ISMS 資訊安全管理系統

ISO 17799:2005 & BS 7799-2:2005 新版(草案)介紹

Peter Pu (蒲樹盛), BSi 英國標準協會
- BSI Pacific Regional Training Manager
BS7799 Lead Auditor
Peter.pu@bsi-taiwan.com

全球最權威之專業驗證機構-國際標準制定機構

- 1901- 全球第一個國際性標準組織
- 1926- 全球第一國際性產品認證標章
- 1929- 英國皇家特許機構
- 1948- 國際驗證標準組織(ISO)創始會員
- 1979- BS 5750正式公告(ISO 組織引用為9000)
- 1992- BS 7750正式公告(ISO組織引用為14001)
- 1999- BSi正式公告OHSAS 18001
- **1999- BSi正式公告BS 7799 (ISO 組織引用為17799)**
- 2003- BSi正式公告BS 15000
- **首家取得TAF(台灣認證基金會）認可之CNS 17800驗證機構**

BSI 稽核員對標準解讀一致性全球最高

BSI
We shape the future

全球最權威之專業驗證機構

英國標準協會(BSi -British Standards Institution)

1. BSi全球分公司遍及歐洲大陸、美國、台灣、香港、中國、新加坡、加拿大、墨西哥及南美洲等90餘國，總計約4,500多位員工為全球各型企業服務。

2. **驗證市場佔有率全球之首:** BSi全世界發出的ISO 9000與ISO 14001證書約6萬張，驗證經驗及服務範圍涵蓋各行各業。

3.BSi在**BS7799**資訊安全管理系統之驗證專業及權威性已獲全球肯定，**發證量全球第一，台灣地區更高達七成以上之資訊安全證書均以BSi為驗證首選！**

4.BSi為台灣地區第一家通過TAF(Taiwan Accreditation Foundation) BS7799-2:2002認證之驗證機構，可同時提供客戶BS7799及CNS17800 (中華民國國家標準) 驗證服務。

5.**BSi台灣分公司之驗證服務客戶涵蓋**電機、電子、機械、金融、保險、服務、建設、食品、紡織、倉儲、運輸、貿易及醫療等行業別。共計有於各行業**學有專精及經驗豐富專職主導稽核員25位**，提供BSi客戶專業的評審及相關訓練服務。

6.BSi台灣地區提供品質管理系統(ISO 9000 / QS-9000)、環境管理系統(ISO 14001)、職業安全衛生管理系統(OHSAS 18001)等、電子電信業品質管理系統驗證(TL 9000)、資訊安全管理系統驗證(BS 7799)、食品業危害分析管制(HACCP)、整合管理系統驗證(IMSA)等一系列相關整合性驗證及訓練服務。

ISMS ***Information Security Management System***

BSi Management Systems

BSI
We shape the future

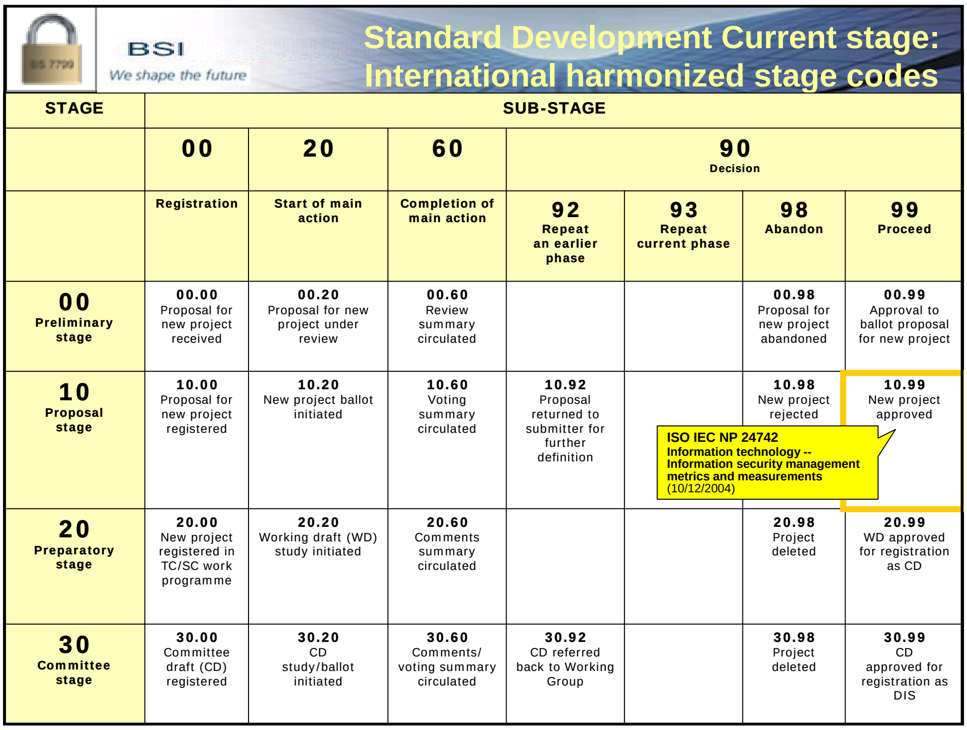
BS7799 Standard

BS 7799-1:2000 / ISO 17799:2000 / CNS17799:2000
Code of practice for information security management
資訊安全管理作業要點

BS 7799-2:2002 / CNS17800:2002
Specification for Information Security Management Systems
資訊安全管理系統要求

ISMS ***Information Security Management System***

BSi Management Systems

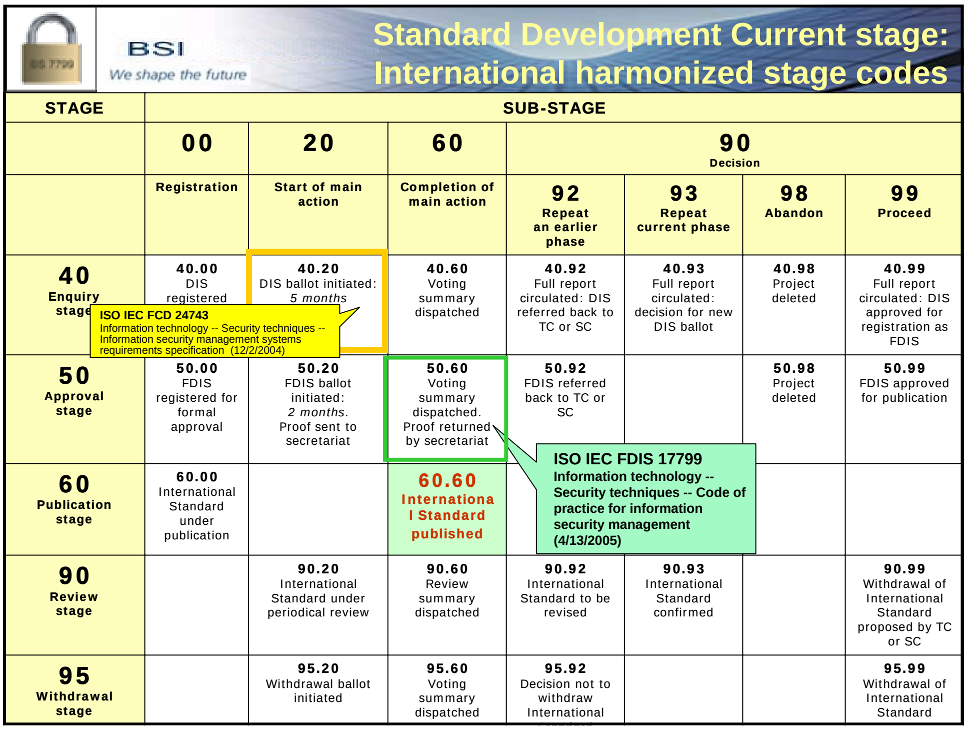


BSI
We shape the future

Standard Development Current stage: International harmonized stage codes

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Review summary circulated			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Voting summary circulated	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Comments summary circulated			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Comments/ voting summary circulated	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS

ISO IEC NP 24742
Information technology -- Information security management metrics and measurements
(10/12/2004)



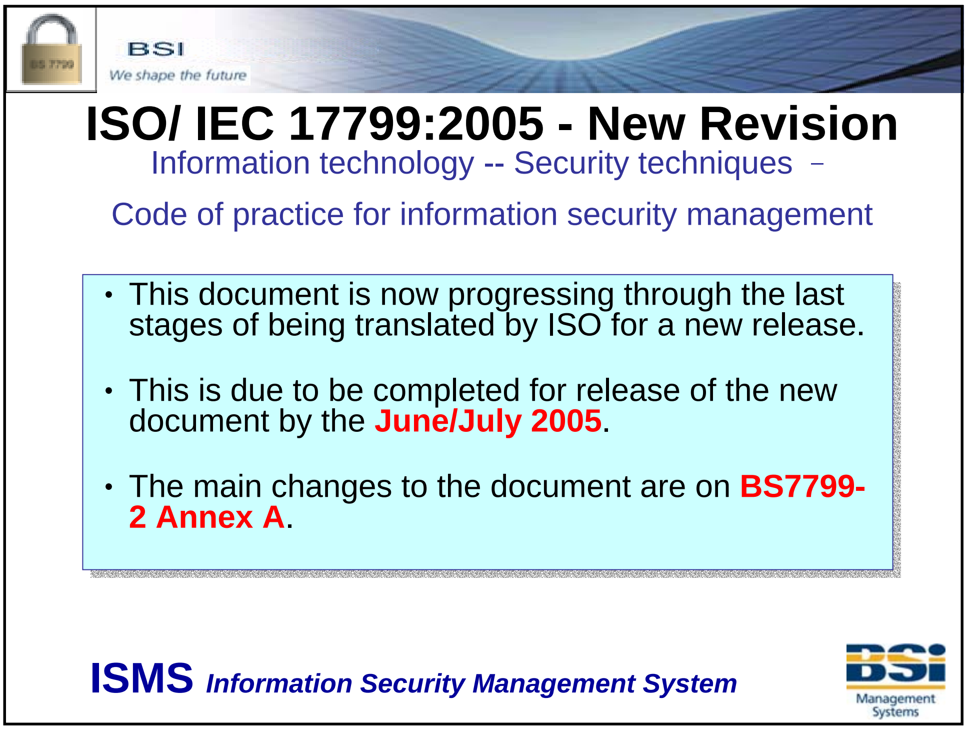
BSI
We shape the future

Standard Development Current stage: International harmonized stage codes

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: *5 months*	40.60 Voting summary dispatched	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval stage	50.00 FDIS registered for formal approval	50.20 FDIS ballot initiated: *2 months*. Proof sent to secretariat	50.60 Voting summary dispatched. Proof returned by secretariat	50.92 FDIS referred back to TC or SC		50.98 Project deleted	50.99 FDIS approved for publication
60 Publication stage	60.00 International Standard under publication		60.60 International Standard published				
90 Review stage		90.20 International Standard under periodical review	90.60 Review summary dispatched	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal stage		95.20 Withdrawal ballot initiated	95.60 Voting summary dispatched	95.92 Decision not to withdraw International			95.99 Withdrawal of International Standard

ISO IEC FCD 24743
Information technology -- Security techniques -- Information security management systems requirements specification (12/2/2004)

ISO IEC FDIS 17799
Information technology -- Security techniques -- Code of practice for information security management
(4/13/2005)



BSI
We shape the future

ISO/ IEC 17799:2005 - New Revision

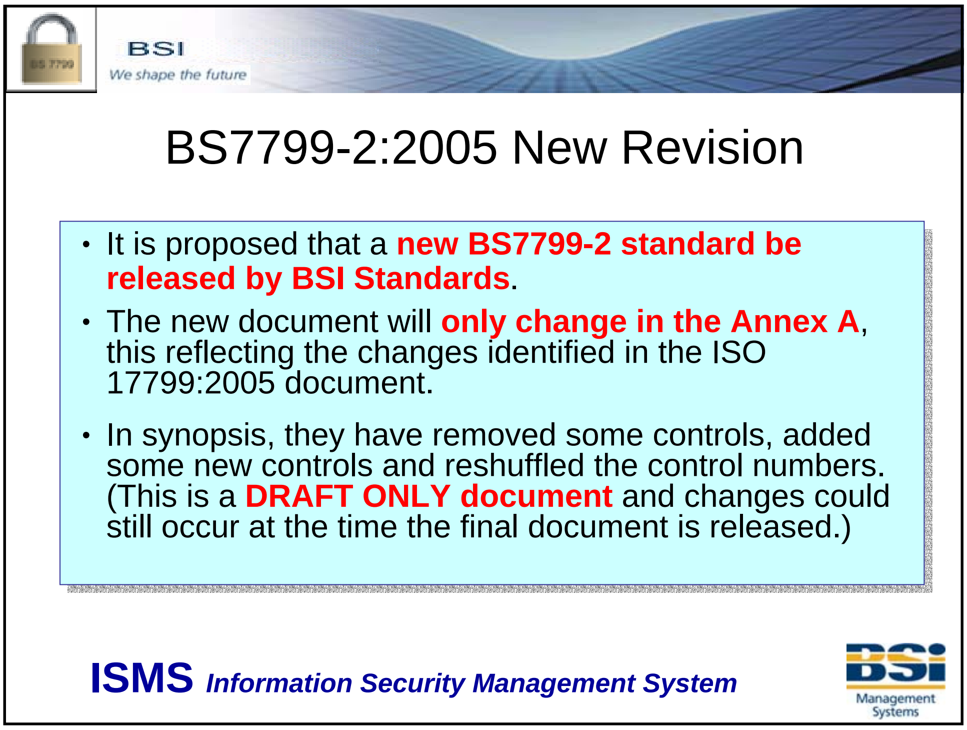
Information technology -- Security techniques –

Code of practice for information security management

- This document is now progressing through the last stages of being translated by ISO for a new release.
- This is due to be completed for release of the new document by the **June/July 2005**.
- The main changes to the document are on **BS7799-2 Annex A**.

ISMS ***Information Security Management System***

BSi Management Systems



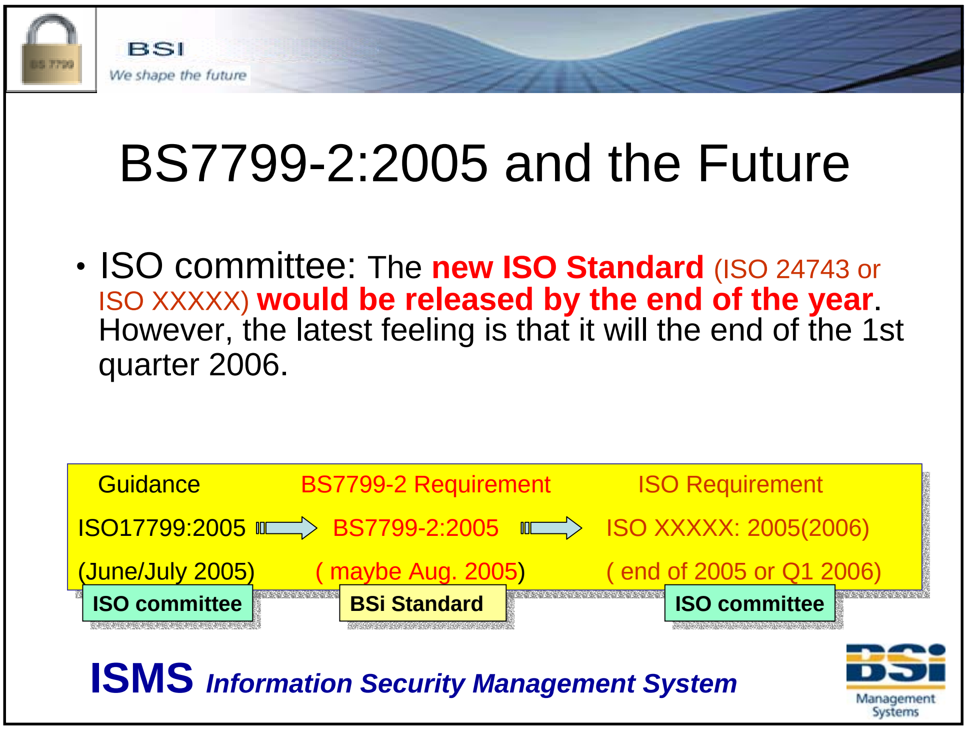
BSI
We shape the future

BS7799-2:2005 New Revision

- It is proposed that a **new BS7799-2 standard be released by BSI Standards**.
- The new document will **only change in the Annex A**, this reflecting the changes identified in the ISO 17799:2005 document.
- In synopsis, they have removed some controls, added some new controls and reshuffled the control numbers. (This is a **DRAFT ONLY document** and changes could still occur at the time the final document is released.)

ISMS ***Information Security Management System***

BSi Management Systems



BSI
We shape the future

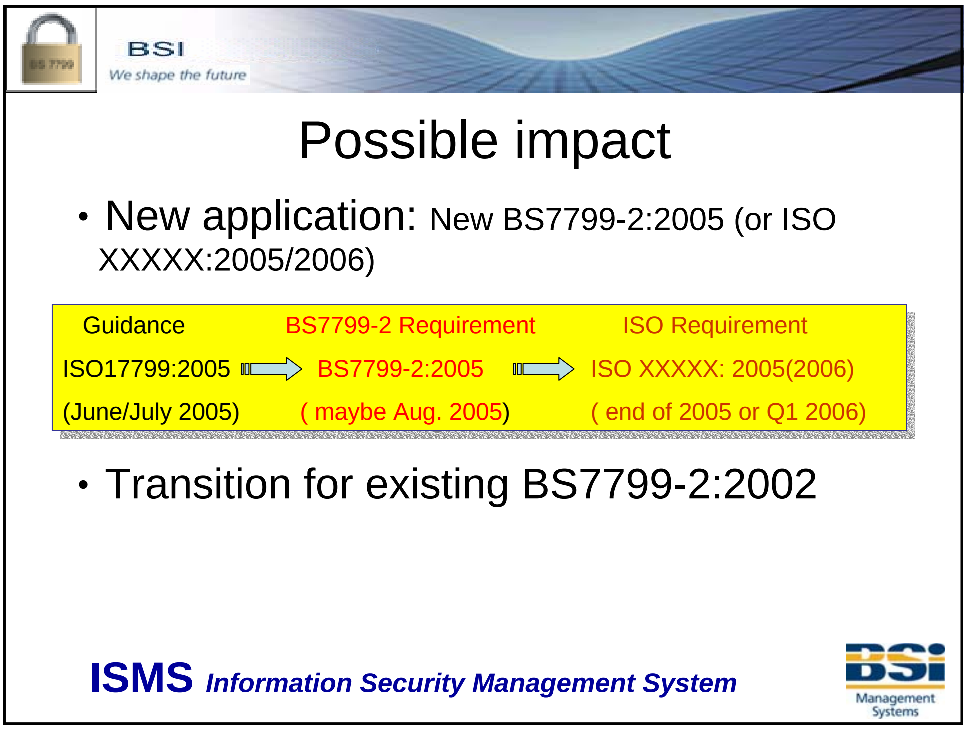
BS7799-2:2005 and the Future

- ISO committee: The **new ISO Standard** (ISO 24743 or ISO XXXXX) **would be released by the end of the year**. However, the latest feeling is that it will the end of the 1st quarter 2006.

Guidance	BS7799-2 Requirement	ISO Requirement
ISO17799:2005 →	BS7799-2:2005 →	ISO XXXXX: 2005(2006)
(June/July 2005)	(maybe Aug. 2005)	(end of 2005 or Q1 2006)
ISO committee	**BSi Standard**	**ISO committee**

ISMS ***Information Security Management System***

BSi Management Systems



BSI
We shape the future

Possible impact

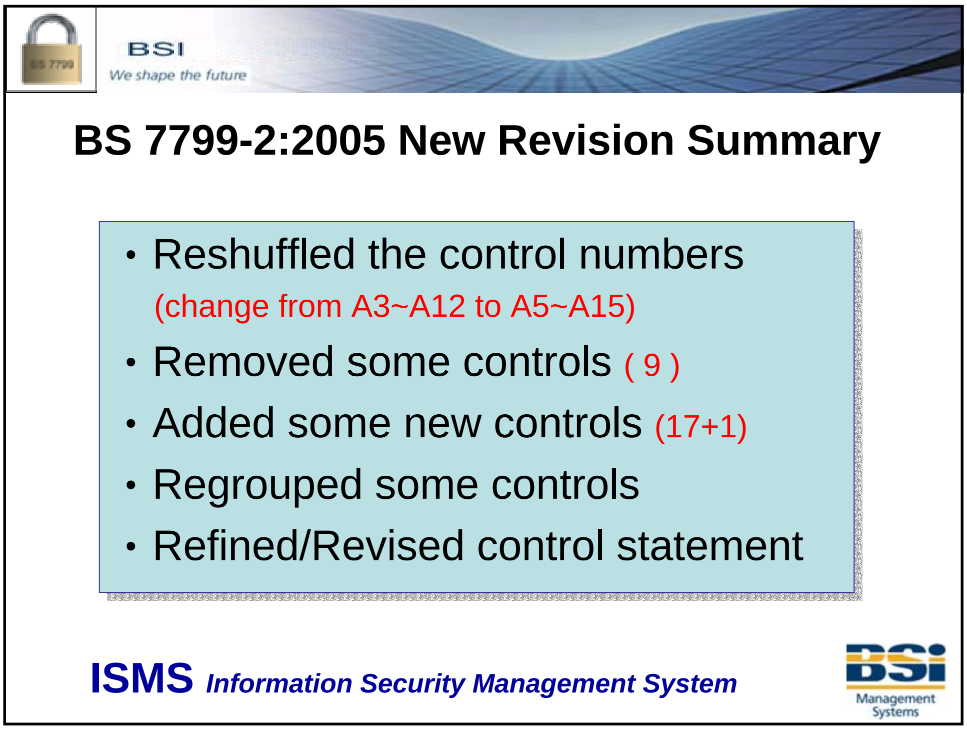
- New application: New BS7799-2:2005 (or ISO XXXXX:2005/2006)

Guidance	BS7799-2 Requirement	ISO Requirement
ISO17799:2005 →	BS7799-2:2005 →	ISO XXXXX: 2005(2006)
(June/July 2005)	(maybe Aug. 2005)	(end of 2005 or Q1 2006)

- Transition for existing BS7799-2:2002

ISMS ***Information Security Management System***

BSi Management Systems



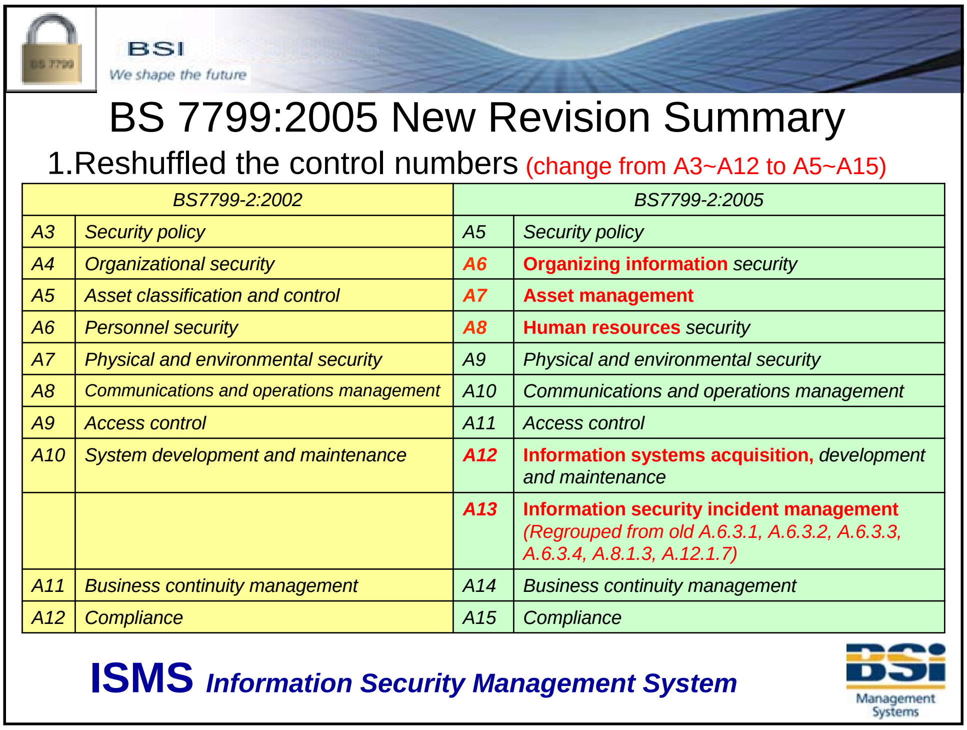
BSI
We shape the future

BS 7799-2:2005 New Revision Summary

- Reshuffled the control numbers (change from A3~A12 to A5~A15)
- Removed some controls (9)
- Added some new controls (17+1)
- Regrouped some controls
- Refined/Revised control statement

ISMS *Information Security Management System*

BSI Management Systems



BSI
We shape the future

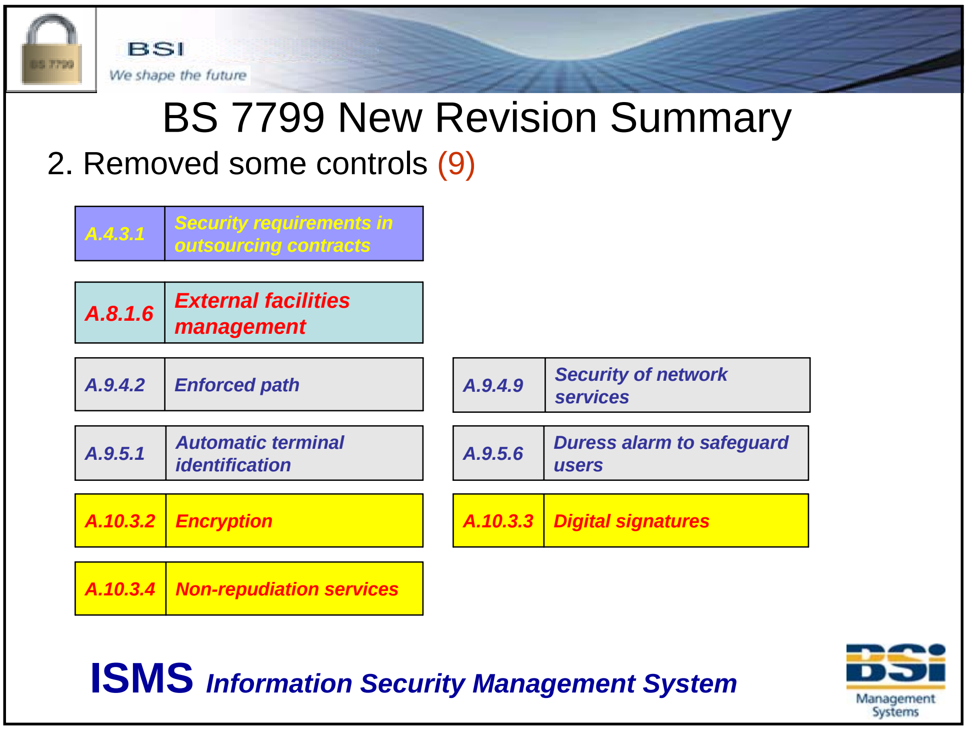
BS 7799:2005 New Revision Summary

1.Reshuffled the control numbers (change from A3~A12 to A5~A15)

BS7799-2:2002		BS7799-2:2005	
A3	*Security policy*	*A5*	*Security policy*
A4	*Organizational security*	***A6***	***Organizing information** security*
A5	*Asset classification and control*	***A7***	***Asset management***
A6	*Personnel security*	***A8***	***Human resources** security*
A7	*Physical and environmental security*	*A9*	*Physical and environmental security*
A8	*Communications and operations management*	*A10*	*Communications and operations management*
A9	*Access control*	*A11*	*Access control*
A10	*System development and maintenance*	***A12***	***Information systems acquisition,** development and maintenance*
		A13	***Information security incident management** (Regrouped from old A.6.3.1, A.6.3.2, A.6.3.3, A.6.3.4, A.8.1.3, A.12.1.7)*
A11	*Business continuity management*	*A14*	*Business continuity management*
A12	*Compliance*	*A15*	*Compliance*

ISMS *Information Security Management System*

BSI Management Systems



BSI
We shape the future

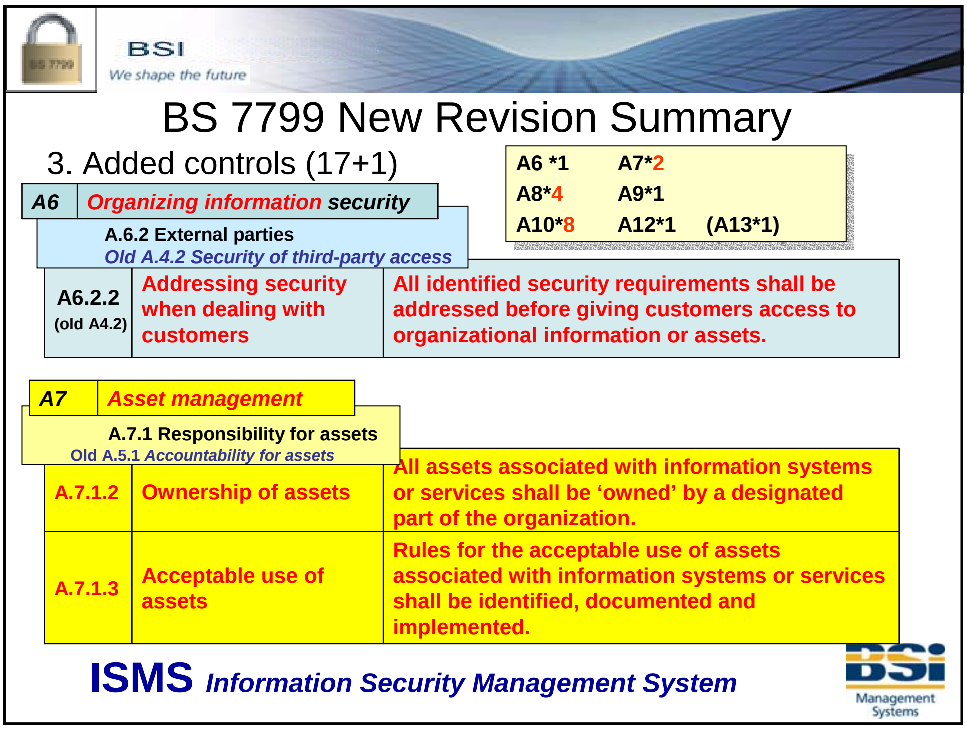
BS 7799 New Revision Summary

2. Removed some controls (9)

A.4.3.1	*Security requirements in outsourcing contracts*
A.8.1.6	*External facilities management*
A.9.4.2	*Enforced path*
A.9.4.9	*Security of network services*
A.9.5.1	*Automatic terminal identification*
A.9.5.6	*Duress alarm to safeguard users*
A.10.3.2	*Encryption*
A.10.3.3	*Digital signatures*
A.10.3.4	*Non-repudiation services*

ISMS ***Information Security Management System***

BSI Management Systems



BSI
We shape the future

BS 7799 New Revision Summary

3. Added controls (17+1)

A6 *1	A7*2	
A8*4	A9*1	
A10*8	A12*1	(A13*1)

A6 ***Organizing information security***

A.6.2 External parties
Old A.4.2 Security of third-party access

A6.2.2 (old A4.2)	**Addressing security when dealing with customers**	**All identified security requirements shall be addressed before giving customers access to organizational information or assets.**

A7 ***Asset management***

A.7.1 Responsibility for assets
Old A.5.1 *Accountability for assets*

A.7.1.2	**Ownership of assets**	**All assets associated with information systems or services shall be 'owned' by a designated part of the organization.**
A.7.1.3	**Acceptable use of assets**	**Rules for the acceptable use of assets associated with information systems or services shall be identified, documented and implemented.**

ISMS ***Information Security Management System***

BSI Management Systems

BSI
We shape the future

BS 7799 New Revision Summary

3. Added controls

A8 ***Human resources security***

A.8.2 During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

(old A.6.2 User training)

A.8.2.1	**Management responsibilities**	**Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.**

employees ⇨ **employees, contractors and third party users**

ISMS ***Information Security Management System***

BSI Management Systems

BSI
We shape the future

BS 7799 New Revision Summary

3. Added controls

A8 ***Human resources security***

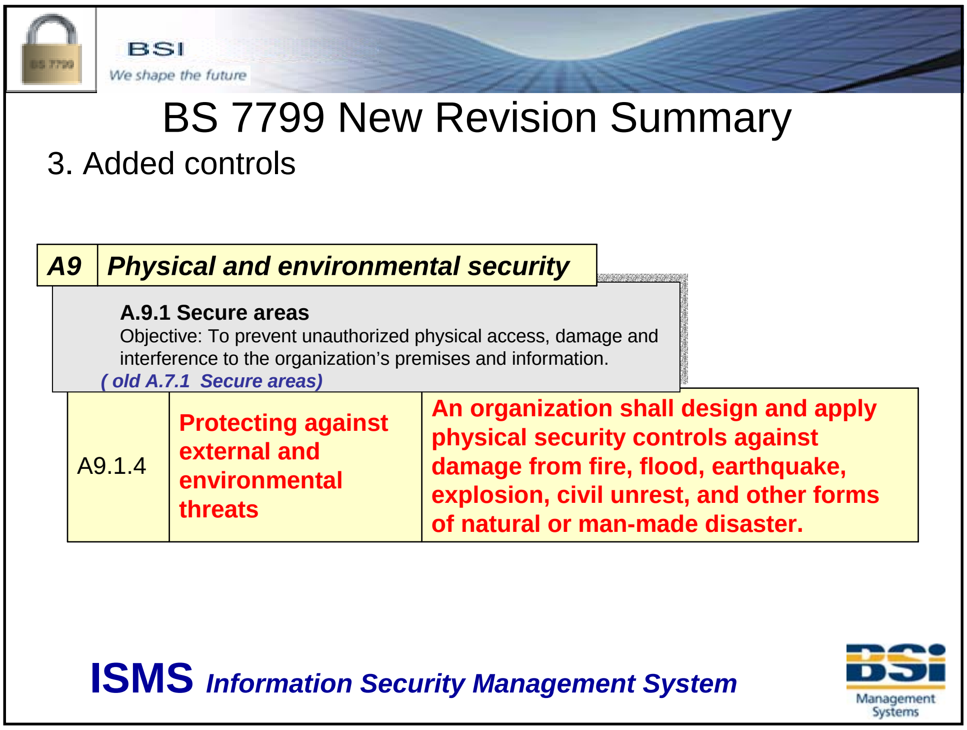
A8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

A8.3.1	**Termination responsibilities**	**Responsibilities for performing employment termination shall be clearly defined and assigned.**
A8.3.2	**Return of assets**	**All employees, contractors and third party users shall return all organizational assets in their possession upon termination of their employment, contract or agreement.**
A8.3.3	**Removal of access rights**	**The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.**

ISMS ***Information Security Management System***

BSI Management Systems



BSI
We shape the future

BS 7799 New Revision Summary

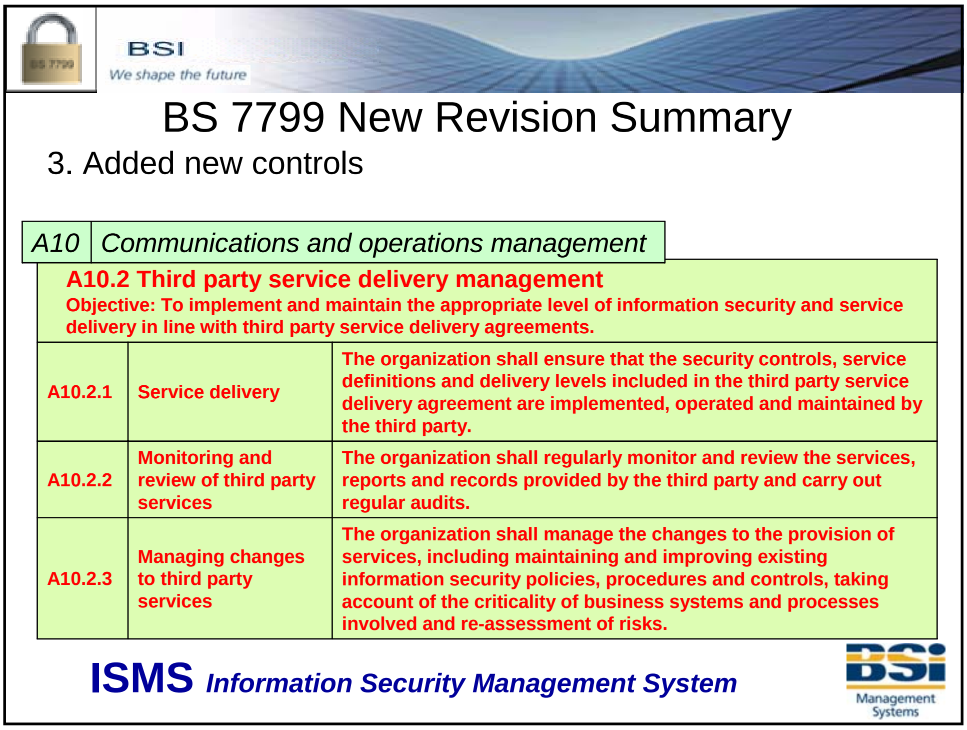
3. Added controls

A9 | ***Physical and environmental security***

A.9.1 Secure areas
Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.
(old A.7.1 Secure areas)

A9.1.4	**Protecting against external and environmental threats**	**An organization shall design and apply physical security controls against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.**

ISMS ***Information Security Management System***



BSI
We shape the future

BS 7799 New Revision Summary

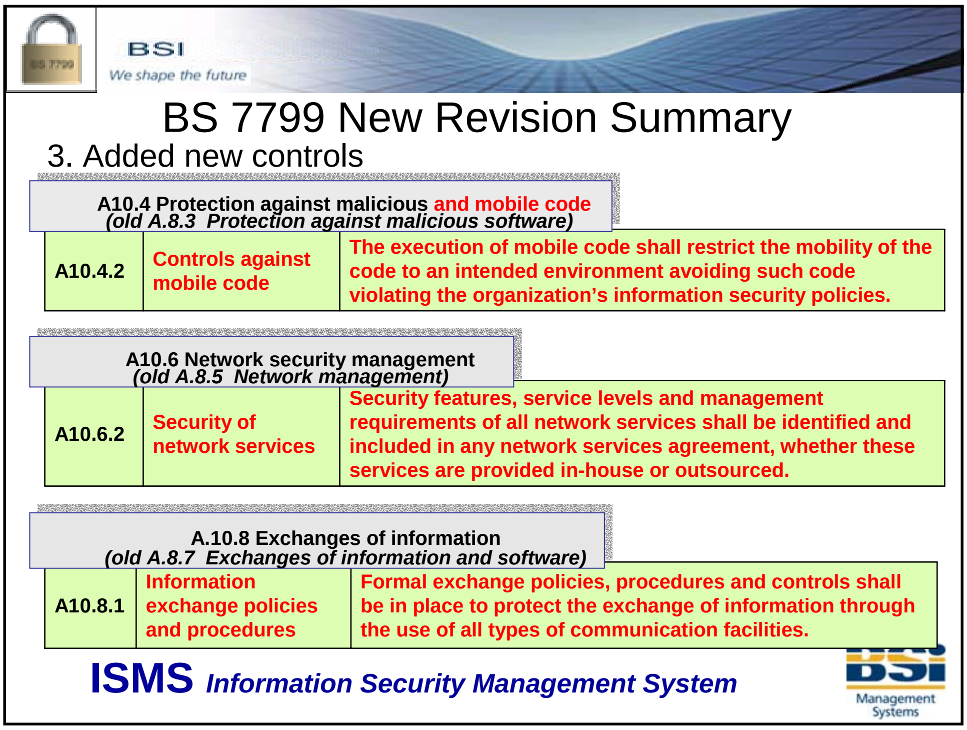
3. Added new controls

A10 | *Communications and operations management*

A10.2 Third party service delivery management
Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

A10.2.1	**Service delivery**	**The organization shall ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.**
A10.2.2	**Monitoring and review of third party services**	**The organization shall regularly monitor and review the services, reports and records provided by the third party and carry out regular audits.**
A10.2.3	**Managing changes to third party services**	**The organization shall manage the changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, taking account of the criticality of business systems and processes involved and re-assessment of risks.**

ISMS ***Information Security Management System***



BSI

We shape the future

BS 7799 New Revision Summary

3. Added new controls

A10.4 Protection against malicious and mobile code
(old A.8.3 Protection against malicious software)

A10.4.2	**Controls against mobile code**	**The execution of mobile code shall restrict the mobility of the code to an intended environment avoiding such code violating the organization's information security policies.**

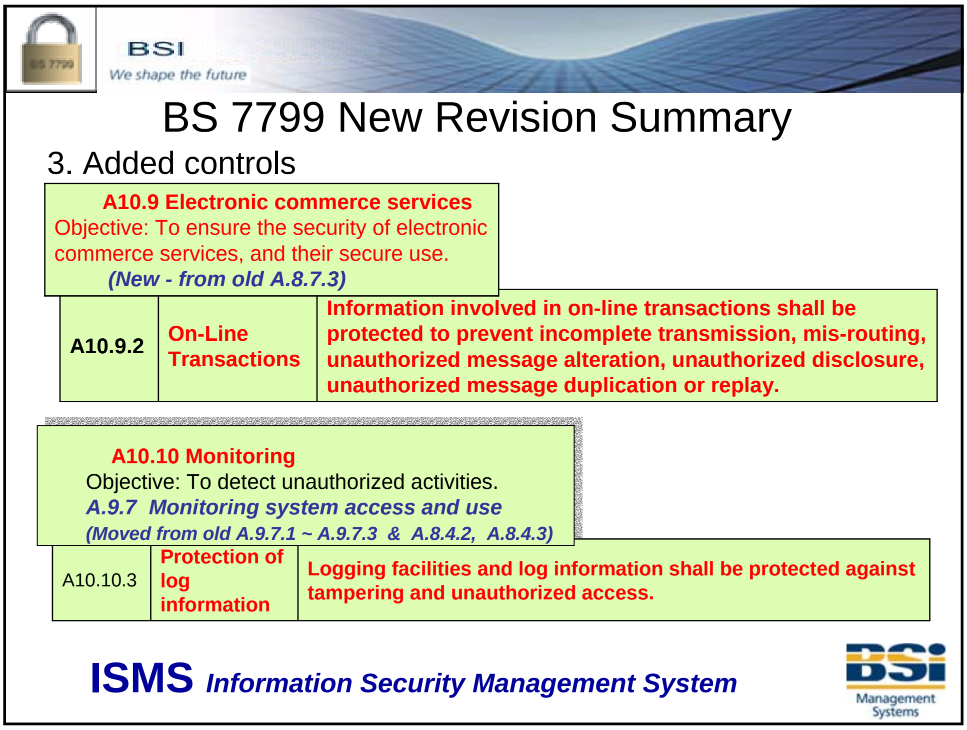
A10.6 Network security management
(old A.8.5 Network management)

A10.6.2	**Security of network services**	**Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.**

A.10.8 Exchanges of information
(old A.8.7 Exchanges of information and software)

A10.8.1	**Information exchange policies and procedures**	**Formal exchange policies, procedures and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.**

ISMS ***Information Security Management System***



BSI

We shape the future

BS 7799 New Revision Summary

3. Added controls

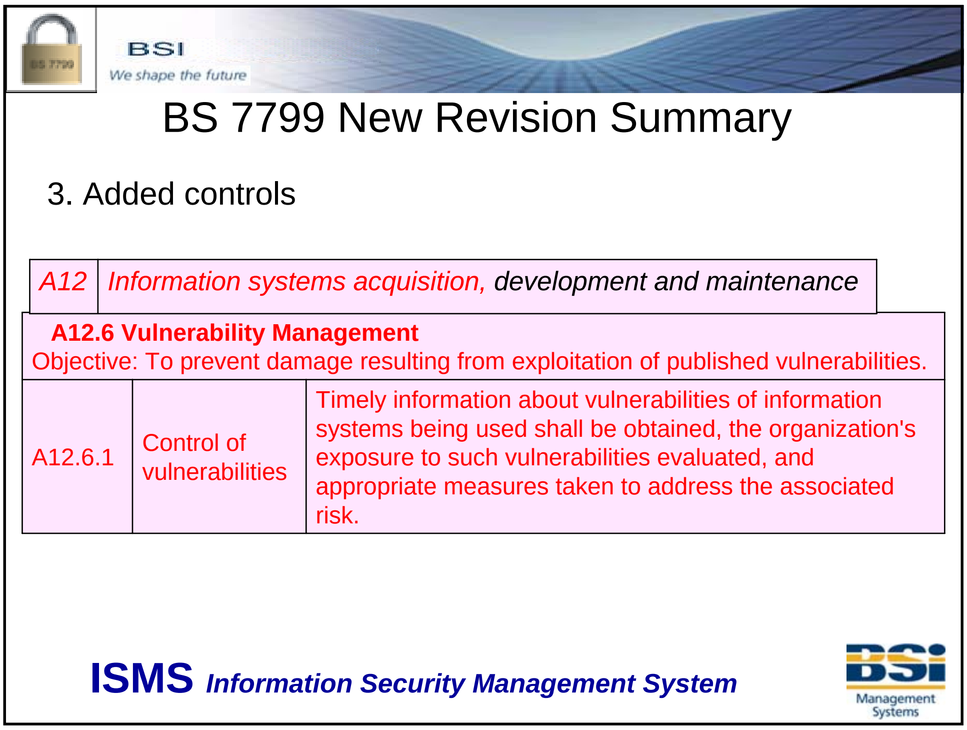
A10.9 Electronic commerce services
Objective: To ensure the security of electronic commerce services, and their secure use.
(New - from old A.8.7.3)

A10.9.2	**On-Line Transactions**	**Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.**

A10.10 Monitoring
Objective: To detect unauthorized activities.
A.9.7 Monitoring system access and use
(Moved from old A.9.7.1 ~ A.9.7.3 & A.8.4.2, A.8.4.3)

A10.10.3	**Protection of log information**	**Logging facilities and log information shall be protected against tampering and unauthorized access.**

ISMS ***Information Security Management System***



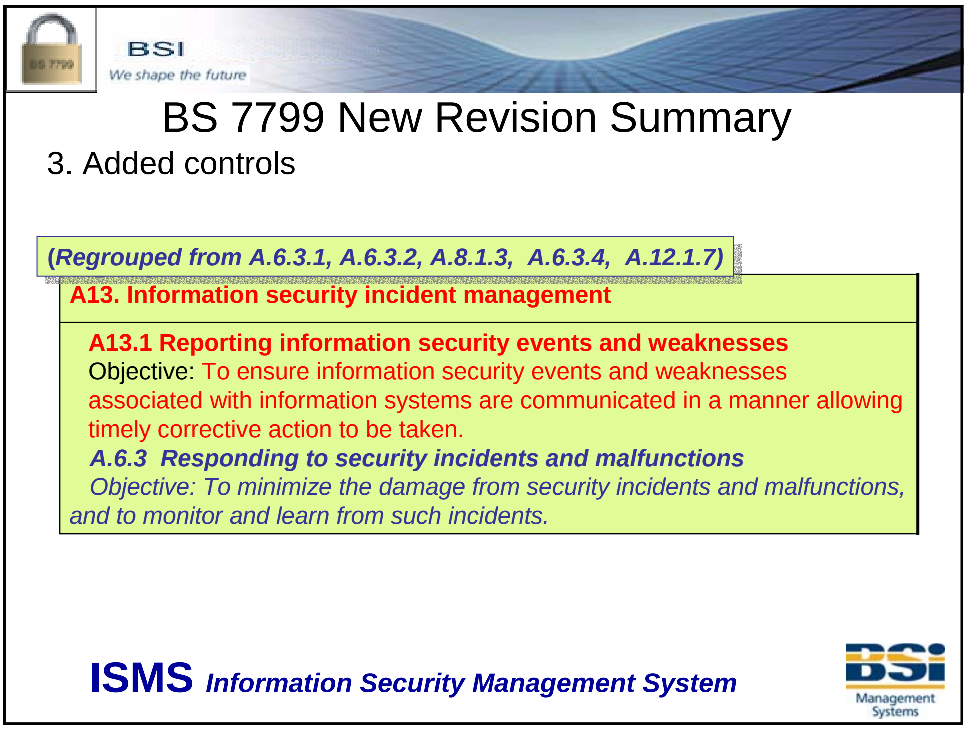
BSI
We shape the future

BS 7799 New Revision Summary

3. Added controls

A12	*Information systems acquisition, development and maintenance*	
A12.6 Vulnerability Management Objective: To prevent damage resulting from exploitation of published vulnerabilities.		
A12.6.1	Control of vulnerabilities	Timely information about vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

ISMS ***Information Security Management System***



BSI
We shape the future

BS 7799 New Revision Summary

3. Added controls

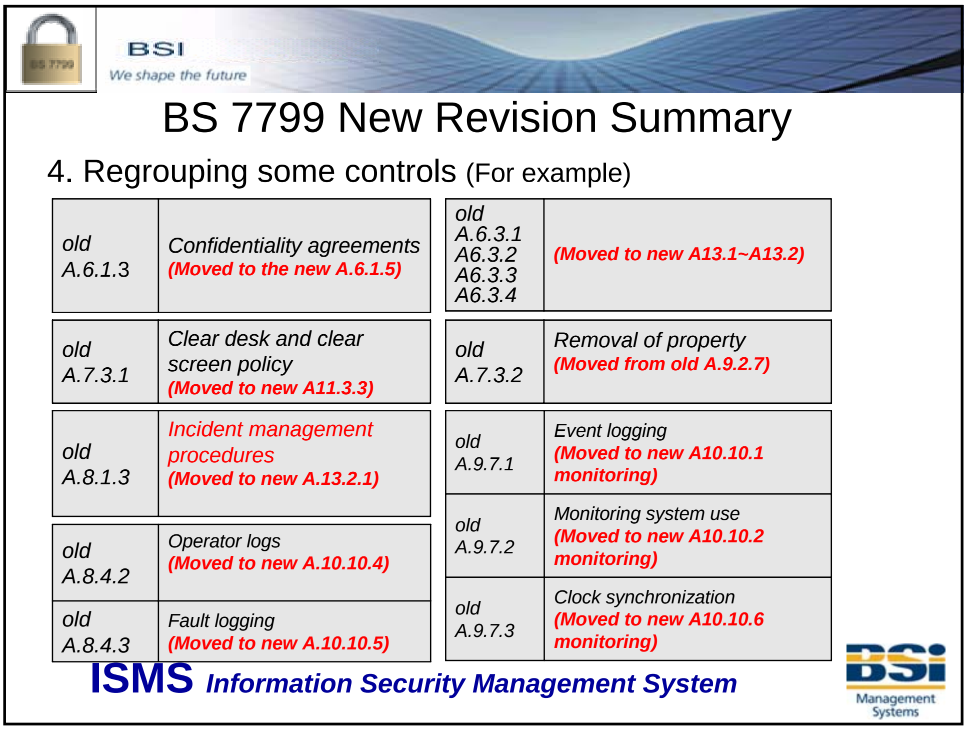
(Regrouped from A.6.3.1, A.6.3.2, A.8.1.3, A.6.3.4, A.12.1.7)

A13. Information security incident management

A13.1 Reporting information security events and weaknesses
Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.6.3 Responding to security incidents and malfunctions
Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

ISMS ***Information Security Management System***



BSI
We shape the future

BS 7799 New Revision Summary

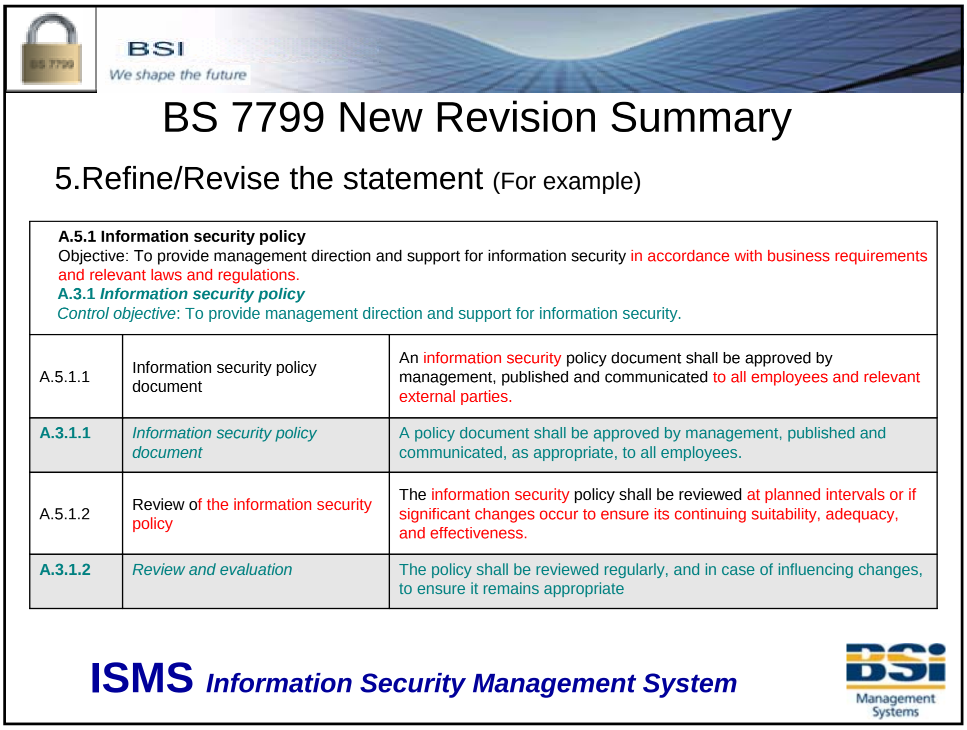
4. Regrouping some controls (For example)

old A.6.1.3	*Confidentiality agreements* ***(Moved to the new A.6.1.5)***
old A.7.3.1	*Clear desk and clear screen policy* ***(Moved to new A11.3.3)***
old A.8.1.3	*Incident management procedures* ***(Moved to new A.13.2.1)***
old A.8.4.2	*Operator logs* ***(Moved to new A.10.10.4)***
old A.8.4.3	*Fault logging* ***(Moved to new A.10.10.5)***

old A.6.3.1 A6.3.2 A6.3.3 A6.3.4	***(Moved to new A13.1~A13.2)***
old A.7.3.2	*Removal of property* ***(Moved from old A.9.2.7)***
old A.9.7.1	*Event logging* ***(Moved to new A10.10.1 monitoring)***
old A.9.7.2	*Monitoring system use* ***(Moved to new A10.10.2 monitoring)***
old A.9.7.3	*Clock synchronization* ***(Moved to new A10.10.6 monitoring)***

ISMS ***Information Security Management System***

BSI Management Systems



BSI
We shape the future

BS 7799 New Revision Summary

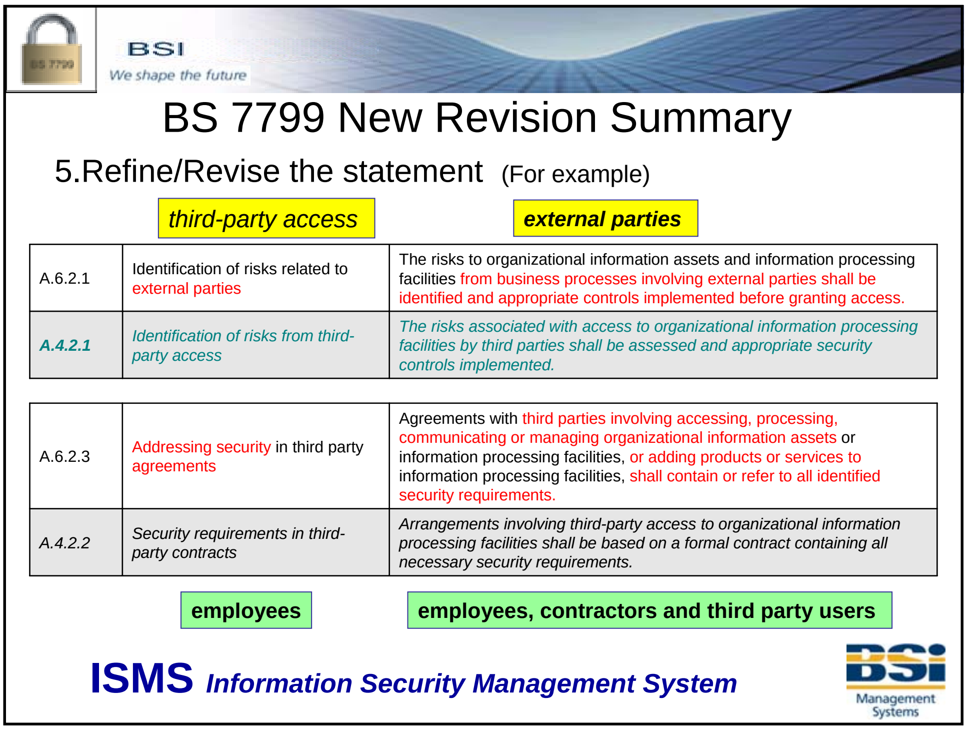
5.Refine/Revise the statement (For example)

A.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.
A.3.1 Information security policy
Control objective: To provide management direction and support for information security.

A.5.1.1	Information security policy document	An information security policy document shall be approved by management, published and communicated to all employees and relevant external parties.
A.3.1.1	*Information security policy document*	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.3.1.2	*Review and evaluation*	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate

ISMS ***Information Security Management System***

BSI Management Systems



BSI
We shape the future

BS 7799 New Revision Summary

5.Refine/Revise the statement (For example)

third-party access **external parties**

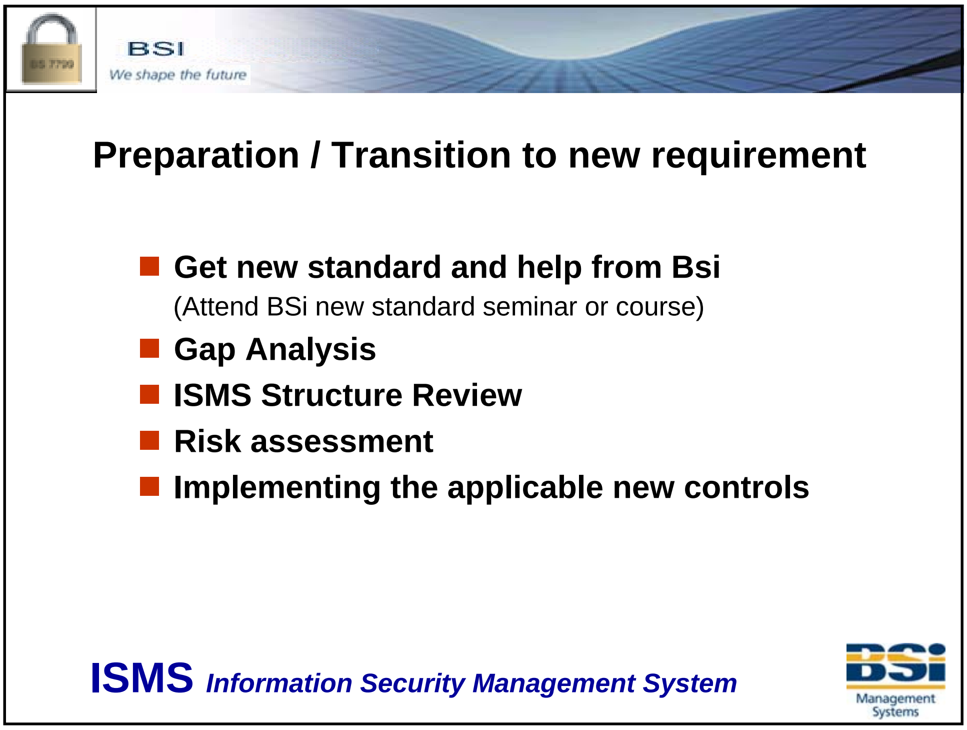
A.6.2.1	Identification of risks related to external parties	The risks to organizational information assets and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.4.2.1	*Identification of risks from third-party access*	*The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.*

A.6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing organizational information assets or information processing facilities, or adding products or services to information processing facilities, shall contain or refer to all identified security requirements.
A.4.2.2	*Security requirements in third-party contracts*	*Arrangements involving third-party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.*

employees **employees, contractors and third party users**

ISMS ***Information Security Management System***

BSi Management Systems



BSI
We shape the future

Preparation / Transition to new requirement

- **Get new standard and help from Bsi**
  (Attend BSi new standard seminar or course)
- **Gap Analysis**
- **ISMS Structure Review**
- **Risk assessment**
- **Implementing the applicable new controls**

ISMS ***Information Security Management System***

BSi Management Systems

BS 7799

BSI

We shape the future

If your information is not safe,

your future is not secure!

Thank You

英國標準協會

ISMS ***Information Security Management System***

BSI

Management Systems