



**Business Continuity Management
Legislations, Regulations and Standards**

Version 4 – June 2010

INTRODUCTION

The BCI is regularly asked by members and other interested parties about current legislation, regulation and standards that exist nationally and internationally for Business Continuity Management.

It is difficult to provide a definitive list because there are regular changes and amendments at a country level and often inconsistent terminology between countries, sectors and legislators.

The document that follows is the most comprehensive that it was possible to produce based upon information provided to us by our members around the world. Where we have country input we have included it alphabetically. At the end of the document we have a page summarising current and projected international initiatives particularly those supported by the International Standards Organisation (ISO) and the Basel Committee on Banking Supervision.

Each section is divided into four headings. For some countries we might have no available data in a particular section and this will be shown as "None Available". Countries for which we have no information available under any of the 4 headings will not be included. If any reader has additional information to help us fill in these gaps, then please submit it to jan.gilbert@thebci.org for future amendment of the document.

The four headings are:

LEGISLATION: Government laws which include aspects of Business Continuity Management by name or are sufficiently similar in nature (Disaster Recovery, Emergency Response, Crisis Management) to be treated as BCM legislation for this purpose. To be included in this category they must be legally enforceable legislation passed by a national, federal, state or provincial government depending upon the legal structure in each particular country.

REGULATION: Mandatory rules or audited guidance documents from official regulatory bodies in all sectors such as Financial Services, Energy, Oil and Gas, which could reasonably be construed as having some implications on an organisation's BCM provisions. General help, guidance and suggestions are included under Guidelines.

STANDARDS: Official standards from national (and international) accredited standards bodies which relate to Business Continuity as a whole or specific related subset such as IT Service Continuity. The list also includes standards for different but related topics (like Information Security) when BCM is included only as a minor requirement for compliance. "Standards" that are issued by 3rd parties or professional groups will only be included if they are ratified by an accredited national standards body or accredited directly by a national accreditation service affiliated to the International Accreditation Forum (IAF).

GUIDELINES: Guidelines published as good (or best) practice by various authoritative organisations. These documents may form part of a wider set of advice provided by a professional body for whom BCM is only a peripheral activity, or alternatively they might be issued by a BCM professional body as general guidance either locally or internationally. They will provide no mandated rules but will be used and recognised as credible by BCM professionals.

WARNING

The BCI has done its best to check the validity of these details but takes no responsibility for their accuracy and currency at any particular time or in any particular circumstances.

Some of the listed items (particularly under legislation and regulation) are only indirectly related to Business Continuity Management, and should not be interpreted as specifically designed for BCM. However they will contain sections which can be useful to a BCM practitioner, and are consequently included in this reference document.

It should also be noted that in some countries Regulatory Practices and/or ISO Standards might be incorporated into national legislation, thus giving the document additional importance in those specific countries.

Lyndon Bird FBCI
International Technical Director
The Business Continuity Institute

HISTORY PAGE

Approvals

Role	Approved by	Date
------	-------------	------

Distribution List

From	Date	Contact details
------	------	-----------------

Jan Gilbert 19.2.09 Jan.gilbert@thebci.org

To	Action	Due date	Contact details
----	--------	----------	-----------------

Action types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify):

Version History

File Reference	Date	Author / amend	Description	Status
0.1	October 09	Jan Gilbert		Draft
0.2	April 2010	Jan Gilbert	Updated Australia	DRAFT
0.3	June 2010	Jan Gilbert	Amendments from L Bird	DRAFT
0.4	June 2010	Jan Gilbert		Complete
0.5				
0.6				

© The BCI Limited 2009.

CONTENTS

INTRODUCTION	1
HISTORY PAGE	3
COUNTRY: AUSTRALIA	3
Legislation	3
Regulation	3
Standards	3
Good Practice	3
COUNTRY: BAHAMAS	4
Legislation	4
Regulation	4
Standards	4
Good Practice	4
COUNTRY: BRAZIL	5
Legislation	5
Regulation	5
Standards	5
Good Practice	5
COUNTRY: CANADA	6
Legislation	6
Regulation	6
Standards	6
Good Practice	6
COUNTRY: CHINA (including Hong Kong and Macau)	7
Legislation	7
Regulation	7
Standards	8
Good Practice	8
COUNTRY: INDIA	9
Legislation	9
Regulation	9
Standards	9
Good Practice	9
COUNTRY: INDONESIA	10
Legislation	10
Regulation	10
Standards	10
Good Practice	10
COUNTRY: JAPAN	11
Legislation	11
Regulation	11
Standards	11
Good Practice	11
COUNTRY: MALAYSIA	12
Legislation	12
Regulation	12
Standards	12
Good Practice	12
COUNTRY: NEW ZEALAND	13
Legislation	13
Regulation	13
Standards	13
Good Practice	13

COUNTRY: PHILIPPINES	14
Legislation	14
Regulation	14
Standards	14
Good Practice	14
COUNTRY: RUSSIA (Russian Federation)	15
Legislation	15
Regulation	15
Standards	15
Good Practice	15
COUNTRY: SINGAPORE	16
Legislation	16
Regulation	16
Standards	16
Good Practice	16
COUNTRY: SOUTH AFRICA	18
Legislation	18
Regulation	18
Standards	19
Good Practice	19
COUNTRY: SOUTH KOREA (Republic of Korea)	20
Legislation	20
Regulation	20
Standards	20
Good Practice	20
COUNTRY: SWITZERLAND	21
Legislation	21
Regulation	21
Standard	21
Good Practice	21
COUNTRY: THAILAND	22
Legislation	22
Regulation	22
Standards	22
Good Practice	22
COUNTRY: UK	23
Legislation	23
Regulation	23
Standards	24
Good Practice	24
COUNTRY: USA	25
Legislation	25
Regulation	27
Standards	31
Good Practice	32
COUNTRY: INTERNATIONAL	36
Legislation	36
Regulation	36
Standards	37
Good Practice	39

COUNTRY: AUSTRALIA

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
APS232	Australian Prudential Regulatory Authority (APRA)	APRA regulation for BCM in regulated Financial Services firms
APS 231	APRA	Outsourcing, which includes BCM requirements
APS 222	APRA	Related Facilities, which includes BCM requirements

Standards

TITLE	AUTHORITY	SUMMARY
AS/NZ 5050 PENDING	Standards Australia	Standard for Business Continuity Management, due for ratification 2010.
ANZ HB 221:2004	Standards Australia	Business Continuity Handbook
ANZ HB 292:2006	Standards Australia	Practitioners Guide to BCM
ANZ HB 293:2006	Standards Australia	Executive Guide to BCM

Good Practice

TITLE	AUTHORITY	SUMMARY
Business Continuity Management, Building Resilience in public sector entities	Australian National Audit Office (ANAO)	
AIIMS 2004 - Australian Inter-service Incident Management System	Australian Fire Authority Council	Now used by many infrastructure providers
Australian Emergency Manual Series (several volumes)	Emergency Management Australia	

COUNTRY: BAHAMAS

Legislation

TITLE	AUTHORITY	SUMMARY
Disaster Preparedness and Response Act 2006 Emergency Relief Guarantee Fund Act 1999	National Emergency Management Agency (NEMA)	NEMA is the government agency of the Commonwealth of The Bahamas. It is responsible for all disaster planning and related legislation and guidance, particularly related to hurricanes.

Regulation

TITLE	AUTHORITY	SUMMARY
PU19-0406 - Supervisory and Regulatory Guidelines – Business Continuity 1 st May 2007	The Central Bank of the Bahamas	The guidelines apply to all commercial banks (domestic or foreign) operating in all territories of the Bahamas. They are based upon the Basel Committee's Joint Forum "High Level Principles"

Standards

TITLE	AUTHORITY	SUMMARY
None	The Bahamas tend to use US ANSI standards rather than British or ISO equivalents.	Many banks are Canadian owned and they are influenced by the Canadian standard CAN/CSA-Z 731-03

Good Practice

TITLE	AUTHORITY	SUMMARY
Guidelines provided by NEMA (printed and downloadable from NEMA website)	NEMA	Publications include: <ul style="list-style-type: none"> - Family Disaster Plan - Disaster Supplies Kit - Shelter Information - Mobility Checklists - Pets in Disasters

COUNTRY: BRAZIL

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
NBR15999-1 Gestão de continuidade de negócios - Parte 1: Código de prática	ABNT (Associação Brasileira de Normas Técnicas)	Brazilian Portuguese straight translation of the English standard BS 25999-1 Business continuity management. Code of practice
NBR15999-2 Gestão de continuidade de negócios - Parte 2: Requisitos	ABNT (Associação Brasileira de Normas Técnicas)	Brazilian Portuguese straight translation of the English standard BS 25999-2 Specification for business continuity management
NBR ISO/IEC24762 Tecnologia da informação - Técnicas de segurança - Diretrizes para os serviços de recuperação após um desastre na tecnologia da informação e de comunicação	ABNT (Associação Brasileira de Normas Técnicas)	Brand new, very recently announced, Brazilian Portuguese straight translation of the ISO standard 24762 - Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

Standards

TITLE	AUTHORITY	SUMMARY
See Regulation		

Good Practice

TITLE	AUTHORITY	SUMMARY
Summary version in Portuguese of BCI GPG2008	BCI	To be replaced by GPG2010

COUNTRY: CANADA

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
IDA By-Law 17.19 – Business Continuity Plan Requirement	OSC (Ontario Securities Commission)	The purpose of the proposed by-law is to require each IDA member to establish and maintain a business continuity plan, such that the member can stay in business in the event of a significant business disruption and can meet obligations to its customers and other capital markets counterparts.

Standards

TITLE	AUTHORITY	SUMMARY
CAN/CSA-Z 731-03	CSA (Canadian Standards Association)	Canada's emergency preparedness and response standards
CSA Z1600		Proposed Canadian standard for integrating business continuity and emergency management programs, based on NFPA 1600

Good Practice

TITLE	AUTHORITY	SUMMARY
Information Technology Control Guidelines	Canadian Institute of Chartered Accountants	Crisis Management for Directors
Letter to Federally Regulated Financial Institutions, Insurance Companies, CBA etc March 2006		

COUNTRY: CHINA (including Hong Kong and Macau)

Legislation

TITLE	AUTHORITY	SUMMARY
Personal Data (Privacy) Ordinance	Office of the Privacy Commissioner for Personal Data – the Government of the Hong Kong Special Admin Region	The purpose of the Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well-being by safeguarding the free flow of personal data.

Regulation

TITLE	AUTHORITY	SUMMARY
Business continuity planning supervisory policy manual – TM-G-2	The Hong Kong Monetary Authority	Sets out the HKMA's latest supervisory policies and practices, the minimum standards authorised institutions (AI'S) are expected to attain in order to satisfy the requirements of the Banking ordinance and recommendations on best practices
Circular to licensed corporations – “Business continuity planning against serious communicable diseases”	Securities and Futures Commission of Hong Kong	Circular to remind licensed persons to take precautions against a re-occurrence of SARS or other serious communicable diseases
HKMA Supervisory Policy Manual, BCP TM-G-2 V1 02.12.02	Hong Kong Monetary Authority	Enforced by onsite examinations, requires need for BCP documentation and testing at least annually, planning for different scenarios and prolong outages.
HKMA Supervisory Policy Manual, General Principles for Technology Risk Management TM-G-1 V.1 24.06.03	Hong Kong Monetary Authority	Refers to TM-G-2 on BCP on the need to provide continuous service
HKMA, Supervisory Policy Manual, Supervision of E-Banking TM-E-1 V.1	Hong Kong Monetary Authority	Refers to TM-G-2 on BCP on the need to provide continuous and /or

17.02.04		alternative services
IT Security Guidelines – G3	Information Technology Services Dept – The Government of the Hong Kong Special Admin Region	Introduces general concepts relating to IT Security and elaborates interpretations on the Baseline IT Security policy. It also provides readers some guidelines and considerations in defining security requirements.
Management, Supervision and Internal Control Guidelines ("the Internal Control Guidelines")	Securities and Futures Commission of Hong Kong	A licensed or registered person should have internal control procedures and financial and operational capabilities which can be reasonably expected to protect its operations, its clients and other licensed or registered persons from financial loss arising.

Standards

TITLE	AUTHORITY	SUMMARY
None specific to China, Hong Kong or Macau. Use of ISO, ANSI or BS standards in use by international firms.		

Good Practice

TITLE	AUTHORITY	SUMMARY
General Principles for Technology Risk Management V1 – TM-G-1	The Hong Kong Monetary Authority	To provide AIs with guidance on general principles which AIs are expected to consider in managing technology-related risks.
Guidance Note on the Use of internet for Insurance activities (GN8)	Office of the Commissioner of Insurance – The Government of the Hong Kong special administrative region	To better protect the insuring public and ensuring the healthy development of the industry in the formation technology era.
BCI Good Practice Guidelines - 2008	BCI	Versions in both English and Mandarin.

COUNTRY: INDIA

Legislation

TITLE	AUTHORITY	SUMMARY
There is no specific BCM legislation; however it is becoming more popular these days as a good business practice.		

Regulation

TITLE	AUTHORITY	SUMMARY
India BCP	<ol style="list-style-type: none"> 1. Reserve Bank of India (RBI) 2. Securities & Exchange Board of India (SEBI) 3. National Stock Exchange (NSE) 4. Bombay Stock Exchange (BSE) 	Enforced by audit, requires need for BCP documentation and testing for least annually.

Standards

TITLE	AUTHORITY	SUMMARY
ISO and BS standards are well known and heavily used in India.		

Good Practice

TITLE	AUTHORITY	SUMMARY
Banking		In Banking/Financial institutions BCM is usually integrated with Risk Management.
BPO (Business Process Outsourcers)		In IT/BPO organisations, BCM is based on internal business requirements and often global customer specific requirements.

COUNTRY: INDONESIA

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
Regulation No 9/15/PBI/2007	Bank Indonesia	Implementation of Risk Management in the use of information technology by commercial banks.
Regulation no. 6/8/PBI/2004	Bank Indonesia	The Bank Indonesia real time gross settlement system (unofficial translation)
Indonesia BCP	Bank Indonesia (Central Bank)	Requires BCP documentation and at least annually with focus on Bank Indonesia RTGS system. Requires internal audit to conduct an audit at least annually and provide report to Bank Indonesia.

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: JAPAN

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
Manual for the Development of Contingency Plans in Financial Institutions. Japan FSA	FISC (The Center for Financial Industry Information System)	Audit matter Appointment of BCP Manager Implementation of policy & standard Proper documentation Regular review of plan Corporate-wide testing at least annually Planning for different scenarios No clear guideline to follow

Standards

TITLE	AUTHORITY	SUMMARY
In Japan ISO standards are well accepted and often incorporated into corporate law. This might be the case in future with ISO 22301 or even ISO 22399.		

Good Practice

TITLE	AUTHORITY	SUMMARY
Business Continuity at Bank of Japan	BOJ (Bank of Japan)	Assures an approach to aim at operational continuity.
BCI Good Practice Guidelines - 2008	BCI	Version available in Japanese.

COUNTRY: MALAYSIA

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
BNM/RH/GL013-3	Central Bank of Malaysia	Outlines and enforces minimum BCM requirements on the institution so as to ensure the continuity of critical business functions and essential services within a specified timeframe in the event of a major disruption.
Guidelines on Management of IT Environment	BNM – Bank Malaysia Central Bank	Outlines minimum responsibilities and requirements for planning and managing, as well as, establishing preventive and detective measures that should be implemented by institutions to mitigate the risks pertaining to IT environment

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: NEW ZEALAND

Legislation

TITLE	AUTHORITY	SUMMARY
The Civil Defence & Emergency Management Act (2002)		

Regulation

TITLE	AUTHORITY	SUMMARY
None		

Standards

TITLE	AUTHORITY	SUMMARY
SAA/SNZ HB221:2004		Business continuity management
AS/NZS 4360		HB436 Risk Management

Good Practice

TITLE	AUTHORITY	SUMMARY
Australian Handbooks		Used in both Australia and New Zealand

COUNTRY: PHILIPPINES
Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
542	Philippines Central Bank	Consumer protection for electronic banking
-	Philippines Central Bank	Back up operation centers and data recovery sites
-	Philippines Central Bank	Business continuity plan
-	Philippines Central Bank	Updated business continuity plan
-	Philippines Central Bank	Extension of submission of business continuity plan
-	Philippines Central Bank	Business continuity plan
269	Philippines Central Bank	New guidelines concerning electronic banking activities
268	Philippines Central Bank	Implementing rules and regulations of Sec 55.1 (e) of the General Banking Law 2000
-	Philippines Central Bank	Year 2000 business continuity/business resumption contingency planning
Manila Bank BCP	Bank of Central Philippines (local central bank)	Enforced by audit, requires all banks to set up of a disaster recovery facility

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: RUSSIA (Russian Federation)

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
242-P	Bank of Russia	Banking internal control

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: SINGAPORE
Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
MAS Business Continuity Management Guidelines (June 2003)	MAS (Monetary authority of Singapore)	7 Guiding principles on senior management responsibilities for BCM; embedding BCM into business-as-usual activities, incorporating sound practices, testing BCP regularly, completely and meaningfully; developing recovery strategies and setting RTO for criteria
Please refer to the URL below	SGX (Singapore Exchange)	Rules requiring SGX member firms to develop robust "Business Continuity Management (BCM)" arrangements

http://www.sgx.com/wps/wcm/connect/cp_en/site/press_room/news_releases/sgx+member+firms+implement+robust+business+continuity+arrangements+by+2010?presentationtemplate=design_lib/PT_Printer_Friendly

Standards

TITLE	AUTHORITY	SUMMARY
SS 540:20-08	SPRING Singapore (Singapore productivity and innovation)	Specifies requirements for setting up and managing an effective business continuity management system (BCMS)

Good Practice

TITLE	AUTHORITY	SUMMARY
BCI Good Practice Guidelines - 2008	BCI	Versions in both English and Mandarin.
MAS Consultation Paper	MAS	Guidelines to encourage

<p>on Business Continuity Planning (BCP) Guidelines (10 Jan 2003)</p>		<p>adoption of BCP practices by financial institutions in Singapore. Guidelines to help financial institutions to prepare to be aware by establishing a comprehensive business continuity plan</p>
<p>MAS Guidelines on Outsourcing – Section 6.6 BCM (Oct 2004)</p>	<p>MAS</p>	<p>Guidelines on ensuring BC preparedness is not compromised by outsourcing; taking steps to evaluate and satisfy itself that interdependency risk arising from the outsourcing arrangement can be adequately mitigated; and assurance on the functionality</p>

COUNTRY: SOUTH AFRICA

Legislation

TITLE	AUTHORITY	SUMMARY
Ministry for Provincial & local Government Disaster Management Act, 2002		Proposed national disaster management framework. Provides for an integrated and co-ordinated disaster management policy that focuses on preventing and reducing the risk of disasters, mitigating the severity of disasters and emergency preparedness.
Major Hazard Installation Regulations, 1993	Occupational Health & Safety	Talks about emergency plans (emergency plan" means a plan in writing which, on the basis of identified potential incidents at the installation, together with their consequences, describes how such incidents and their consequences should be dealt with.

Regulation

TITLE	AUTHORITY	SUMMARY
Public Finance Management Act, 1999 – Draft Treasury Relations		Unable to find anything specific to BC or DR ... "availability of financial information" was included ...
SAMOS and CLS Business Continuity Procedures – SA Reserve Bank	South African Reserve Bank National Payment System Department	Business Continuity Procedures for SA Reserve Bank and participants
King I Report 1994 King II Report – 2002	King Committee on Corporate Governance	This is a standard for good corporate governance which most companies in South Africa make reference to in their AFS and try to adhere to.

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
BCI Good Practice Guidelines - 2010	BCI	Printed and downloadable versions available.

COUNTRY: SOUTH KOREA (Republic of Korea)
Legislation

TITLE	AUTHORITY	SUMMARY
Disaster Mitigation Act	National Emergency Management Agency (NEMA)	To promote BCP and Disaster management for local companies

Regulation

TITLE	AUTHORITY	SUMMARY
Korea BCP	Foreign Financial Supervisory	Recovery of core business (bank, securities, futures) within 3 hours Need for proper capacity planning Appropriate access control to DR system Regular & ad hoc test requirement

Standards

TITLE	AUTHORITY	SUMMARY
KS A ISO/PAS22399	Korean Industrial Standards	Adopted and made as a Korean Industrial Standard from ISO 22399

Good Practice

TITLE	AUTHORITY	SUMMARY
BCI Good Practice Guidelines - 2008	BCI	Versions in both English and Korean available.

COUNTRY: SWITZERLAND
Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
FINMA Recommendations for BCM: Nov 2007	Swiss Financial Market Supervisory Authority	Overall BCM is not mandated but two elements BIA and BCM Strategy are binding as minimum standards under supervisory law.
SFBC 06/6	Swiss Federal Banking Commission (SFBC)	Supervision of Internal Control
SFBC 06/3	SFBC	Capital Adequacy for Operational Risk
SBA Self Regulation	Swiss Bankers Association	Self regulatory guidelines for BCM, supported by SFBC. These are based upon the Basel Joint Forum " High-Level Principles for Business Continuity"

Standard

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: THAILAND

Legislation

TITLE	AUTHORITY	SUMMARY
None		

Regulation

TITLE	AUTHORITY	SUMMARY
Thailand BCP	Bank of Thailand/Securities and Exchange Commission, Thailand	The FCC's network Reliability Interoperability Council provides best practices for business continuity and disaster recovery in the telecommunications industry (www.nric.org)

Standards

TITLE	AUTHORITY	SUMMARY
None		

Good Practice

TITLE	AUTHORITY	SUMMARY
None		

COUNTRY: UK

Legislation

TITLE	AUTHORITY	SUMMARY
Civil Contingencies Act (2004 & 2005)	UK Government	The CCA defines various categories of responders to manage incidents and mandates BCM for all category 1 providers. It provides the legal framework for the establishment of local resilience forums and delegates responsibility of BCM awareness to local authorities.
National Infrastructure	The Centre for the Protection of National Infrastructure (CPNI)	<p>CPNI provides information, personnel and physical security advice to the businesses and organisations which make up the UK's national infrastructure, helping to reduce its vulnerability to terrorism and other threats.</p> <p>It can call on resources from other government departments and agencies, including MI5, the Communications Electronics Security Group and other Government departments responsible for national infrastructure.</p>

Regulation

TITLE	AUTHORITY	SUMMARY
Business Continuity Practice Guide	UK Tripartite Authorities <ul style="list-style-type: none"> - Financial Services Authority (FSA) - HM Treasury - Bank of England 	Guidance on BCM requirements for regulated firms. The FSA base its BCM inspection regime on the 7 High Level principles from the Basel Joint Forum.

Standards

TITLE	AUTHORITY	SUMMARY
BS25999-1 : 2006 Code of Practice for Business Continuity management	British Standards Institution	Guidance and recommendations on setting up and managing a business continuity management programme
BS25999-2 : 2007 Specification for Business Continuity management	British Standards Institution	Specifies requirements for setting up and managing an effective business continuity management system (BCMS) to measure compliance and provide formal certification.
BS25777: 2008 IT Service Continuity	British Standards Institution	Guidelines and recommendations to ensure that IT systems and infrastructures can be recovered in a disaster
PD 25888 Business Recovery	British Standards Institution	Additional guidance in support of BS25999
PD 25666 Exercising BCM	British Standards Institution	Additional guidance in support of BS25999
PD 25111 Human Aspects of BCM	British Standards Institution	Additional guidance in support of BS25999
PD Work Group on Supply Chain Continuity	British Standards Institution	Additional guidance in support of BS25999
PAS 200 (Pending)	British Standards Institution	Publicly available specification for guidance on Crisis Management

Good Practice

TITLE	AUTHORITY	SUMMARY
BCI GPG 2010	The Business Continuity Institute	Establishes global guidelines for Business Continuity across the 6 professional practices in the BCM lifecycle.
Risk Management Standard, AIRMIC, ALARM, IRM: 2002	AIRMIC (Association of Insurance and Risk Managers) ALARM (National Forum for risk management in the public sector)	Establishes guidelines for Risk Management including <ul style="list-style-type: none"> • Risk Assessment • Risk Reporting • Risk Treatment
FSA BCM Staff Guide 2007	Financial Services Authority	Advice for FSA staff involved with BCM internally or within regulated firms

COUNTRY: USA

Legislation

TITLE	AUTHORITY	SUMMARY
California SB 1386 Security of Non-encrypted customer information (July 2003)	State of California	Bill requires all agencies, persons or businesses that conduct business in California that owns or licenses computerised data containing personal information to notify the owner or licensee of the information of any breach of security of the data
Computer Fraud and Abuse Act	FTC (Federal Trade Commission)	Makes it a federal offence to produce, buy, sell or transfer a credit card or other access devices that are counterfeit, forged, lost or stolen
Consumer Credit Protection Act (CCPA) of 1992 Section 2001 Title IX – Electronic Funds Transfer		Provides a basic framework establishing the rights, liabilities and responsibilities of participants in electronic fund transfer systems
Electronic Fund Transfer Act (EFTA)	OCC	Establishes the basic responsibilities, rights & liabilities of consumers and financial institutions who use electronic fund transfer services.
Fair Credit Reporting Act	FTC (Federal Trade Commission)	Ensures credit information is accurate and up to date
FDICIA – Federal Deposit Insurance Corporation Improvement Act of 1991	FDIC (Federal Deposit Insurance Company_	Requires all FDIC insured depository institutions with total assets of \$500 million or more to certify that there is effective functioning of their internal controls systems
Financial Institutions Reform, Recovery and Enforcement Act (FIRREA) of 1989; (P.L. 101-73 1989 HR 1278)	FIRREA	Policy allows regulators/examiners to impose civil penalties for violations or non compliance with regulations, laws, temporary agency orders or any breach of a written

		agreement between an agency and the institution.
FISMA: Federal Information Security management Act of 2002	FTC	Details requirements to Assess risk, determine levels of security necessary to protect such information, periodically test and evaluate information security controls and techniques etc.
Foreign Corrupt Practices Act 1977 (P.L 95-213)		Policy states that Directors and Officers can be held liable for “failure to enact standards of care” and should they fail to document their assessment processing determining not to develop a contingency plan.
Gramm-Leach-Bliley Act of 1999, section 501 (b) (PL 106-102 1999 S 900)	Public Law	Guidelines in this section address standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information
HIPAA (Health Insurance Portability and Accountability Act) Final Security Rule #7. Contingency Plan (164.308 (a) (7) (i))	GAO	Proposed contingency plan in effect with data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures and applications and data criticality analysis
Privacy Act of 1974 (SUSC552a)		Requires management to safeguard and to keep the information accurate and current to protect the individual
Sarbanes-Oxley Act of 2002 (PL 107-204 2002 HR 3763) – Section 404	PCAOB (Public Company Accounting Oversight Board)	Auditors are increasing scrutiny of all areas of internal control, including security and business continuity controls Potential for data loss (ability of identify and rebuild lost transactions and source documents)
Sarbanes-Oxley Act of	PCAOB	Issuers must disclose

2002 : Section 409		information on material changes in financial condition on a result basis.
Securities and Exchange Act, Sections 32(a) and (b)	SEC	Policy addresses criminal liability of Directors and officers for failure to protect computerised information/document process used to assess risks of information loss/exercise duty of care

Regulation

TITLE	AUTHORITY	SUMMARY
2002 ACH Rules Book	ACH (Federal Reserve's automated clearinghouse association).	Requires 6 year file retention on all ACH transactions. An ACH transaction is a batch-processed, value dated electronic funds transfer between originating and receiving financial institution
6 CFR 29	Code of Federal Regulations	Continuity of operations for critical infrastructure. Disclosure of critical information to the government
ANSI/ARMA 5-2003	American National Standards Institute	Sets requirements for establishing a vital records program by identifying and protecting vital records; assessing and analysing their vulnerability & determining the impact of their loss on the organisation
Bulletin R-67	Federal Home loan bank	Follows intent of BC177 which required documented, exercised and maintained recovery plans are required for all user environments and business functions
Business continuity planning committee best practice guidelines (Aug 2002)	SIA (Securities Industry Association)	Each firm should have in place a BC program
Federal Acquisition Regulation: Electronic Funds Transfer Final Rule	SEC	Addresses the collection of EFT information through the contract process for

		vendors providing goods and services to the Federal Government
FFIEC FIL 67-97/82-96	FFIEC (Federal Financial Institutions Examination Council)	Board of Directors is responsible for ensuring that a comprehensive business resumption and contingency plan has been implemented, to encompass distributed computing and external service bureaus
FFIEC Policy SP-5	FFIEC	Policy mandating corporate wide contingency planning, including the development of recovery alternatives for distributed processing and service bureau information processing
FRB (Federal Reserve Banks) SR 96-22	Board of Governors of the Federal Reserve System	Reviews and enforces the FFIEC's Interagency Supervisory Statement on Risk Management of Client/Server Systems SP-12
GFAO Supplier Requirements	GAO (Government Accountability Office)	Requirements for federal agencies to include the requirement for contingency plans in contracts with private sector organisations providing data processing services
Interagency Paper for Strengthening the Resilience of US Financial System (May 2003: Implementation in 2007)	FRB (Federal Reserve Bank) OCC (Office of the Comptroller of the Currency) SEC (Securities and Exchange Commission)	<p>During discussions about the lessons learned from September 11th, industry participants and others agreed that three business continuity objectives have special importance for all financial firms and the US financial system as a whole.</p> <ul style="list-style-type: none"> • Rapid recovery and timely resumption of critical operations following a wide-scale disruption • Rapid recovery and timely resumption of critical operations

		<p>following the loss or inaccessibility of staff in at least one major operating location</p> <ul style="list-style-type: none"> • A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible
IRS Procedure 91-59 (superseded IRS Procedure 86-19)	IRS (Internal Revenue Service)	<ul style="list-style-type: none"> • Legal requirements for computer records containing tax information • Requires off site protection and documentation of computer records maintaining tax information
JCAHO Accreditation Manual for Hospitals (1997)		Guidelines for information management established by JCAHO Standard Label IM.1.20 – The (organisation) plans for the continuity of its information management processes.
NASD Rule 108 (Sept 9, 02) and SR-NASD 2002-112 (March 10 2003) (Release No. 34-48503; File NO SR-NASD-2002-108)	NASD (North American Securities Dealers Association) / SEC	<p>Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption.</p> <p>Must update this plan in the event of any material change to the members' operations, structure.</p>
NASD Rule 3500: Emergency Preparedness Part 3510: Business Continuity Plans	NASD	<p>Requires business continuity plan addressing:</p> <ul style="list-style-type: none"> • Alternative communications between customers, firm and employees • Business constituent, bank and counter party impact

		<ul style="list-style-type: none"> • Regulatory reposting • Mission critical systems • Operational and financial
NASD Rule 3500: Emergency Preparedness Part 3520: Emergency Contact information	NASD	Rule 3520 requires NASD members to provide NASD with emergency contact information and to update information upon the occurrence of a material change. The Rule requires members to designate two emergency contact persons that NASD may contact in the emergency
NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan	CFTC (Commodity Futures Trading Commission)	Requires all National Futures Association members to establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant disruption.
NYSE Rule 446 : Business Continuity and Contingency Planning	NYSE (New York Stock Exchange)	Members and member organisations must develop and maintain a written business continuity and contingency plan establishing procedures to be followed in the event of an emergency or disruption. Yearly review must be conducted of the plan
OCC 2001-47. Third Party Relationships (Nov 1 2001)	OCC	Provides guidance to national banks on managing risks resulting from business relationships with third parties.
OSHA- Occupational Safety and Health Administration	OSHA (Occupational Safety & Health Administration)	Disasters preparedness. OSHA requires that all businesses with more than 10 employees have a written Emergency Contingency Plan (ECP). For businesses with 10 or less, a written plan is not mandated but recommended

Standards

TITLE	AUTHORITY	SUMMARY
PS-Prep	Department of Homeland Security and private sector.	<p>PS-Prep is a partnership between DHS and the private sector that enables private entities to receive emergency preparedness certification from a DHS accreditation system created in coordination with the private sector.</p> <p>The standards—developed by the National Fire Protection Association, the British Standards Institution and ASIS International—were published for public comment in the Federal Register in Oct. 2009. The adoption of the final standards was published in a Federal Register notice today following a series of regional public meetings and the incorporation of public comments.</p> <p>DHS will continue to accept comments on PS-Prep, the three adopted standards, and/or proposals to adopt any other similar standard that satisfies the target criteria of the December 2008 Federal Register notice which announced the program</p>
ASIS GDL BC 10 – 2004	ASIS International	Tool to allow organisations to consider the factors and steps necessary to prepare for a crisis (disaster or emergency) so that it can manage and survive the crisis and take appropriate actions to ensure its continued viability
NFPA Standard 1600 on	NFPA	Establishes minimum criteria

Disaster/Emergency Management and Business Continuity Programs		for disaster management for the private and public sectors in the development of a program for effective disaster mitigation, preparedness, response and recovery
ASIS SPC. 12009	ASIS	Guidance on addressing organisational resilience issues
ASIS/BSI Joint US Standard	ASIS/BSI	Detailed structure and guidance on business continuity planning
NYSE Rule 446	NYSE	Rules established by SEC/NYSE requiring members to create business continuity plans
P.L. 110-53 Title IX		Legislates voluntary implementation of business continuity plans and accreditation and certification of those plans by authorised third party organisations
NASD 3510/3520		Rules established by SEC/NASD requiring members to create business continuity plans and provide emergency contact information
NFPA 1600:2007 (2010 version in review phase)		American national standard for emergency management and business continuity, includes detailed guidance for BC
NIST SP 800-34		Detailed guidance and recommendations for IT disaster recovery
NIST SP 800-84		Detailed guidance and recommendations for planning and executing IT DR/BC plans and related activities.

Good Practice

TITLE	AUTHORITY	SUMMARY
COSO Enterprise Risk Management Framework (Sept 2004)	COSO (Committee of Sponsoring Organisations of the Treadway Commission)	Defines essential enterprise risk management components, discusses key

		ERM principles and concepts, suggests a common ERM language and provides clear direction & guidance for enterprise risk management
CTIA Telecommunication Industry BCM Standard and certification	CTIA (Cellular Telecommunications and Internet Association)	Plans to offer standard business continuity guidance to the communications industry
FEMA 141: Disaster Planning Guide for Business and Industry	FEMA (Federal Emergency Management Agency)	Designed to provide guidance for business and industry officials to respond and recover from disasters
FEMA Emergency Management Guide for Business and Industry	FEMA	A step by step approach to emergency planning, response and recovery for companies of all sizes
FFIEC BCP Handbook: Business Continuity Planning (May 2003) "IT Examination Handbook"	FFIEC	Emphasises that business continuity planning is about maintaining, resuming and recovering the whole business.
FFIEC FIL-81-2005 Information Technology Risk Management Program (IT-RMP) for conducting IT examinations	FDIC (Federal Deposit Insurance Corporation)	For conducting IT examinations of FDIC supervised financial institutions and cover practices for Risk Assessment, Operations Security & Risk Management, Audit and independent review
Homeland Security Strategy for Critical Infrastructure Protection in Financial Services Sector (may 2004)	FSSCC (Financial Services Sector Coordinating Council for Critical Infrastructure Protection)	Ensuring the resiliency of the nation to minimise the damage and expedite the recovery from attacks that do occur.
NFPA 111: Standard on Stored Electrical Energy Emergency and Standby Power Systems	NFPA (National Fire Protection Association)	Guideline of a step by step approach to emergency planning, response and recovery for companies
NFPA 232 : Standard on Protection of Records	NFPA	Standards for protection of business records, archives and record centres
NIST SP 800-34 Contingency Planning Guide	NIST (National Institute of Standards and Technology)	Details the fundamental planning principles necessary for developing an effective contingency capability. Contingency planning guidance includes

		preliminary planning, business impact analysis, alternative site selection and recovery strategies.
OCC 2003-18 : FFIEC (March 2003)	OCC	Information Technology Examination Handbook- Business Continuity Planning and supervision of Technology Service Providers Booklets
OCC 97-23: Corporate Business Resumption and Contingency Planning (May 16 1997)	OCC	
OCC 99-9: Infrastructure Threats from Cyber Terrorists (March 5 1999)	OCC	Identifies and raises awareness of vulnerabilities and threats of cyber terrorism to the financial services industry, including ensuring that these threats are taken into account when preparing and testing a disaster recovery/business contingency plan
Post 9-11 Crisis Communications, Best Practices for Crisis Planning Prevention and Continuous Improvement (June 2002)	Business Roundtable (The Southwestern Area Commerce & Industry Association of Connecticut)	This document is a toolkit to enable companies to develop a crisis communications plan that includes crisis preparation, prevention and continuous improvement
Supervision of Technology Service Providers Booklets (May 2003)	FFIEC	Business Continuity Planning, Supervision of Technology Service Provider Guidance, release by Federal Financial Regulators. The Business Continuity Planning booklet provides guidance and examination procedures to assist examiners in evaluating financial institutions and service provider risk management processes to ensure the availability of critical financial services
DRII/DRJ GAP		Detailed process level document that provides guidance,

		recommendations and checklists for developing business continuity programs.
FFIEC BC Handbook 2008		Guidance to financial institutions regarding the planning and implementation of BC plans and processes

COUNTRY: INTERNATIONAL

Legislation

TITLE	AUTHORITY	SUMMARY
Global		There is no global legislation for BCM or related subjects
European Union	EU Commission, Brussels	<p>The European Programme for Critical Infrastructure Protection ([EPCIP]) has been laid out in EU Directives by the Commission (e.g. EU COM (2006) 786 final). It has proposed a list of European critical infrastructures based upon inputs by its Member States.</p> <p>Each designated ECI will have to have an Operator Security Plan (OSP) covering the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures.</p>

Regulation

TITLE	AUTHORITY	SUMMARY
High Level Principles for Business Continuity	<p>Basel Joint Forum:</p> <ul style="list-style-type: none"> - Basel Committee on Banking Supervision - International Organisation of Securities Commissions (IOSCO) - International Association of Insurance Supervisors 	The principles that should be used internationally by financial regulators to access competence of financial organisations within their jurisdiction.

	Published by Bank of International Settlements, Basel in August 2006	
Basel II: new BASEL capital accord (April 2003)	Basel Committee on Banking Supervision	Addresses operational risk and defines it as “the risk of loss resulting from inadequate or failed internal processes, people & systems, or from external events

Standards

TITLE	AUTHORITY	SUMMARY
COBIT – Control Objectives for information & related technology 4.1 (May 2007)	IT Governance Institute Standards	Generally accepted information technology control objectives for information technology
ISO 9000	ISO (International Organisation for Standardisation)	<p>ISO 900:2000, Quality management systems – Fundamentals and vocabulary, covers the basics of what quality management systems are and also contains the core language of the SIO 9000 series of standards.</p> <p>Purpose is to determine elements of quality control systems, especially maintenance of records and verification standards. While business continuity planning is not required by statute, vendors report that records retention and data availability are issues with their customers and that they are specifically asked about their plans.</p>
ISO 9001	ISO	ISO 9001:2000 Quality management systems – Requirements is intended for use n any organisation which designs, develops, manufactures, installs and/or services any product or provides any form of service. It provides

		a number of requirements which an organisation needs to fulfil if it is to achieve customer satisfaction through consistent products and services which meet customer expectations. This is the only implementation for which third-party auditors may grant certifications.
ISO 9002, Quality assurance standard	ISO	Addresses risk management and continuity planning issues for compliance
ISO 9004 Quality management systems – Guidelines for performance improvement	ISO	ISO 9004:2000 Quality management systems – Guidelines for performance improvements – cover continual improvement. This gives you advice on what you could do to enhance a mature system. This standard very specifically states that it is not intended as a guide to implementation.
ITIL – IT Infrastructure Library	ITIL (IT Infrastructure Library)	Global standard in the area of service management. Contains comprehensive publicly accessible specialist documentation on the planning provision and support of IT services.
ISO 170XX Series		Series of international standards focusing on the processing of assessing and validating one's conformity to established standards
ISO 24762:2008		Standards for IT disaster recovery; developed based on requirements stated in ISO 27001 and ISO 27002 for information security
ISO 27001:2005		Standards for establishing an information security management system (isms), includes business continuity management
ISO 27002:2005		Guidance and recommendations for

		establishing an information security operating structure in an organisation, includes business continuity management
ISO PAS 22399: 2007	Code of Practice	Guidance for establishing incident response and continuity programs that cross over between public and private sectors (i.e. societal security).
ISO 22301 PENDING	Specification Standard	A planned ISO certification standard for Business Continuity Management that might become available in late 2011. It is similar but not identical to BS25999.

Good Practice

TITLE	AUTHORITY	SUMMARY
Ten Professional Practices for Business Continuity Professionals	DRII (Disaster Recovery Institute International)	Professional practice including developing business continuity management strategies and other contingency planning measures
BCI GPG 2010	BCI (Business Continuity Institute)	Global best practice
ISACA Doc G32		Provides audit guidance for assessing BC plans from the perspective of IT audit and control standards, such as CoBIT.