2.2 Compliance with security policies and standards
- A.18.2.3 Technical compliance review

ISO27001.As (1)

- IS0 27001:2013

ISO27001.AOBJs (35)

- A11.2 Equipment
- A14.2 Security in development and support processes
- A16.1 Management of information security incidents and improvements
- A9.2 User access management
- A11.1 Secure areas
- A6.1 Internal organisation
- A9.4 System and application access control
- A18.1 Compliance with legal and contractual requirements
- A8.1 Responsibility for assets
- A12.1 Operational procedures and responsibilities
- A12.4 Logging and monitoring
- A13.2 Information transfer
- A7.2 During employment
- A8.2 Information classification
- A8.3 Media handling
- A13.1 Network security management
- A14.1 Security requirements of information systems
- A15.1 Information security in supplier relationships
- A17.1 Information security continuity
- A18.2 Information security reviews
- A5.1 Management direction for information security
- A6.2 Mobile devices and teleworking
- A7.1 Prior to employment
- A9.1 Business requirements of access control
- A10.1 Cryptographic controls
- A12.6 Technical vulnerability management
- A15.2 Supplier service delivery management
- A7.3 Termination and change of employment
- A9.3 User responsibilities
- A12.2 Protection from malware
- A12.3 Backup
- A12.5 Control of operational software
- A12.7 Information systems audit considerations
- A14.3 Test data
- A17.2 Redundancies

ISO27001.AFAMs (14)

- A12 Operations security
- A9 Access control
- A7 Human resource security
- A8 Asset management
- A14 System acquisition, development and maintenance
- A6 Organisation of information security

A11 Physical and environmental security	A13 Communications security
A15 Supplier relationships	A17 Information security aspects of business continuity management
A18 Compliance	A5 Security Policies
A10 Cryptography	A16 Information security incident management

3. Entity Details

ISO27001.A

7FORTRESS.ISO27001.A

IS0 27001:2013

ISO27001.A	IS0 27001:2013
Size	253
Bookmark	-1

Outgoing (14)

ISO27001.AFAM	A5 Security Policies
ISO27001.AFAM	A6 Organisation of information security
ISO27001.AFAM	A7 Human resource security
ISO27001.AFAM	A8 Asset management
ISO27001.AFAM	A9 Access control
ISO27001.AFAM	A10 Cryptography
ISO27001.AFAM	A11 Physical and environmental security
ISO27001.AFAM	A12 Operations security
ISO27001.AFAM	A13 Communications security
ISO27001.AFAM	A14 System acquisition, development and maintenance
ISO27001.AFAM	A15 Supplier relationships
ISO27001.AFAM	A16 Information security incident management
ISO27001.AFAM	A17 Information security aspects of business continuity management
ISO27001.AFAM	A18 Compliance

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A11.2 Equipment

ISO27001.AOBJ	A11.2 Equipment
Size	229
Bookmark	-1

Incoming (1)

ISO27001.AFAM	A11 Physical and environmental security

Outgoing (9)

ISO27001.ACTRL	A.11.2.1 Equipment siting and protection
ISO27001.ACTRL	A.11.2.2 Supporting utilities
ISO27001.ACTRL	A.11.2.3 Cabling security
ISO27001.ACTRL	A.11.2.4 Equipment maintenance
ISO27001.ACTRL	A.11.2.5 Removal of assets
ISO27001.ACTRL	A.11.2.6 Security of equipment and assets off-premises
ISO27001.ACTRL	A.11.2.7 Secure disposal or re-use of equipment
ISO27001.ACTRL	A.11.2.8 Unattended user equipment
ISO27001.ACTRL	A.11.2.9 Clear desk and clear screen policy

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A14.2 Security in development and support processes

ISO27001.AOBJ	A14.2 Security in development and support processes
Size	229
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A14 System acquisition, development and maintenance
Outgoing (9)		
●	ISO27001.ACTRL	A.14.2.1 Secure development policy
●	ISO27001.ACTRL	A.14.2.2 System change control procedures
●	ISO27001.ACTRL	A.14.2.3 Technical review of applications after operating platform changes
●	ISO27001.ACTRL	A.14.2.4 Restrictions on changes to software packages
●	ISO27001.ACTRL	A.14.2.5 Secure system engineering principles
●	ISO27001.ACTRL	A.14.2.6 Secure development environment
●	ISO27001.ACTRL	A.14.2.7 Outsourced development
●	ISO27001.ACTRL	A.14.2.8 System security testing
●	ISO27001.ACTRL	A.14.2.9 System acceptance testing

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A12 Operations security

ISO27001.AFAM	A12 Operations security
Size	214
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	ISO 27001:2013
Outgoing (7)		
♜	ISO27001.AOBJ	A12.1 Operational procedures and responsibilities
♜	ISO27001.AOBJ	A12.2 Protection from malware
♜	ISO27001.AOBJ	A12.3 Backup
♜	ISO27001.AOBJ	A12.4 Logging and monitoring
♜	ISO27001.AOBJ	A12.5 Control of operational software
♜	ISO27001.AOBJ	A12.6 Technical vulnerability management
♜	ISO27001.AOBJ	A12.7 Information systems audit considerations

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A16.1 Management of information security incidents and improvements

ISO27001.AOBJ	A16.1 Management of information security incidents and improvements
Size	214
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A16 Information security incident management
Outgoing (7)		
●	ISO27001.ACTRL	A.16.1.1 Responsibilities and procedures
●	ISO27001.ACTRL	A.16.1.2 Reporting information security events
●	ISO27001.ACTRL	A.16.1.3 Reporting information security weaknesses
●	ISO27001.ACTRL	A.16.1.4 Assessment of and decision on information security events
●	ISO27001.ACTRL	A.16.1.5 Response to information security incidents
●	ISO27001.ACTRL	A.16.1.6 Learning from information security incidents
●	ISO27001.ACTRL	A.16.1.7 Collection of evidence

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A9.2 User access management

ISO27001.AOBJ	A9.2 User access management
Size	205
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A9 Access control
Outgoing (6)		
●	ISO27001.ACTRL	A.09.2.1 User registration and de-registration
●	ISO27001.ACTRL	A.09.2.2 User access provisioning
●	ISO27001.ACTRL	A.09.2.3 Management of privileged access rights
●	ISO27001.ACTRL	A.09.2.4 Management of secret authentication information of users
●	ISO27001.ACTRL	A.09.2.5 Review of user access rights
●	ISO27001.ACTRL	A.09.2.6 Removal or adjustment of access rights

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A11.1 Secure areas

ISO27001.AOBJ	A11.1 Secure areas
Size	205
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A11 Physical and environmental security
Outgoing (6)		
●	ISO27001.ACTRL	A.11.1.1 Physical security perimeter
●	ISO27001.ACTRL	A.11.1.2 Physical entry controls
●	ISO27001.ACTRL	A.11.1.3 Securing offices, rooms and facilities
●	ISO27001.ACTRL	A.11.1.4 Protecting against external and environmental threats
●	ISO27001.ACTRL	A.11.1.5 Working in secure areas
●	ISO27001.ACTRL	A.11.1.6 Delivery and loading areas

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A6.1 Internal organisation

ISO27001.AOBJ	A6.1 Internal organisation
Size	195
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A6 Organisation of information security
Outgoing (5)		
●	ISO27001.ACTRL	A.06.1.1 Information security roles and responsibilities
●	ISO27001.ACTRL	A.06.1.2 Segregation of duties
●	ISO27001.ACTRL	A.06.1.3 Contact with authorities
●	ISO27001.ACTRL	A.06.1.4 Contact with special interest groups
●	ISO27001.ACTRL	A.06.1.5 Information security in project management

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A9.4 System and application access control

ISO27001.AOBJ	A9.4 System and application access control
Size	195
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A9 Access control
Outgoing (5)		
●	ISO27001.ACTRL	A.09.4.1 Information access restriction
●	ISO27001.ACTRL	A.09.4.2 Secure log-on procedures
●	ISO27001.ACTRL	A.09.4.3 Password management system
●	ISO27001.ACTRL	A.09.4.4 Use of privileged utility programs
●	ISO27001.ACTRL	A.09.4.5 Access control to program source code

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A18.1 Compliance with legal and contractual requirements

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements
Size	195
Bookmark	-1

Incoming (1)

⚙	ISO27001.AFAM	A18 Compliance

Outgoing (5)

●	ISO27001.ACTRL	A.18.1.1 Identification of applicable legislation and contractual requirements
●	ISO27001.ACTRL	A.18.1.2 Intellectual property rights
●	ISO27001.ACTRL	A.18.1.3 Protection of records
●	ISO27001.ACTRL	A.18.1.4 Privacy and protection of personally identifiable information
●	ISO27001.ACTRL	A.18.1.5 Regulation of cryptographic controls

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A8.1 Responsibility for assets

ISO27001.AOBJ	A8.1 Responsibility for assets
Size	184
Bookmark	-1

Incoming (1)

⚙	ISO27001.AFAM	A8 Asset management

Outgoing (4)

●	ISO27001.ACTRL	A.08.1.1 Inventory of assets
●	ISO27001.ACTRL	A.08.1.2 Ownership of assets
●	ISO27001.ACTRL	A.08.1.3 Acceptable use of assets
●	ISO27001.ACTRL	A.08.1.4 Return of assets

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A9 Access control

ISO27001.AFAM	A9 Access control
Size	184
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	ISO 27001:2013
Outgoing (4)		
♜	ISO27001.AOBJ	A9.1 Business requirements of access control
♜	ISO27001.AOBJ	A9.2 User access management
♜	ISO27001.AOBJ	A9.3 User responsibilities
♜	ISO27001.AOBJ	A9.4 System and application access control

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.1 Operational procedures and responsibilities

ISO27001.AOBJ	A12.1 Operational procedures and responsibilities
Size	184
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A12 Operations security
Outgoing (4)		
●	ISO27001.ACTRL	A.12.1.1 Documented operating procedures
●	ISO27001.ACTRL	A.12.1.2 Change management
●	ISO27001.ACTRL	A.12.1.3 Capacity management
●	ISO27001.ACTRL	A.12.1.4 Separation of development, testing and operational environments

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.4 Logging and monitoring

ISO27001.AOBJ	A12.4 Logging and monitoring
Size	184
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A12 Operations security
Outgoing (4)		
●	ISO27001.ACTRL	A.12.4.1 Event logging
●	ISO27001.ACTRL	A.12.4.2 Protection of log information
●	ISO27001.ACTRL	A.12.4.3 Administrator and operator logs
●	ISO27001.ACTRL	A.12.4.4 Clock synchronisation

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A13.2 Information transfer

ISO27001.AOBJ	A13.2 Information transfer
Size	184
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A13 Communications security
Outgoing (4)		
●	ISO27001.ACTRL	A.13.2.1 Information transfer policies and procedures
●	ISO27001.ACTRL	A.13.2.2 Agreements on information transfer
●	ISO27001.ACTRL	A.13.2.3 Electronic messaging
●	ISO27001.ACTRL	A.13.2.4 Confidentiality or non-disclosure agreements

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A7 Human resource security

ISO27001.AFAM	A7 Human resource security
Size	170
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (3)		
♜	ISO27001.AOBJ	A7.1 Prior to employment
♜	ISO27001.AOBJ	A7.2 During employment
♜	ISO27001.AOBJ	A7.3 Termination and change of employment

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A7.2 During employment

ISO27001.AOBJ	A7.2 During employment
Size	170
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A7 Human resource security
Outgoing (3)		
●	ISO27001.ACTRL	A.07.2.1 Management responsibilities
●	ISO27001.ACTRL	A.07.2.2 Information security awareness, education and training
●	ISO27001.ACTRL	A.07.2.3 Disciplinary process

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A8 Asset management

	ISO27001.AFAM	A8 Asset management
	Size	170
	Bookmark	-1
Incoming (1)		
	ISO27001.A	ISO 27001:2013
Outgoing (3)		
	ISO27001.AOBJ	A8.1 Responsibility for assets
	ISO27001.AOBJ	A8.2 Information classification
	ISO27001.AOBJ	A8.3 Media handling

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A8.2 Information classification

	ISO27001.AOBJ	A8.2 Information classification
	Size	170
	Bookmark	-1
Incoming (1)		
	ISO27001.AFAM	A8 Asset management
Outgoing (3)		
	ISO27001.ACTRL	A.08.2.1 Classification of information
	ISO27001.ACTRL	A.08.2.2 Labelling of information
	ISO27001.ACTRL	A.08.2.3 Handling of assets

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A8.3 Media handling

	ISO27001.AOBJ	A8.3 Media handling
	Size	170
	Bookmark	-1
Incoming (1)		
	ISO27001.AFAM	A8 Asset management
Outgoing (3)		
	ISO27001.ACTRL	A.08.3.1 Management of removable media
	ISO27001.ACTRL	A.08.3.2 Disposal of media
	ISO27001.ACTRL	A.08.3.3 Physical media transfer

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A13.1 Network security management

	ISO27001.AOBJ	A13.1 Network security management
	Size	170
	Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A13 Communications security

Outgoing (3)		
●	ISO27001.ACTRL	A.13.1.1 Network controls
●	ISO27001.ACTRL	A.13.1.2 Security of network services
●	ISO27001.ACTRL	A.13.1.3 Segregation in networks

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A14 System acquisition, development and maintenance

	ISO27001.AFAM	A14 System acquisition, development and maintenance
	Size	170
	Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013

Outgoing (3)		
♜	ISO27001.AOBJ	A14.1 Security requirements of information systems
♜	ISO27001.AOBJ	A14.2 Security in development and support processes
♜	ISO27001.AOBJ	A14.3 Test data

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A14.1 Security requirements of information systems

	ISO27001.AOBJ	A14.1 Security requirements of information systems
	Size	170
	Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A14 System acquisition, development and maintenance

Outgoing (3)		
●	ISO27001.ACTRL	A.14.1.1 Information security requirements analysis and specification
●	ISO27001.ACTRL	A.14.1.2 Securing application services on public networks
●	ISO27001.ACTRL	A.14.1.3 Protecting application services transactions

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A15.1 Information security in supplier relationships

	ISO27001.AOBJ	A15.1 Information security in supplier relationships
	Size	170
	Bookmark	-1
Incoming (1)		
⚙	ISO27001.AFAM	A15 Supplier relationships
Outgoing (3)		
●	ISO27001.ACTRL	A.15.1.1 Information security policy for supplier relationships
●	ISO27001.ACTRL	A.15.1.2 Addressing security within supplier agreements
●	ISO27001.ACTRL	A.15.1.3 Information and communication technology supply chain

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A17.1 Information security continuity

	ISO27001.AOBJ	A17.1 Information security continuity
	Size	170
	Bookmark	-1
Incoming (1)		
⚙	ISO27001.AFAM	A17 Information security aspects of business continuity management
Outgoing (3)		
●	ISO27001.ACTRL	A.17.1.1 Planning information security continuity
●	ISO27001.ACTRL	A.17.1.2 Implementing information security continuity
●	ISO27001.ACTRL	A.17.1.3 Verify, review and evaluate information security continuity

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A18.2 Information security reviews

	ISO27001.AOBJ	A18.2 Information security reviews
	Size	170
	Bookmark	-1
Incoming (1)		
⚙	ISO27001.AFAM	A18 Compliance
Outgoing (3)		
●	ISO27001.ACTRL	A.18.2.1 Independent review of information security
●	ISO27001.ACTRL	A.18.2.2 Compliance with security policies and standards
●	ISO27001.ACTRL	A.18.2.3 Technical compliance review

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A5.1 Management direction for information security

ISO27001.AOBJ	A5.1 Management direction for information security
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A5 Security Policies
Outgoing (2)		
●	ISO27001.ACTRL	A.05.1.1 Policies for information security
●	ISO27001.ACTRL	A.05.1.2 Review of the policies for information security

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A6 Organisation of information security

ISO27001.AFAM	A6 Organisation of information security
Size	153
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A6.1 Internal organisation
♜	ISO27001.AOBJ	A6.2 Mobile devices and teleworking

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A6.2 Mobile devices and teleworking

ISO27001.AOBJ	A6.2 Mobile devices and teleworking
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A6 Organisation of information security
Outgoing (2)		
●	ISO27001.ACTRL	A.06.2.1 Mobile device policy
●	ISO27001.ACTRL	A.06.2.2 Teleworking

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A7.1 Prior to employment

ISO27001.AOBJ	A7.1 Prior to employment
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A7 Human resource security
Outgoing (2)		
●	ISO27001.ACTRL	A.07.1.1 Screening
●	ISO27001.ACTRL	A.07.1.2 Terms and conditions of employment

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A9.1 Business requirements of access control

ISO27001.AOBJ	A9.1 Business requirements of access control
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A9 Access control
Outgoing (2)		
●	ISO27001.ACTRL	A.09.1.1 Access control policy
●	ISO27001.ACTRL	A.09.1.2 Access to networks and network services

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A10.1 Cryptographic controls

ISO27001.AOBJ	A10.1 Cryptographic controls
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A10 Cryptography
Outgoing (2)		
●	ISO27001.ACTRL	A.10.1.1 Policy on the use of cryptographic controls
●	ISO27001.ACTRL	A.10.1.2 Key management

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A11 Physical and environmental security

ISO27001.AFAM	A11 Physical and environmental security
Size	153
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A11.1 Secure areas
♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.6 Technical vulnerability management

ISO27001.AOBJ	A12.6 Technical vulnerability management
Size	153
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A12 Operations security
Outgoing (2)		
●	ISO27001.ACTRL	A.12.6.1 Management of technical vulnerabilities
●	ISO27001.ACTRL	A.12.6.2 Restrictions on software installation

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A13 Communications security

ISO27001.AFAM	A13 Communications security
Size	153
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A13.1 Network security management
♜	ISO27001.AOBJ	A13.2 Information transfer

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A15 Supplier relationships

ISO27001.AFAM	A15 Supplier relationships
Size	153
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A15.1 Information security in supplier relationships
♜	ISO27001.AOBJ	A15.2 Supplier service delivery management

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A15.2 Supplier service delivery management

	ISO27001.AOBJ	A15.2 Supplier service delivery management
	Size	153
	Bookmark	-1
Incoming (1)		
⚙	ISO27001.AFAM	A15 Supplier relationships
Outgoing (2)		
●	ISO27001.ACTRL	A.15.2.1 Monitoring and review of supplier services
●	ISO27001.ACTRL	A.15.2.2 Managing changes to supplier services

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A17 Information security aspects of business continuity management

	ISO27001.AFAM	A17 Information security aspects of business continuity management
	Size	153
	Bookmark	-1
Incoming (1)		
▲	ISO27001.A	IS0 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A17.1 Information security continuity
♜	ISO27001.AOBJ	A17.2 Redundancies

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A18 Compliance

	ISO27001.AFAM	A18 Compliance
	Size	153
	Bookmark	-1

Incoming (1)		
◆	ISO27001.A	ISO 27001:2013
Outgoing (2)		
♜	ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements
♜	ISO27001.AOBJ	A18.2 Information security reviews

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A5 Security Policies

ISO27001.AFAM	A5 Security Policies
Size	132
Bookmark	-1

Incoming (1)		
◆	ISO27001.A	ISO 27001:2013
Outgoing (1)		
♜	ISO27001.AOBJ	A5.1 Management direction for information security

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A7.3 Termination and change of employment

ISO27001.AOBJ	A7.3 Termination and change of employment
Size	132
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A7 Human resource security
Outgoing (1)		
●	ISO27001.ACTRL	A.07.3.1 Termination or change of employment responsibilities

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A9.3 User responsibilities

ISO27001.AOBJ	A9.3 User responsibilities
Size	132
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A9 Access control
Outgoing (1)		
●	ISO27001.ACTRL	A.09.3.1 Use of secret authentication information

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A10 Cryptography

ISO27001.AFAM	A10 Cryptography
Size	132
Bookmark	-1

Incoming (1)

ISO27001.A	ISO 27001:2013

Outgoing (1)

ISO27001.AOBJ	A10.1 Cryptographic controls

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.2 Protection from malware

ISO27001.AOBJ	A12.2 Protection from malware
Size	132
Bookmark	-1

Incoming (1)

ISO27001.AFAM	A12 Operations security

Outgoing (1)

●	ISO27001.ACTRL	A.12.2.1 Controls against malware

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.3 Backup

ISO27001.AOBJ	A12.3 Backup
Size	132
Bookmark	-1

Incoming (1)

ISO27001.AFAM	A12 Operations security

Outgoing (1)

●	ISO27001.ACTRL	A.12.3.1 Information backup

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.5 Control of operational software

ISO27001.AOBJ	A12.5 Control of operational software
Size	132
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A12 Operations security
Outgoing (1)		
●	ISO27001.ACTRL	A.12.5.1 Installation of software on operational systems

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A12.7 Information systems audit considerations

ISO27001.AOBJ	A12.7 Information systems audit considerations
Size	132
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A12 Operations security
Outgoing (1)		
●	ISO27001.ACTRL	A.12.7.1 Information systems audit controls

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A14.3 Test data

ISO27001.AOBJ	A14.3 Test data
Size	132
Bookmark	-1

Incoming (1)		
⚙	ISO27001.AFAM	A14 System acquisition, development and maintenance
Outgoing (1)		
●	ISO27001.ACTRL	A.14.3.1 Protection of test data

ISO27001.AFAM

7FORTRESS.ISO27001.AFAM

A16 Information security incident management

ISO27001.AFAM	A16 Information security incident management
Size	132
Bookmark	-1

Incoming (1)		
▲	ISO27001.A	ISO 27001:2013
Outgoing (1)		
♜	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.AOBJ

7FORTRESS.ISO27001.AOBJ

A17.2 Redundancies

ISO27001.AOBJ	A17.2 Redundancies
Size	132
Bookmark	-1

Incoming (1)

ISO27001.AFAM	A17 Information security aspects of business continuity management

Outgoing (1)

ISO27001.ACTRL	A.17.2.1 Availability of information processing facilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.05.1.1 Policies for information security

ISO27001.ACTRL	A.05.1.1 Policies for information security
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A5.1 Management direction for information security

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.05.1.2 Review of the policies for information security

ISO27001.ACTRL	A.05.1.2 Review of the policies for information security
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A5.1 Management direction for information security

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.1.1 Information security roles and responsibilities

ISO27001.ACTRL	A.06.1.1 Information security roles and responsibilities
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A6.1 Internal organisation

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.1.2 Segregation of duties

ISO27001.ACTRL	A.06.1.2 Segregation of duties
Size	101
Bookmark	-1

Incoming (1)

	ISO27001.AOBJ	A6.1 Internal organisation

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.1.3 Contact with authorities

ISO27001.ACTRL	A.06.1.3 Contact with authorities
Size	101
Bookmark	-1

Incoming (1)

	ISO27001.AOBJ	A6.1 Internal organisation

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.1.4 Contact with special interest groups

ISO27001.ACTRL	A.06.1.4 Contact with special interest groups
Size	101
Bookmark	-1

Incoming (1)

	ISO27001.AOBJ	A6.1 Internal organisation

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.1.5 Information security in project management

ISO27001.ACTRL	A.06.1.5 Information security in project management
Size	101
Bookmark	-1

Incoming (1)

	ISO27001.AOBJ	A6.1 Internal organisation

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.2.1 Mobile device policy

ISO27001.ACTRL	A.06.2.1 Mobile device policy
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A6.2 Mobile devices and teleworking

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.06.2.2 Teleworking

ISO27001.ACTRL	A.06.2.2 Teleworking
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A6.2 Mobile devices and teleworking

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.1.1 Screening

ISO27001.ACTRL	A.07.1.1 Screening
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.1 Prior to employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.1.2 Terms and conditions of employment

ISO27001.ACTRL	A.07.1.2 Terms and conditions of employment
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.1 Prior to employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.2.1 Management responsibilities

ISO27001.ACTRL	A.07.2.1 Management responsibilities
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.2 During employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.2.2 Information security awareness, education and training

ISO27001.ACTRL	A.07.2.2 Information security awareness, education and training
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.2 During employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.2.3 Disciplinary process

ISO27001.ACTRL	A.07.2.3 Disciplinary process
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.2 During employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.07.3.1 Termination or change of employment responsibilities

ISO27001.ACTRL	A.07.3.1 Termination or change of employment responsibilities
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A7.3 Termination and change of employment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.1.1 Inventory of assets

ISO27001.ACTRL	A.08.1.1 Inventory of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.1 Responsibility for assets

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.1.2 Ownership of assets

ISO27001.ACTRL	A.08.1.2 Ownership of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.1 Responsibility for assets

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.1.3 Acceptable use of assets

ISO27001.ACTRL	A.08.1.3 Acceptable use of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.1 Responsibility for assets

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.1.4 Return of assets

ISO27001.ACTRL	A.08.1.4 Return of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.1 Responsibility for assets

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.2.1 Classification of information

ISO27001.ACTRL	A.08.2.1 Classification of information
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.2 Information classification

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.2.2 Labelling of information

ISO27001.ACTRL	A.08.2.2 Labelling of information
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.2 Information classification

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.2.3 Handling of assets

ISO27001.ACTRL	A.08.2.3 Handling of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.2 Information classification

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.3.1 Management of removable media

ISO27001.ACTRL	A.08.3.1 Management of removable media
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A8.3 Media handling

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.3.2 Disposal of media

ISO27001.ACTRL	A.08.3.2 Disposal of media
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A8.3 Media handling

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.08.3.3 Physical media transfer

ISO27001.ACTRL	A.08.3.3 Physical media transfer
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A8.3 Media handling

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.1.1 Access control policy

ISO27001.ACTRL	A.09.1.1 Access control policy
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.1 Business requirements of access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.1.2 Access to networks and network services

ISO27001.ACTRL	A.09.1.2 Access to networks and network services
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.1 Business requirements of access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.1 User registration and de-registration

ISO27001.ACTRL	A.09.2.1 User registration and de-registration
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.2 User access provisioning

ISO27001.ACTRL	A.09.2.2 User access provisioning
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.3 Management of privileged access rights

ISO27001.ACTRL	A.09.2.3 Management of privileged access rights
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.4 Management of secret authentication information of users

ISO27001.ACTRL	A.09.2.4 Management of secret authentication information of users
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.5 Review of user access rights

ISO27001.ACTRL	A.09.2.5 Review of user access rights
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.2.6 Removal or adjustment of access rights

ISO27001.ACTRL	A.09.2.6 Removal or adjustment of access rights
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.2 User access management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.3.1 Use of secret authentication information

ISO27001.ACTRL	A.09.3.1 Use of secret authentication information
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.3 User responsibilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.4.1 Information access restriction

ISO27001.ACTRL	A.09.4.1 Information access restriction
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.4 System and application access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.4.2 Secure log-on procedures

ISO27001.ACTRL	A.09.4.2 Secure log-on procedures
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.4 System and application access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.4.3 Password management system

ISO27001.ACTRL	A.09.4.3 Password management system
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.4 System and application access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.4.4 Use of privileged utility programs

ISO27001.ACTRL	A.09.4.4 Use of privileged utility programs
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.4 System and application access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.09.4.5 Access control to program source code

ISO27001.ACTRL	A.09.4.5 Access control to program source code
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A9.4 System and application access control

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.10.1.1 Policy on the use of cryptographic controls

ISO27001.ACTRL	A.10.1.1 Policy on the use of cryptographic controls
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A10.1 Cryptographic controls

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.10.1.2 Key management

ISO27001.ACTRL	A.10.1.2 Key management
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A10.1 Cryptographic controls

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.1 Physical security perimeter

ISO27001.ACTRL	A.11.1.1 Physical security perimeter
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.2 Physical entry controls

ISO27001.ACTRL	A.11.1.2 Physical entry controls
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.3 Securing offices, rooms and facilities

ISO27001.ACTRL	A.11.1.3 Securing offices, rooms and facilities
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.4 Protecting against external and environmental threats

ISO27001.ACTRL	A.11.1.4 Protecting against external and environmental threats
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.5 Working in secure areas

ISO27001.ACTRL	A.11.1.5 Working in secure areas
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.1.6 Delivery and loading areas

ISO27001.ACTRL	A.11.1.6 Delivery and loading areas
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.1 Secure areas

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.1 Equipment siting and protection

ISO27001.ACTRL	A.11.2.1 Equipment siting and protection
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.2 Supporting utilities

ISO27001.ACTRL	A.11.2.2 Supporting utilities
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.3 Cabling security

ISO27001.ACTRL	A.11.2.3 Cabling security
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.4 Equipment maintenance

ISO27001.ACTRL	A.11.2.4 Equipment maintenance
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.5 Removal of assets

ISO27001.ACTRL	A.11.2.5 Removal of assets
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.6 Security of equipment and assets off-premises

ISO27001.ACTRL	A.11.2.6 Security of equipment and assets off-premises
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.7 Secure disposal or re-use of equipment

ISO27001.ACTRL	A.11.2.7 Secure disposal or re-use of equipment
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.8 Unattended user equipment

ISO27001.ACTRL	A.11.2.8 Unattended user equipment
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.11.2.9 Clear desk and clear screen policy

ISO27001.ACTRL	A.11.2.9 Clear desk and clear screen policy
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A11.2 Equipment

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.1.1 Documented operating procedures

ISO27001.ACTRL	A.12.1.1 Documented operating procedures
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A12.1 Operational procedures and responsibilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.1.2 Change management

ISO27001.ACTRL	A.12.1.2 Change management
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A12.1 Operational procedures and responsibilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.1.3 Capacity management

ISO27001.ACTRL	A.12.1.3 Capacity management
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A12.1 Operational procedures and responsibilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.1.4 Separation of development, testing and operational environments

ISO27001.ACTRL	A.12.1.4 Separation of development, testing and operational environments
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.1 Operational procedures and responsibilities

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.2.1 Controls against malware

ISO27001.ACTRL	A.12.2.1 Controls against malware
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.2 Protection from malware

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.3.1 Information backup

ISO27001.ACTRL	A.12.3.1 Information backup
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.3 Backup

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.4.1 Event logging

ISO27001.ACTRL	A.12.4.1 Event logging
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.4 Logging and monitoring

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.4.2 Protection of log information

ISO27001.ACTRL	A.12.4.2 Protection of log information
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.4 Logging and monitoring

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.4.3 Administrator and operator logs

ISO27001.ACTRL	A.12.4.3 Administrator and operator logs
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.4 Logging and monitoring

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.4.4 Clock synchronisation

ISO27001.ACTRL	A.12.4.4 Clock synchronisation
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.4 Logging and monitoring

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.5.1 Installation of software on operational systems

ISO27001.ACTRL	A.12.5.1 Installation of software on operational systems
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.5 Control of operational software

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.6.1 Management of technical vulnerabilities

ISO27001.ACTRL	A.12.6.1 Management of technical vulnerabilities
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.6 Technical vulnerability management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.6.2 Restrictions on software installation

ISO27001.ACTRL	A.12.6.2 Restrictions on software installation
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.6 Technical vulnerability management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.12.7.1 Information systems audit controls

ISO27001.ACTRL	A.12.7.1 Information systems audit controls
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A12.7 Information systems audit considerations

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.1.1 Network controls

ISO27001.ACTRL	A.13.1.1 Network controls
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A13.1 Network security management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.1.2 Security of network services

ISO27001.ACTRL	A.13.1.2 Security of network services
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.1 Network security management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.1.3 Segregation in networks

ISO27001.ACTRL	A.13.1.3 Segregation in networks
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.1 Network security management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.2.1 Information transfer policies and procedures

ISO27001.ACTRL	A.13.2.1 Information transfer policies and procedures
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.2 Information transfer

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.2.2 Agreements on information transfer

ISO27001.ACTRL	A.13.2.2 Agreements on information transfer
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.2 Information transfer

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.2.3 Electronic messaging

ISO27001.ACTRL	A.13.2.3 Electronic messaging
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.2 Information transfer

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.13.2.4 Confidentiality or non-disclosure agreements

ISO27001.ACTRL	A.13.2.4 Confidentiality or non-disclosure agreements
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A13.2 Information transfer

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.1.1 Information security requirements analysis and specification

ISO27001.ACTRL	A.14.1.1 Information security requirements analysis and specification
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.1 Security requirements of information systems

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.1.2 Securing application services on public networks

ISO27001.ACTRL	A.14.1.2 Securing application services on public networks
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.1 Security requirements of information systems

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.1.3 Protecting application services transactions

ISO27001.ACTRL	A.14.1.3 Protecting application services transactions
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A14.1 Security requirements of information systems

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.1 Secure development policy

ISO27001.ACTRL	A.14.2.1 Secure development policy
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.2 System change control procedures

ISO27001.ACTRL	A.14.2.2 System change control procedures
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.3 Technical review of applications after operating platform changes

ISO27001.ACTRL	A.14.2.3 Technical review of applications after operating platform changes
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.4 Restrictions on changes to software packages

ISO27001.ACTRL	A.14.2.4 Restrictions on changes to software packages
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.5 Secure system engineering principles

ISO27001.ACTRL	A.14.2.5 Secure system engineering principles
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.6 Secure development environment

ISO27001.ACTRL	A.14.2.6 Secure development environment
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.7 Outsourced development

ISO27001.ACTRL	A.14.2.7 Outsourced development
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.8 System security testing

ISO27001.ACTRL	A.14.2.8 System security testing
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.2.9 System acceptance testing

ISO27001.ACTRL	A.14.2.9 System acceptance testing
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.2 Security in development and support processes

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.14.3.1 Protection of test data

ISO27001.ACTRL	A.14.3.1 Protection of test data
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A14.3 Test data

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.15.1.1 Information security policy for supplier relationships

ISO27001.ACTRL	A.15.1.1 Information security policy for supplier relationships
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A15.1 Information security in supplier relationships

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.15.1.2 Addressing security within supplier agreements

ISO27001.ACTRL	A.15.1.2 Addressing security within supplier agreements
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A15.1 Information security in supplier relationships

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.15.1.3 Information and communication technology supply chain

ISO27001.ACTRL	A.15.1.3 Information and communication technology supply chain
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A15.1 Information security in supplier relationships

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.15.2.1 Monitoring and review of supplier services

ISO27001.ACTRL	A.15.2.1 Monitoring and review of supplier services
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A15.2 Supplier service delivery management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.15.2.2 Managing changes to supplier services

ISO27001.ACTRL	A.15.2.2 Managing changes to supplier services
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A15.2 Supplier service delivery management

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.1 Responsibilities and procedures

ISO27001.ACTRL	A.16.1.1 Responsibilities and procedures
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.2 Reporting information security events

ISO27001.ACTRL	A.16.1.2 Reporting information security events
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.3 Reporting information security weaknesses

ISO27001.ACTRL	A.16.1.3 Reporting information security weaknesses
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.4 Assessment of and decision on information security events

ISO27001.ACTRL	A.16.1.4 Assessment of and decision on information security events
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.5 Response to information security incidents

ISO27001.ACTRL	A.16.1.5 Response to information security incidents
Size	101
Bookmark	-1

Incoming (1)

♟	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.6 Learning from information security incidents

ISO27001.ACTRL	A.16.1.6 Learning from information security incidents
Size	101
Bookmark	-1

Incoming (1)

♟	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.16.1.7 Collection of evidence

ISO27001.ACTRL	A.16.1.7 Collection of evidence
Size	101
Bookmark	-1

Incoming (1)

♟	ISO27001.AOBJ	A16.1 Management of information security incidents and improvements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.17.1.1 Planning information security continuity

ISO27001.ACTRL	A.17.1.1 Planning information security continuity
Size	101
Bookmark	-1

Incoming (1)

♟	ISO27001.AOBJ	A17.1 Information security continuity

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.17.1.2 Implementing information security continuity

ISO27001.ACTRL	A.17.1.2 Implementing information security continuity
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A17.1 Information security continuity

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.17.1.3 Verify, review and evaluate information security continuity

ISO27001.ACTRL	A.17.1.3 Verify, review and evaluate information security continuity
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A17.1 Information security continuity

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.17.2.1 Availability of information processing facilities

ISO27001.ACTRL	A.17.2.1 Availability of information processing facilities
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A17.2 Redundancies

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.1.1 Identification of applicable legislation and contractual requirements

ISO27001.ACTRL	A.18.1.1 Identification of applicable legislation and contractual requirements
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.1.2 Intellectual property rights

ISO27001.ACTRL	A.18.1.2 Intellectual property rights
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.1.3 Protection of records

ISO27001.ACTRL	A.18.1.3 Protection of records
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.1.4 Privacy and protection of personally identifiable information

ISO27001.ACTRL	A.18.1.4 Privacy and protection of personally identifiable information
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.1.5 Regulation of cryptographic controls

ISO27001.ACTRL	A.18.1.5 Regulation of cryptographic controls
Size	101
Bookmark	-1

Incoming (1)

ISO27001.AOBJ	A18.1 Compliance with legal and contractual requirements

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.2.1 Independent review of information security

ISO27001.ACTRL	A.18.2.1 Independent review of information security
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A18.2 Information security reviews

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.2.2 Compliance with security policies and standards

ISO27001.ACTRL	A.18.2.2 Compliance with security policies and standards
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A18.2 Information security reviews

ISO27001.ACTRL

7FORTRESS.ISO27001.ACTRL

A.18.2.3 Technical compliance review

ISO27001.ACTRL	A.18.2.3 Technical compliance review
Size	101
Bookmark	-1

Incoming (1)

♜	ISO27001.AOBJ	A18.2 Information security reviews