WELCOME

ISO/IEC 27001:2017 Information Briefing

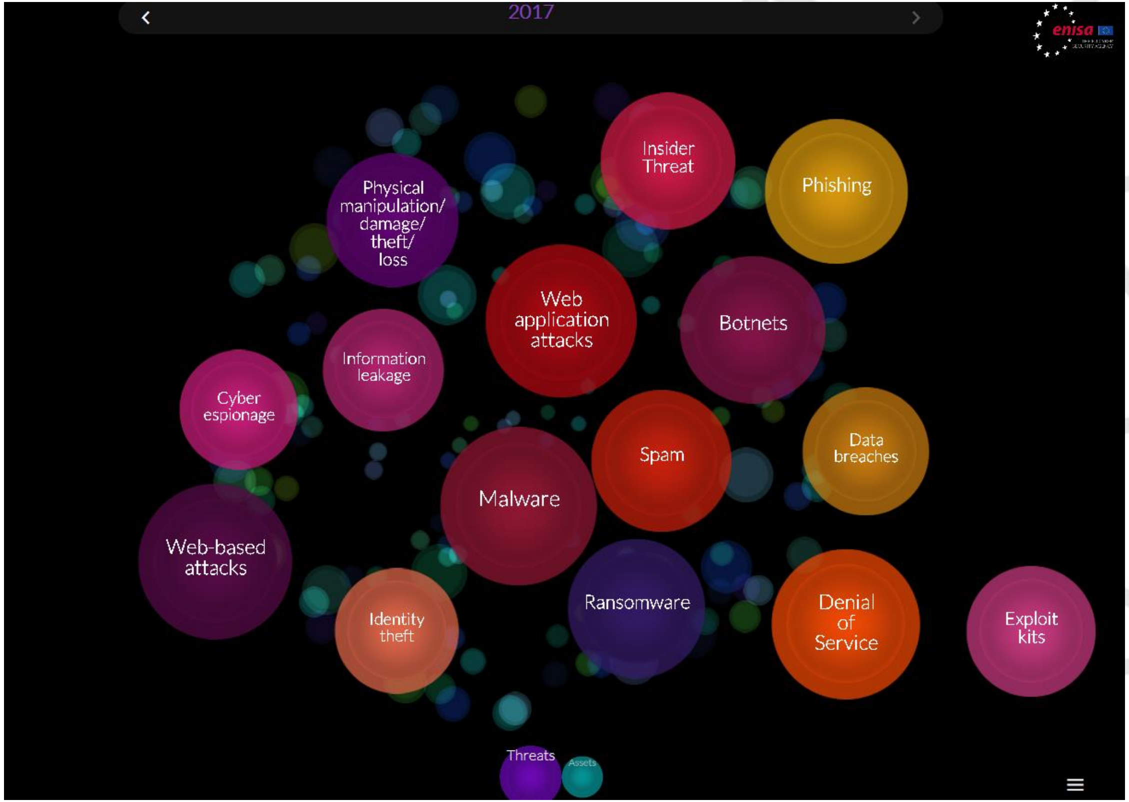
Denis Ryan
C.I.S.S.P
NSAI Lead Auditor

NSAI

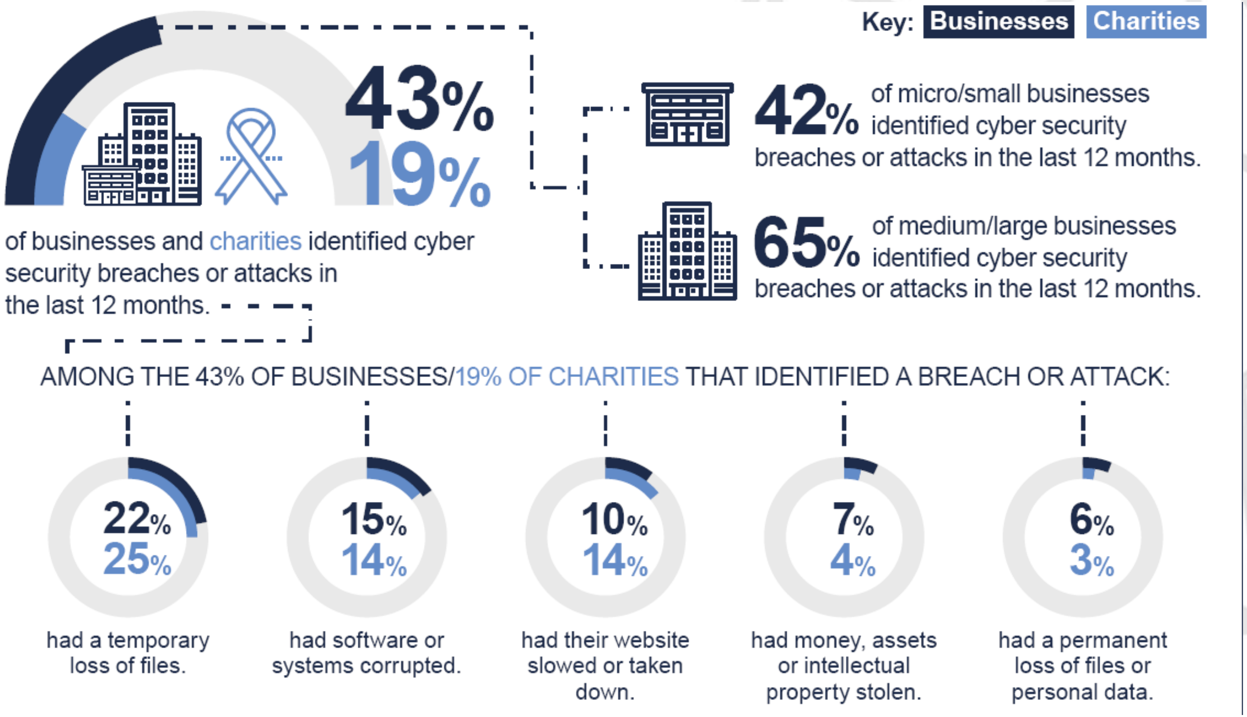
Running Order

1. Market survey
2. Why ISO 27001
3. Requirements of ISO 27001
4. Annex A
5. Registration process
6. Questions – discussion

ENISA profile



Survey UK Department for Digital, Culture, Media 2018



Key: Businesses Charities

43% 19% of businesses and charities identified cyber security breaches or attacks in the last 12 months.

42% of micro/small businesses identified cyber security breaches or attacks in the last 12 months.

65% of medium/large businesses identified cyber security breaches or attacks in the last 12 months.

AMONG THE 43% OF BUSINESSES/19% OF CHARITIES THAT IDENTIFIED A BREACH OR ATTACK:

22% 25% had a temporary loss of files.

15% 14% had software or systems corrupted.

10% 14% had their website slowed or taken down.

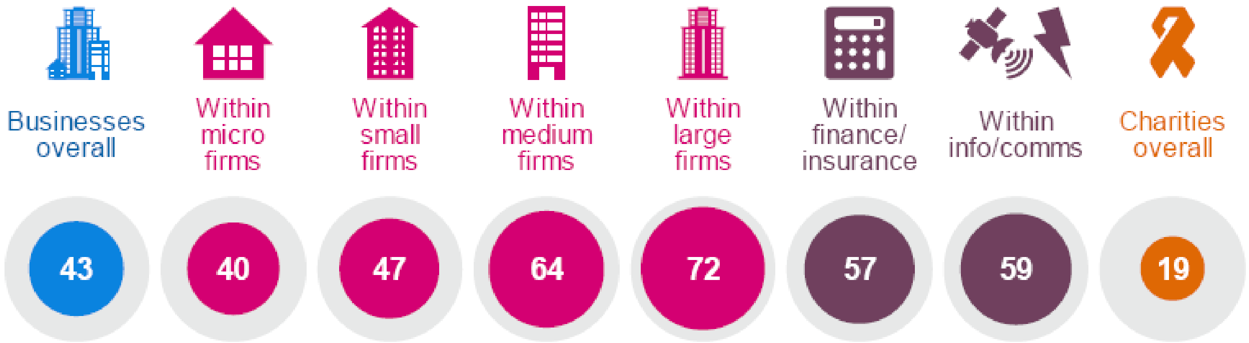
7% 4% had money, assets or intellectual property stolen.

6% 3% had a permanent loss of files or personal data.

Survey published May 2018

Figure 5.1: Proportion of organisations that have identified breaches or attacks in the last 12 months

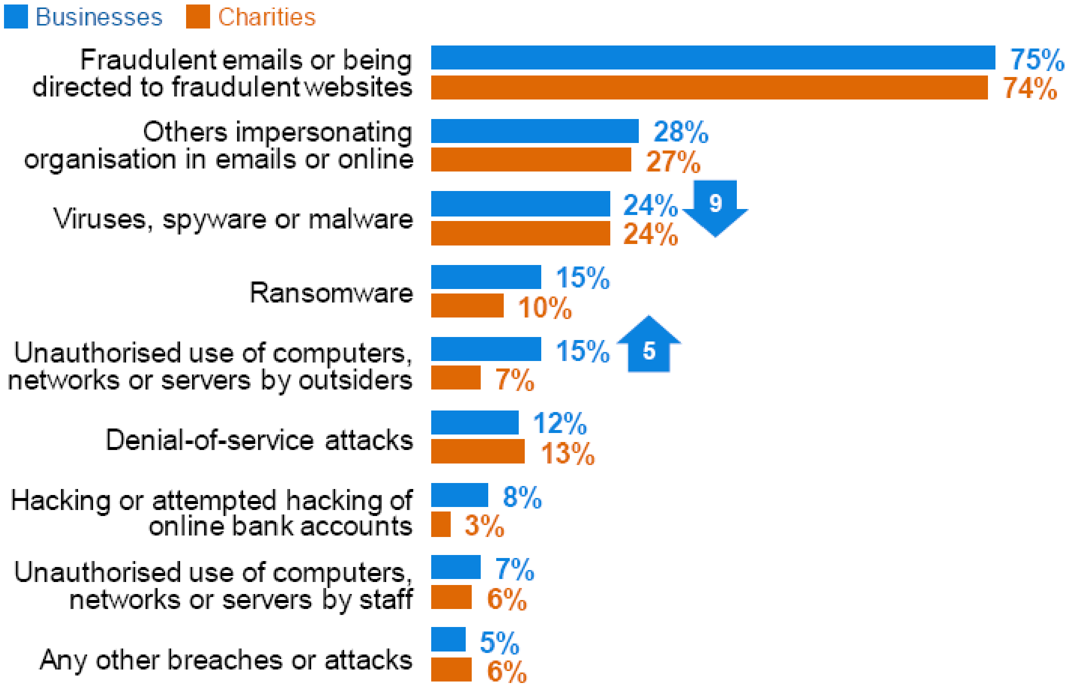
% experiencing a cyber security breach or attack in last 12 months



Bases: 1,519 UK businesses; 655 micro firms; 349 small firms; 263 medium firms; 252 large firms; 105 finance or insurance firms; 99 information or communications firms; 569 charities

Survey

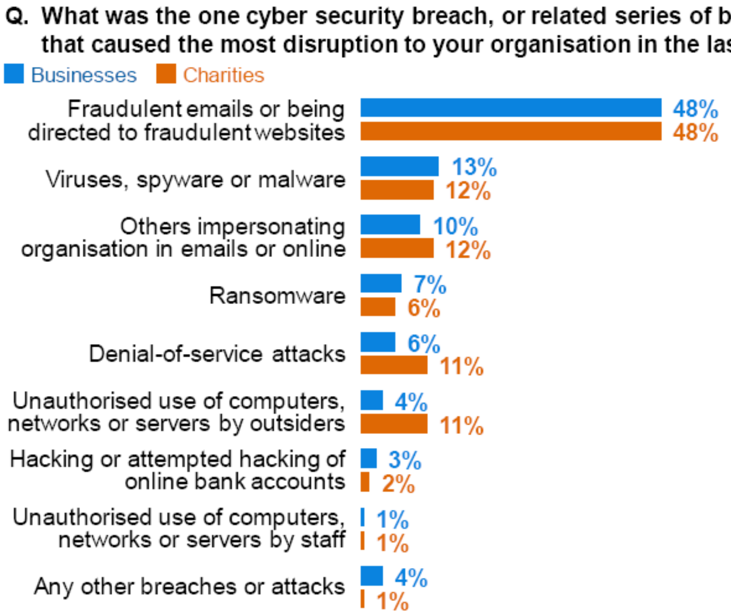
Q. Have any of the following happened to your organisation in the last 12 months?



Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

Survey

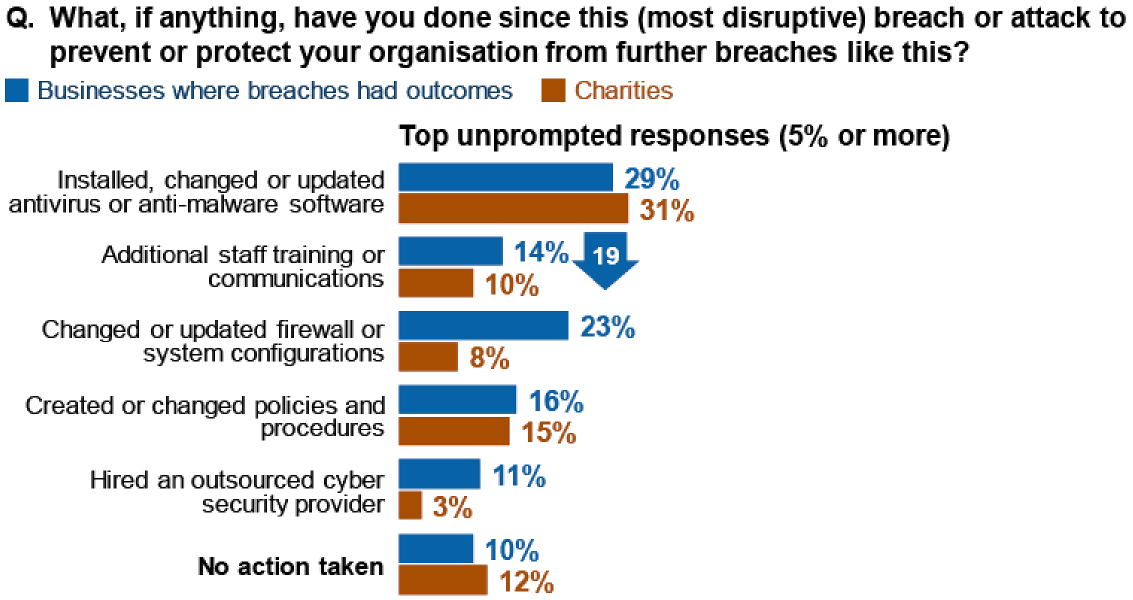
Figure 5.3: The single most disruptive breach suffered among the organisations that have identified breaches



Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

Survey

Figure 6.6: Most common actions following the most disruptive breach of the last 12 months, where breaches had material outcomes

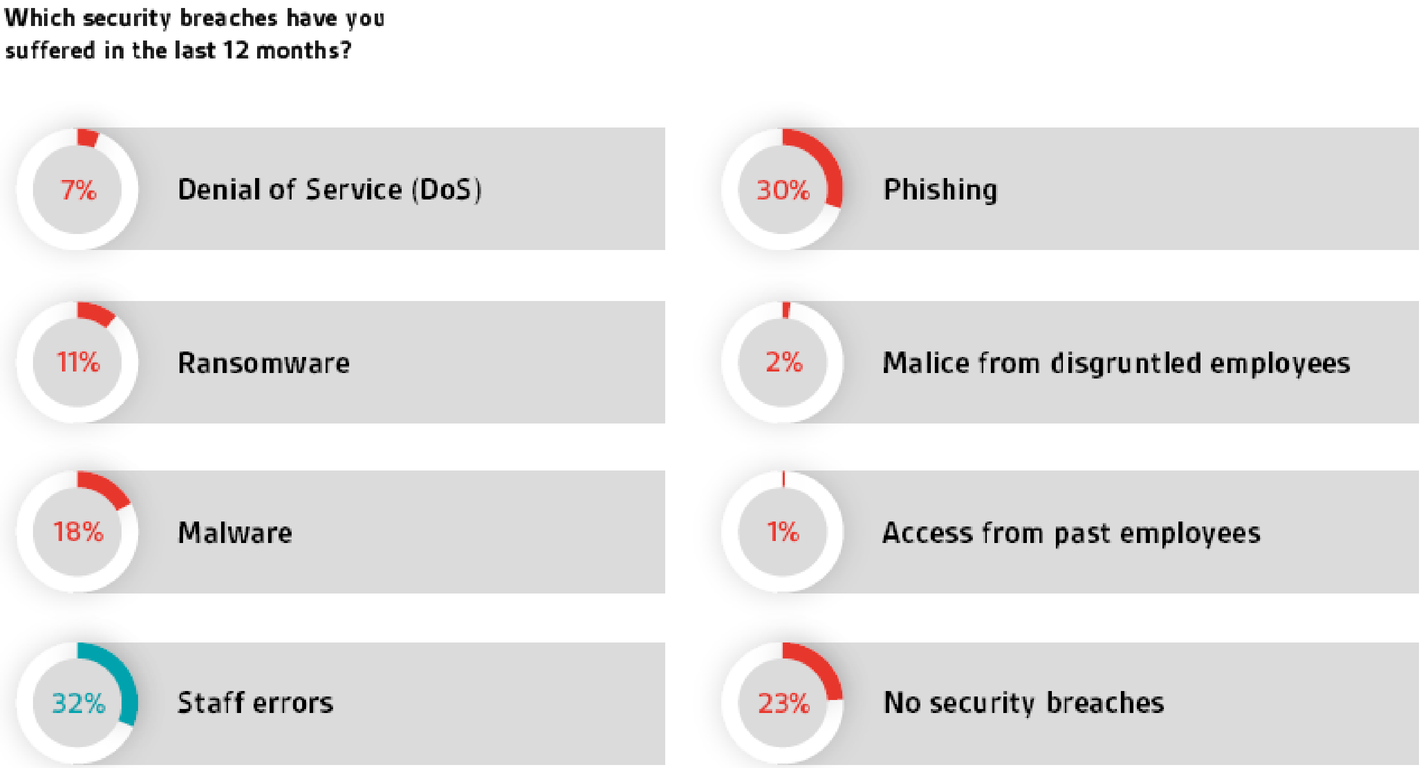


Q. What, if anything, have you done since this (most disruptive) breach or attack to prevent or protect your organisation from further breaches like this?

Bases: 287 businesses that identified a breach or attack with an outcome in the last 12 months; 87 charities

Public service

Survey bsi 2018 (745 org)



Which security breaches have you suffered in the last 12 months?

7%	Denial of Service (DoS)
11%	Ransomware
18%	Malware
32%	Staff errors
30%	Phishing
2%	Malice from disgruntled employees
1%	Access from past employees
23%	No security breaches

Information Security Management Systems

- Framework to protect information such as financial data, intellectual property, sensitive customer information, data, IT.
- Identify risks and implement security measures.
- Continuous review and improvement.

Benefits of implementing ISO 27001

1. Compliance

- reputational damage caused by ineffective security.
- Compliance with legislation and stakeholder need and expectations.
- Enables secure exchange of information.

Benefits of Implementing ISO 27001

2. Marketing

- win new business and retain existing clients.
- increased credibility when tendering for contracts.
- expand into new markets.
- demonstrates best practice.

Benefits of Implementing ISO 27001

3. Structure your business

- define responsibilities.
- improved management process and risk strategy.

4. GDPR - EU Data protection regulation

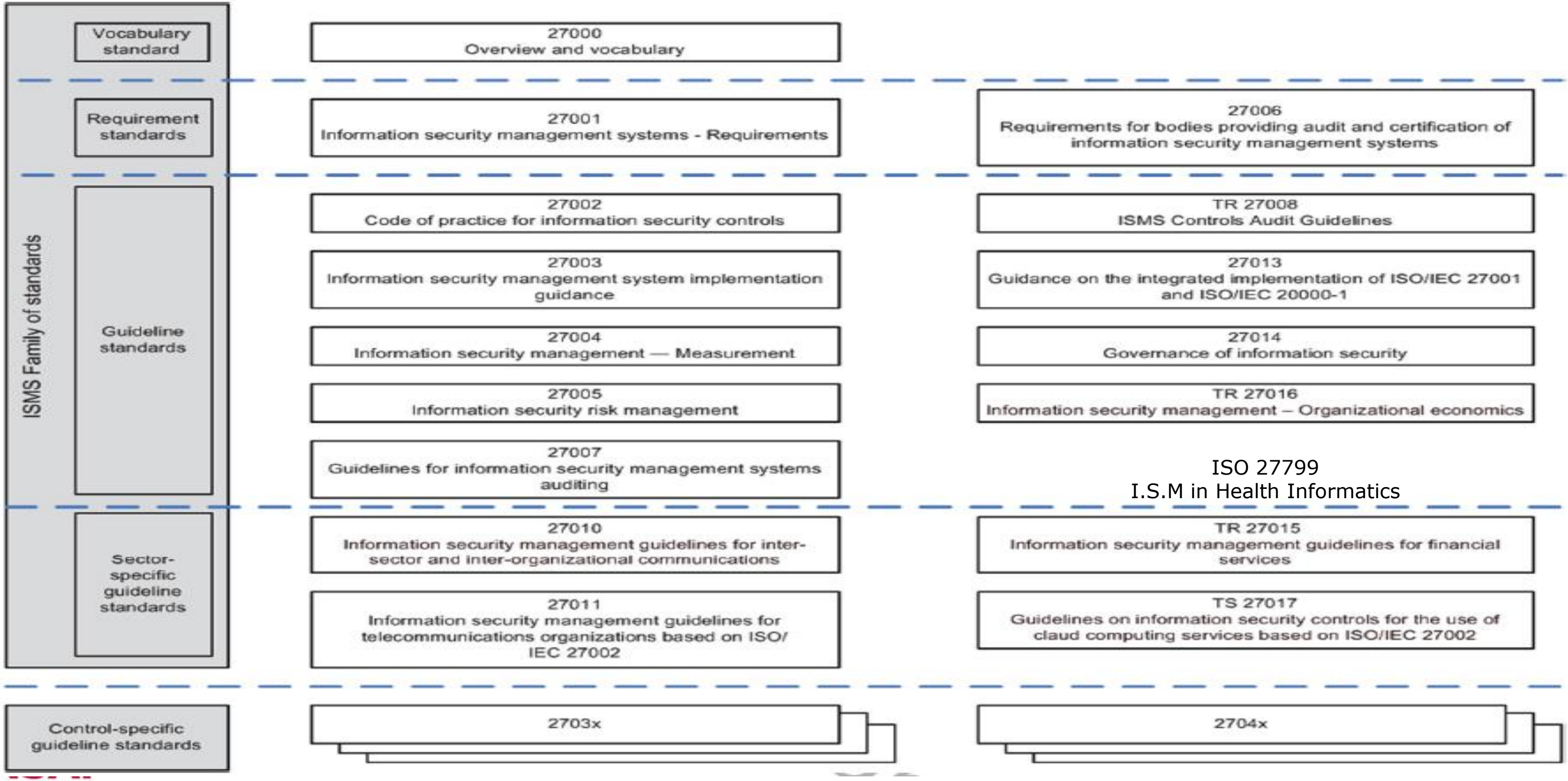
ISO 27001 support of GDPR

- Risk assessment
- Compliance
- Data classification/documentation
- Incident mgmt./breach notification
- Asset management
- Privacy by design
- Supplier relationships

NIS Directive

- EU wide legislation on Cybersecurity.
- National Law May 2018 (transposition in progress)
- Id operator of essential services, Nov 2018
- CSIR response team

ISO 27000 Family structure



ISMS Family of standards

Vocabulary standard	27000 Overview and vocabulary	
Requirement standards	27001 Information security management systems - Requirements	27006 Requirements for bodies providing audit and certification of information security management systems
Guideline standards	27002 Code of practice for information security controls	TR 27008 ISMS Controls Audit Guidelines
	27003 Information security management system implementation guidance	27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
	27004 Information security management — Measurement	27014 Governance of information security
	27005 Information security risk management	TR 27016 Information security management – Organizational economics
	27007 Guidelines for information security management systems auditing	ISO 27799 I.S.M in Health Informatics
Sector-specific guideline standards	27010 Information security management guidelines for inter-sector and inter-organizational communications	TR 27015 Information security management guidelines for financial services
	27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	TS 27017 Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002
Control-specific guideline standards	2703x	2704x

Structure of ISO 27001

- ISO 27001 requirements
  - Annex A
    - 14 security categories
    - 114 mandatory controls

Structure of ISO 27001

4 Context

Interested parties, scope.

5 Leadership.

Commitment, Policy, roles, responsibilities, authority.

6 Planning

- Risks assessment, Risk treatment plans, SOA, Objectives and plans

7 Support

- Resources, Competence, Awareness, Communication, Documented information

Structure of ISO 27001

8 Operation

- Planning and control, risk assessment, risk treatment

9 Performance evaluation

- Monitoring, Internal audit, mgmt. review

10 Improvement

- NC and Corrective action, Continual improvement

Annex A Requirements

A5 Information Security Policies

review of policies

A6 Organisation of IS

Internal organisation- roles and responsibilities
Segregation of duties
Contact with authorities
Contact with special interest groups
I.S in .Project mgmt,
Mobile devices
Policy
Teleworking security measures.

Annex A

A7 Human resource security

Screening

Terms and conditions

Responsibilities of employees and contractors

I.S awareness, education and training

Disciplinary process

Termination or change of employment

Annex A (cont’d)

A8 Asset management

Inventory of assets
Ownership of assets
Acceptable use of assets
Return of assets
Information classification
Labelling of information
Handling of assets
Management of removable media
Disposal of media
Physical media transfer

Annex A (cont’d)

A9 Access control

Access control policy

Access to networks and services

User registration and de-registration

User access provisioning

Management of privileged access rights

Management of secret authentication

Review of user access rights

Removal or adjustment of access rights

Annex A cont'd

A9 **Access control (cont'd)**

use of secret authentication information

System and application

Information access restriction

secure log in procedures

Password management system

use of privileged utility programs

access control to program source code

Annex A (cont'd)

A10 Cryptography

Policy

Key management

Annex A (cont'd)

A11 Physical and Environmental

Physical security

Physical entry controls

Securing offices, rooms, facilities

Protecting against external and environmental threats

Working in secure areas

Delivery and loading areas

Equipment siting and protection

Supporting utilities

Annex A (cont'd)

A11 Physical and Environmental (cont'd)

Cabling security

Equipment maintenance

Removal of assets

Security of equipment and assets off premises

Secure disposal or reuse of equipment

Unattended user equipment

Clear desk and clear screen policy

Annex A (cont'd)

A12 Operations Security

Procedures and responsibilities
Change management
Capacity management
Development, testing, operational environments
Protection from malware
Backup
Logging and monitoring
Event log review
Admin and operator logs
Control of operational software
Technical vulnerability
Restrictions on software installations

Annex A (cont’d)

A13 Communications security

Network security management

Network controls

Security of network services

Segregation in networks

Information transfer policies and procedures

Agreements on information transfer

Electronic messaging

NDA

Annex A (cont'd)

A14 **System Acquisition Dev and Maintenance**

IS in requirements analysis and specification
Securing application services on public network
Protecting Application services transactions
Secure development policy
System change control
Technical review of applications after operating platform changes
Secure system engineering principals
Secure development environment
Outsourced development
System security development
System acceptance testing
Test data

Annex A (cont'd)

A15 Supplier relationships

IS policy for supplier relationships

Security within supplier agreements

Information and communication technology within supply chain

Monitor and review of supplier services

Managing changes to supplier services

Supplier service delivery management

Annex A (cont’d)

A16 IS Incident Management.

responsibility and procedures

reporting I.S events

reporting I.S weaknesses

assessment of and decision on I.S events

response to I.S events

learning from I.S events

collection of evidence

Annex A (cont’d)

A17 Business Continuity Management

Planning I.S continuity

Implementing I.S continuity

Verify, review, evaluate I.S continuity

Availability of info processing facilities (redundancy)

Annex A (cont'd)

A18 Compliance

Id of applicable and contractual requirements

Intellectual property rights

Protection of records

Privacy and protection of P.I.I

Regulation of cryptographic controls

Independent review of I.S security

Managers review of f compliance in their area

Technical compliance review

Standard structure

NSAI Website

Self Assessment Checklist

Information in the Cloud

- **ISO 27017**

  Code of practice for information security controls for cloud services.

- **ISO 27018**

  Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO 27001 registration process

1. Familiarise yourself with the requirements of ISO 27001

2. Conduct a self assessment; download self assessment questionnaire from the NSAI website (ISO 27001 webpage)

ISO 27001 registration process

3. Follow system implementation methodology

- ISO 27002 code of practice
- ISO 27003 implementation guidance
- check industry guidance

ISO 27001 registration process

4. Apply for certification
   - Download, complete and return RFQ
   - Sign and return quotation
5. Agree Phase 1 and Phase 2 dates with Lead Auditor
6. Conduct certification audit
7. Certification decision

Resilient Organisation

- Quality (ISO 9001)
- Information Security (ISO 27001)
- Health and Safety (ISO 45001)
- Environment (ISO 14001)

Lets do business!

Thank you.

WWW.NSAI.IE

certification@nsai.ie

Search "NSAI"