

Physical Assets

Physical Assets - **(New)** Name: Value: 0 Owner: Location:
 Description: Sub-location:
 Comments: Type:
 Make: Model:
 Serial Number:

Related Assets

Software Assets	Information Assets	Paper Assets	Users \ Responsible	Legal Requirements
Name	Database Name	Description	Name	Legislation
*	*	*	*	*

Security Risks

ISO27001 Controls

Related Vulnerabilities	Related Threats	BS7999 Controls
Description	Description	Control N Status Comments
*	*	*

- Absence of personnel
- Complicated user interface
- Dial-up lines
- Disposal or reuse of storage media without proper erasure
- Inadequate network management
- Inadequate or careless use of physical protection for the building, do
- Inadequate recruitment procedures
- Insufficient maintenance/faulty installation of storage media
- Insufficient security training
- Lack of audit-trail
- Lack of care at disposal
- Lack of documentation
- Lack of effective change control
- Lack of identification and authentication mechanisms like user auth
- Lack of monitoring mechanisms

Navigation Pane

Physical Assets

Physical Assets - **(New)** Name: Value: 0 Owner: Location:

Description:

Comments:

Sub-location:

Type:

Make: Model:

Serial Number:

Related Assets

Software Assets	Information Assets	Paper Assets	Users \ Responsible	Legal Requirements
Name	Database Name	Description	Name	Legislation
*	*	*	*	*

Security Risks

ISO27001 Controls

Related Vulnerabilities	Related Threats	BS7999 Controls
Description	Description	Control N Status Comments
*	*	*
	Air conditioning failure	
	Airborne particles/dust	
	Bomb attack	
	Communications infiltration	
	Damage to communication lines/cables	
	Deterioration of storage media	
	Earthquake	
	Eavesdropping	
	Environmental contamination (and other forms of natural or m	
	Extremes of temperature and humidity	
	Failure of communications services	
	Failure of network components	
	Failure of power supply	
	Failure of water supply	
	Fire	

Navigation Pane

ISO27002:2005 Statement of Applicability

Control	Description	Content	App	Status	Statement of Applicability
5.1	INFORMATION SECURITY POLICY		<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
5.1.1	Information security policy document	An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
5.1.2	Review of the information security policy	The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	<input checked="" type="checkbox"/>	Partially Implemented	See Security Policy Document
6	ORGANISATION OF INFORMATION SECURITY		<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1	INTERNAL ORGANISATION		<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1.1	Management commitment to information security	Management should actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1.2	Information security co-ordination	Information security activities should be co-ordinated by representatives from different parts of the organisation with relevant roles and job functions.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1.3	Allocation of information security responsibilities	All information security responsibilities should be clearly defined.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1.4	Authorisation process for information security responsibilities	A management authorisation process for new information processing should be defined and implemented.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document
6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified and regularly reviewed.	<input type="checkbox"/>		
6.1.6	Contact with authorities	Appropriate contact with relevant authorities should be maintained.	<input type="checkbox"/>		
6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialists security forums and professional associations should be maintained.	<input type="checkbox"/>		
6.1.8	Information security training	Information security training should be provided to all employees and relevant external parties.	<input checked="" type="checkbox"/>	Fully Implemented	See Security Policy Document

Navigation Pane

Navigation Pane

ISO27002:2005 Risk Assessment

Physical Asset 250 E-Mail Server

Security Risk: 6

Value 4

Offsite Backup and Mail Exchange Hosted Mailboxes using Enta DSL. Xeon Processor, Intel Server Board, 2Gb RAM, 2 x 80Gb Disks RAID1, 2 x 500Gb Disks RAID 1. IP Address 10.10.100.1

Computer Users

Stored Paper Assets

Installed Software Assets

Installed Information Assets

ID 93742412
Value 1
Name Windows 2008 Server

ID 93742415
Value 2
Name Exchange Server 2007

ID 93742403
Value 1
Name Symantec Anti-Virus Corporate V10

Vulnerabilities

Threats

Susceptibility of equipment to voltage variations
Single point of failure

Failure of power supply

Hardware failure

Failure of network components

Lack of effective change control

Software failure

Uncontrolled downloading and using software

Malicious software (e.g. viruses, worms, Trojan Hc

Network access by unauthorised persons