

Advances in International Information Security Standards

Mr. Dale Johnstone

Member ISO

Information Security Committee

JTC 1 / SC 27 / WG 1

Chairman ISMS

International User Group

Hong Kong & Macau Chapter

Principal Consultant

Risk Management & Compliance

PCCW Limited

- **In the Beginning**
- **Move to ISO**
- **Evolution within ISO**
- **What to Expect (2005)**
- **Financial Sector**
- **ISMS Road Map (Future)**

In the Beginning



BS 7799-1

1995



ISMS

BS 7799-1 Published as a UK Standard



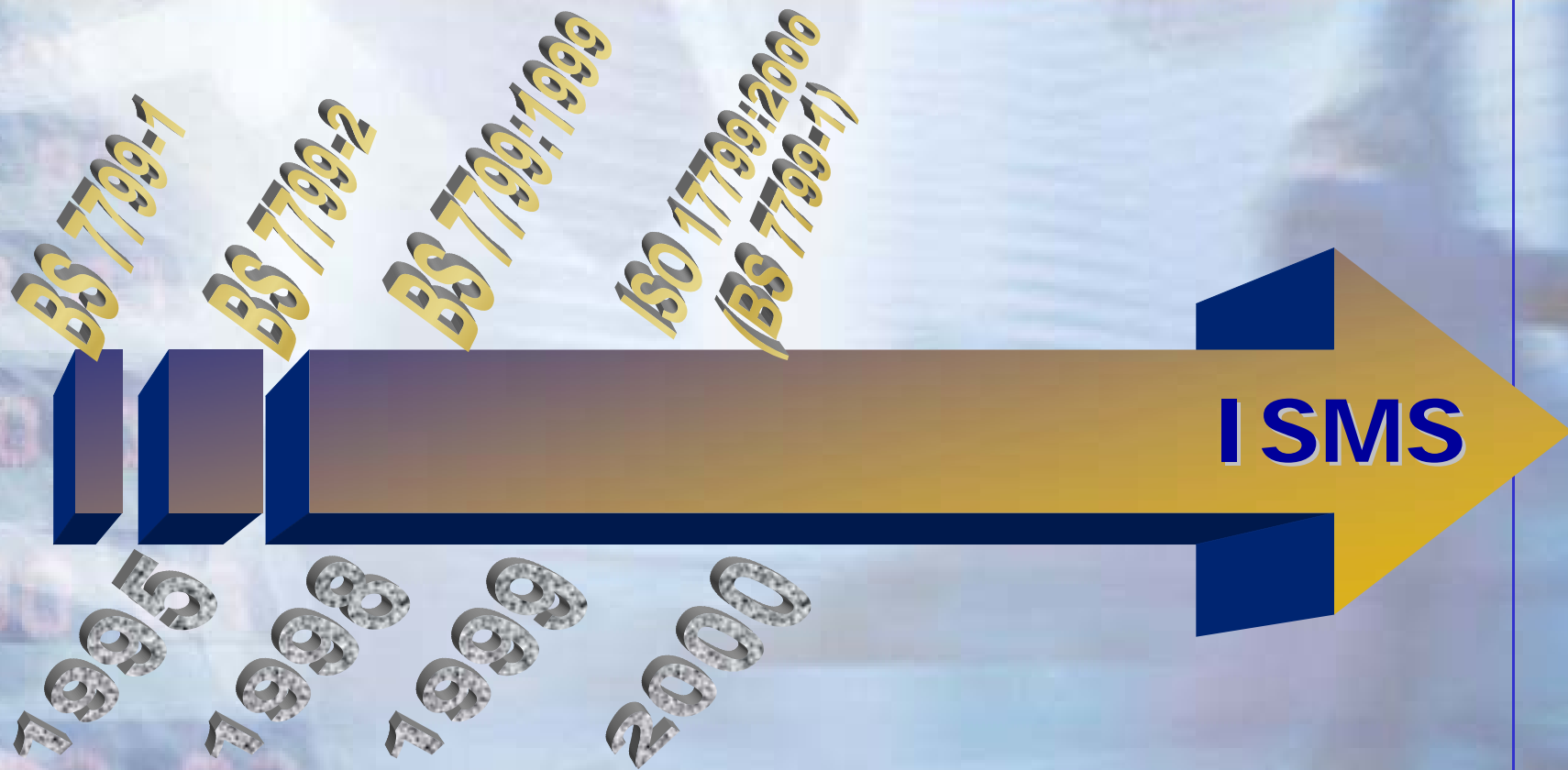
Need for an Information Security
Management System Identified
BS7799-2 - Published



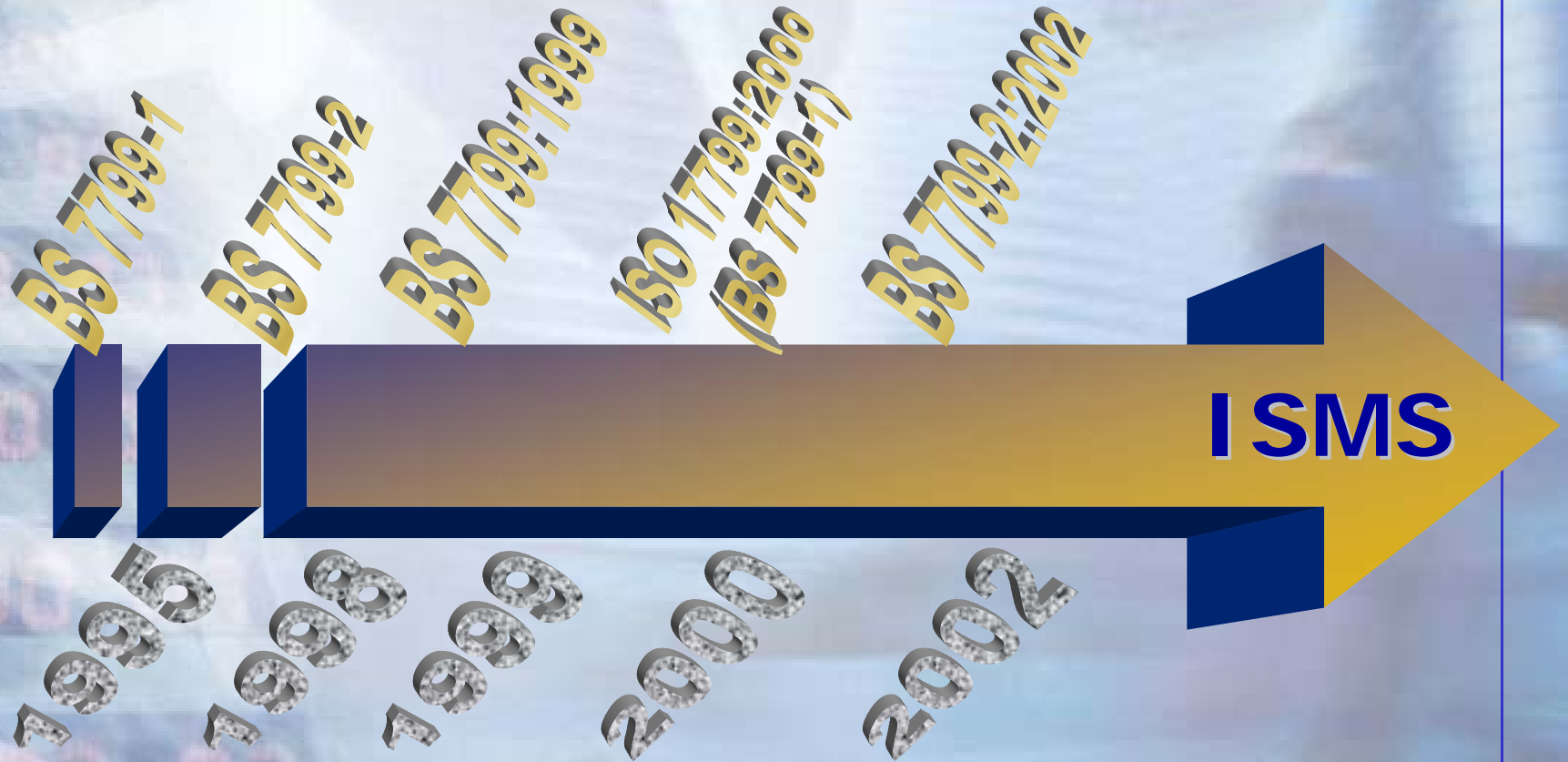
BS7799-1 Updated to be Non-UK Centric &
Republished

Move to ISO





Growing International Interest – BS7799-1
sent to ISO International Standard
Committee



BS7799-2 – Updated & Reissued to align
with ISO 9000 PDCA Model / ISO 17799
Controls

Evolution within ISO



Evolution within ISO (ISO 17799)

December 2000	ISO 17799 Published – 75.4% Approval Vote	
April 2001	Due to Close Vote – Irregular Step taken to <u>Immediately Commence</u> Review	
October 2001	150 Pages of Comments Received	
April 2002	100 Pages of Comments Received	
October 2002	162 Pages of Comments Received	
April 2003	210 Pages of Comments Received	
October 2003	202 Pages of Comments Received	
April 2004	202 Pages of Comments Received	
October 2004	64 Pages of Comments Received	

Evolution within ISO (BS7799-2)

**October
2002**

Call for Interest – Justification Study

**April
2003**

Study Period Commenced – BS7799-2 Submitted

**October
2003**

44 Pages of Comments Received

**April
2004**

40 Pages of Comments Received

**October
2004**

**New Work Item Proposal Commenced
63 Pages of Comments Received**

**April
2005**

**61 Pages of Comments Received
Approval Received to Proceed to FCD**

What to Expect (2005)



ISO 17799

May/June

100% Approval Vote Received

Off to Publishers

ISO 17799

May/June

100% Approval Vote Received

Off to Publishers

BS 7799-2

November/
December

??% Approval Vote Received

Off to Publishers

ISO 17799

100% Approval Vote Received

May/June

Off to Publishers

ISO 27001

??% Approval Vote Received

**November/
December**

Off to Publishers

ISMS Road Map (Future)



- **Code of practice for information security management**
 - ISO 17799
 - 2007 = ISO 27002?

Has obtained unanimous approval from all countries throughout the world involved in ISO Information Security Committee

Maintaining the greatest influence over all information security management standards

- **ISMS – Requirements (BS7799-2)**

Has obtained majority support to proceed to final drafting stage

**To better enable companies demonstrate compliance with legislative requirements
ISO 27001 certification is expected to grow significantly in 2006/2007**

- **ISMS – Implementation Guidelines** (in-progress)

Setting up and managing an ISMS requires the same approach as for any other management system

Observing a continuous cycle designed to ensure organizational best practices are documented, reinforced & improved over time

- **ISMS – Measurements & Metrics** (in-progress)

Define implementation objectives, effectiveness & efficiency criteria, tracking & measuring evolution, assist in benchmarking tools

Analyse information in objective manner, based on facts/real values

Use analytical information as a means to improve ISMS

As part of continuous improvement using metrics & measurements to allow an objective comparison of achieved information security:

1. Over a period of time;
2. between different parts of an organisation; and/ or
3. between organisations.

- **Code of practice for information security management**
- **ISMS – Requirements** (in-progress)
- **ISMS – Implementation Guidelines** (in-progress)
- **ISMS – Measurements & Metrics** (in-progress)

- **ISMS – Concepts & Models** (Under consideration)
- **ISMS – Fundamentals and vocabulary** (Conceptual)
- **ISMS – Monitoring & Review** (Conceptual)
- **ISMS – Auditing** (Conceptual)

ISO 17799 (2005)



11 Security Categories (Chapters)

36 Control Objectives (Level 2 Headings)

133 Controls (Level 3 Headings)

3 Security policy

3.1 Information security policy

Objective: To provide management direction and support for information security.

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

3.1.1 Information security policy document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. As a minimum, the following guidance should be included:

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);
- b) a statement of management intent, supporting the goals and principles of information security;
- c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:
 - 1) compliance with legislative and contractual requirements;
 - 2) security education requirements;
 - 3) prevention and detection of viruses and other malicious software;
 - 4) business continuity management;
 - 5) consequences of security policy violations;
- d) a definition of general and specific responsibilities for information security management, including reporting security incidents;
- e) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);
- b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - 1) compliance with legislative, regulatory, and contractual requirements;
 - 2) security education, training, and awareness requirements;
 - 3) business continuity management;
 - 4) consequences of information security policy violations;
- e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC IS 13335-1:2004.

Clause 5.1

	2000	2005	%
Paragraphs	• 19	• 23	• 21.05
Lines	• 36	• 51	• 41.67
Words	• 251	• 343	• 36.65
Characters	• 1592	• 2202	• 38.32
Characters +spaces	• 1824	• 2528	• 38.60

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);
- b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - 1) compliance with legislative, regulatory, and contractual requirements;
 - 2) security education, training, and awareness requirements;
 - 3) business continuity management;
 - 4) consequences of information security policy violations;
- e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC IS 13335-1:2004.

5 Chapter Title (Security Category)

5.1 Control Objective

5.1.1 Control

Defines specific control statement to satisfy control objective

Implementation guidance

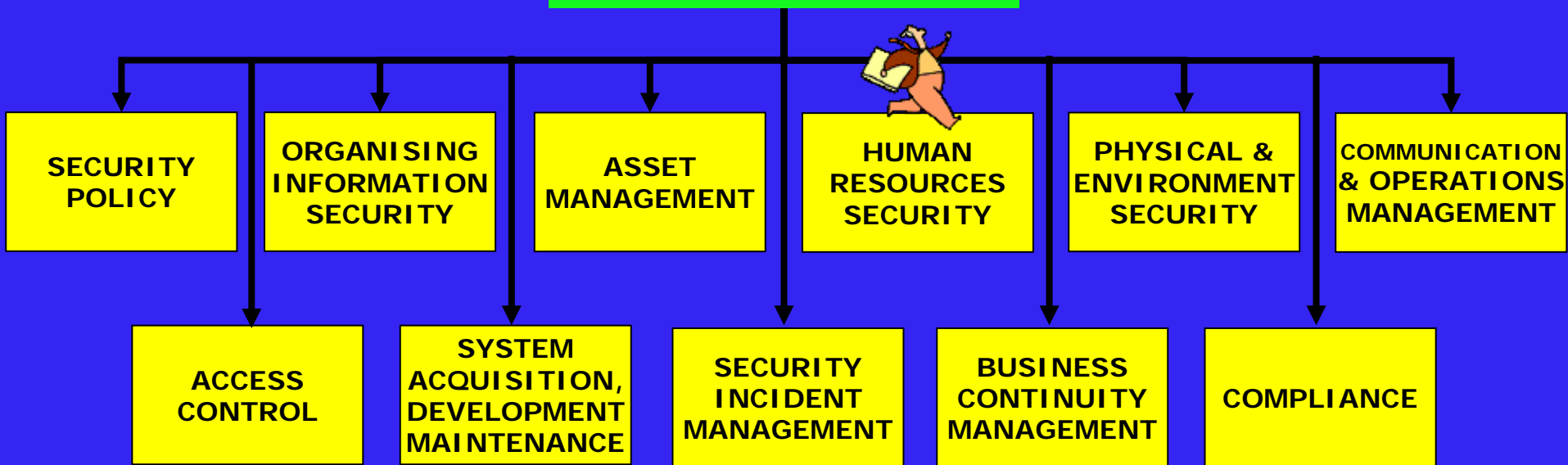
Provides more detailed information supporting implementation of the control and meeting the control objective. Some guidance may not be suitable therefore other ways of implementing control may be more appropriate

Other information

Provides further information to be considered, for example legal considerations and references to other standards

Security Categories (Chapters)

ISO 17799 2005



**ISO 17799
2005**

**SECURITY
POLICY**

INFORMATION SECURITY POLICY (1)

**ISO 17799
2005**

**ORGANISING
INFORMATION
SECURITY**

INTERNAL ORGANIZATION (2)

EXTERNAL PARTIES (3)

**ISO 17799
2005**

**ASSET
MANAGEMENT**

RESPONSIBILITY FOR ASSETS (4)

INFORMATION CLASSIFICATION (5)

**ISO 17799
2005**

**HUMAN
RESOURCES
SECURITY**

PRIOR TO EMPLOYMENT (6)

DURING EMPLOYMENT (7)

**TERMINATION OR CHANGE
OF EMPLOYMENT (8)**

Control Objectives (Level 2)

**ISO 17799
2005**

**PHYSICAL &
ENVIRONMENT
SECURITY**

SECURE AREAS (9)

EQUIPMENT SECURITY (10)

ISO 17799 2005

OPERATIONAL PROCEDURES AND
RESPONSIBILITIES (11)

THIRD PARTY SERVICE DELIVERY
MANAGEMENT (12)

SYSTEM PLANNING AND
ACCEPTANCE (13)

PROTECTION AGAINST MALICIOUS
AND MOBILE CODE (14)

BACK-UP (15)

NETWORK SECURITY
MANAGEMENT (16)

MEDIA HANDLING
(17)

EXCHANGE OF INFORMATION
(18)

ELECTRONIC COMMERCE
SERVICES (19)

MONITORING (20)

COMMUNICATION
& OPERATIONS
MANAGEMENT

ISO 17799 2005

BUSINESS REQUIREMENT FOR ACCESS CONTROL (21)

USER ACCESS MANAGEMENT (22)

USER RESPONSIBILITIES (23)

NETWORK ACCESS CONTROL (24)

ACCESS
CONTROL

OPERATING SYSTEM ACCESS CONTROL (25)

APPLICATION & INFORMATION ACCESS CONTROL (26)

MOBILE COMPUTING AND TELEWORKING (27)

Control Objectives (Level 2)

ISO 17799 2005

SECURITY REQUIREMENTS OF
INFORMATION SYSTEMS (28)

CORRECT PROCESSING IN
APPLICATIONS (29)

SYSTEM
ACQUISITION,
DEVELOPMENT
MAINTENANCE

CRYPTOGRAPHIC CONTROLS (30)

SECURITY OF SYSTEM FILES (31)

SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES (32)

TECHNICAL VULNERABILITY MANAGEMENT (33)

**ISO 17799
2005**

**SECURITY
INCIDENT
MANAGEMENT**

**REPORTING INFORMATION SECURITY EVENTS AND
WEAKNESSES (34)**

**MANAGEMENT OF INFORMATION SECURITY INCIDENTS
AND IMPROVEMENTS (35)**

**ISO 17799
2005**

**BUSINESS
CONTINUITY
MANAGEMENT**

**INFORMATION SECURITY ASPECTS OF BUSINESS
CONTINUITY MANAGEMENT (36)**

ISO 17799 2005

COMPLIANCE WITH LEGAL
REQUIREMENTS (37)

COMPLIANCE WITH SECURITY POLICIES
AND STANDARDS AND TECHNICAL
COMPLIANCE (38)

INFORMATION SYSTEMS AUDIT
CONSIDERATIONS (39)



COMPLIANCE

ISO 17799: 2005 (Summary)

Clause	Security Category	Objectives	Controls	v2000	
1	Scope	-	-	-	
2	Terms and Definitions	-	-	-	
3	Structure of the Standard	-	-	-	
4	Risk Assessment and Treatment	-	-	-	
5	Security Policy	1	2	1 – 2	Nil
6	Organising Information Security	2	11	3 – 10	-1 / +1
7	Asset Management	2	5	2 – 3	0 / +2
8	Human Resources Security	3	9	3 – 10	0 / +1
9	Physical and environmental Security	2	13	3 – 13	+1 / 0
10	Communications and Operations Management	10	32	7 – 24	+3 / +8
11	Access Control	7	25	8 – 31	-1 / -6
12	Information Systems Acquisition, Development and Maintenance	6	16	5 – 18	+1 / +2
13	Information Security Incident Management	2	5	0 – 0	+2 / +5
14	Business Continuity Management	1	5	1 – 5	Nil
15	Compliance	3	10	3 – 11	0 / -1
Total		39{36}	133{127}		+3 / +6

Advances in International Information Security Standards

Mr. Dale Johnstone

dale.johnstone@pccw.com

