

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
AS/NZS 5050:2010 Business continuity -	Std	Standards Association of	Australia, New Zealand	Provides a generic guide for Business continuity - Managing disruption-related risk. It may be applied to a wide range of		Wat	document may be purchased; supersedes DR 09013; governance, risk and	http://infostore.saiglobal.com/store/details.aspx?ProductID=1409610	✓	✓	✓	✓	✓	✓	✓
20 Questions Directors Should Ask about Crisis Management	GP	The Risk Management and Governance Board (RMGB) of the Canadian Institute of Chartered Accountants (CICA)	Canada	This briefing describes how directors can become more aware of the potential for crisis and how they can contribute to crisis management. There are four sections of questions and suggestions on the elements that contribute to successful crisis management: responding to sudden crises, detecting early warning signals, responding to the early warning signals of potential crises, and learning from experience.	Jan-2008	Amb	ISBN 978-1-55385-329-9 1. Crisis management. I. Lindsay, Hugh, 1941- II. Canadian Institute of Chartered Accountants III. Title. IV. Title: Twenty questions directors should ask about crisis management. HD49.E55 2008 658.4'056 C2008-901283-6	https://www.cpacanada.ca/en/business-and-accounting-resources/strategy-risk-and-governance/strategy-development-and-implementation/publications/questions-for-directors-about-crisis-management	✓	✓	✓	✓	✓	✓	✓
2014 ACH Rules Online - Operating Rules &	Reg	ACH (Federal Reserve's	U.S.A.	Requires 6 year file retention on all ACH transactionsx		IAI	Login is required to access, but non-member logins are granted and given	http://www.achrulesonline.org/	✓						
Advisory on Business Continuity and Disaster Recovery Planning	GP	CFTC, SEC and FINRA	U.S.A.	The regulators encourage firms to consider implementing the best practices described, which the advisory groups into the following categories: (1) widespread disruption considerations, (2) alternative locations considerations,	Oct-2012	Enf	The CFTC, SEC, and FINRA have issued this advisory following their joint investigation into firms' business continuity and disaster recovery plans ("BCPs") in the wake of Hurricane Sandy.	http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/bcstaffadvisory081613.pdf	✓						
AFMA KRI Definitions & Guidelines	GP	Australian National Audit Office (ANAO)	Australia	Multiple publisked documents provided by the ANAO on the topic of business continuity, including: ANAO REPORT NO.6 OF 2014-2015 Business Continuity Management ANAO REPORT NO.9 OF 2003-2004 Business Continuity Management and Emergency Management in Centrelink ANAO REPORT NO.46 OF 2008-2009 Business Continuity Management and Emergency Management in Centrelink ANAO REPORT NO.53 OF 2002-2003 Business Continuity Management Follow-on Audit ANAO REPORT NO.16 OF 2008-2009 The Australian Taxation Office's Administration of Business Continuity Management SPEECH Published: Wednesday, February 23, 2000 Business Continuity Management: Opening remarks at a launch of a Better Practice Guide		Enf		https://www.anao.gov.au/search/site/Business%20Continuity%20Management	✓						
ANAO Better Practice Guide: Business Continuity Management - Building resilience in public sector entities. June 2009	Std	ANAO (Australian National Audit Office)	Australia, New Zealand	Business continuity management is an essential component of good public sector governance. It is part of an entity's overall approach to effective risk management, and should be closely aligned to the entity's incident management, emergency response management and IT disaster recovery. Successful business continuity management requires a commitment from the executive to raising awareness and implementing sound approaches to build resilience.	Jun-2009	Wat		http://www.anao.gov.au/BetterPracticeGuides/toc.html	✓	✓	✓	✓	✓	✓	✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
ANSI/ARMA 5-2010 Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records	Reg	ANSI (American National Standards Institute) / ARMA (Association of Records Managers and Administrators)	U.S.A.	This standard sets the requirement for establishment of a Vital Records Program. It includes clarification of what a Vital Records Program encompasses and the requirements for identifying and protecting vital records, assessing and analyzing their vulnerability, and determining the impact of their loss on the organization	2010	Enf	This site allows you to order documents at a specific price. Example: ANSI/ARMA 5-2010 - cost to purchase the PDF is \$50.00 US dollars.	http://webstore.ansi.org/RecordDetails.aspx?sku=ANSI%2FARMA+5-2010	✓	✓	✓	✓	✓	✓	✓
APRA - Prudential Standard CPS 232	Std	Australian Prudential	Australia	This Prudential Standard requires each APRA-regulated institution and Head of a group to implement a whole-of-business approach	Jul-2017	Enf		http://www.cpr.cba.gov.au/Assets/Uploads/Prudential%20Standards/Docs/CPS%20232%20Prudential%20CPS%20232.pdf	✓						
AS/NZS ISO 31000:2009 Risk management - Principles and guidelines	Std	Standards Association of Australia	Australia, New Zealand	Provides a generic guide for Risk management - Principles and guidelines. It may be applied to a wide range of activities or operations of any public, private or community enterprise, or group.	Nov-2009	Wat	document may be purchased Supersedes AS/NZS 4360:2004 , DR 09063 CP	http://infostore.saiglobal.com/Store/Details.aspx?ProductID=1378670	✓	✓	✓	✓	✓	✓	✓
AS/NZS ISO 31000:2009 Risk management—Principles and guidelines	Std	Standards Association of Australia	Australia, New Zealand	The AS/NZS ISO 31000:2009 provides the internationally accepted basis for best practice risk management. The standard is non-prescriptive or generic in its application which provides a methodology of managing risk which is applicable for all types of organisations including governments.		Wat	Supersedes AS/NZS 4360; 2004 Non-government employees may purchase a copy at purchase a copy of the 31000 from Standards Australia.	http://www.treasury.act.gov.au/actia/RMISO.htm	✓						
AS/NZS ISO/IEC 27001:2006 Information technology - Security techniques -	Std	Standards Association of Australia	Australia, New Zealand	Adopts ISO/IEC 27001:2006 to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). This Standard can be used in order to assess conformance by		Wat	Supersedes: AS/NZS 7799.2:2003 DR 06091 CP Superceded by AS ISO/IEC 27001:2015	http://infostore.saiglobal.com/Store/Details.aspx?productID=394887	✓						
ASIS American National Standard - Organizational Resilience: Security, Preparedness and	Std	ASIS SPC.1-2009	U.S.A.	This management system Standard (referred to as the "Standard") has the applicability in the private, not-for-profit, non-governmental, and public sector environments. It is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a	2009	Wat	Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard(ASIS SPC.1-2009); document may be purchased	https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1_2009_Item_No._1842.pdf	✓	✓	✓	✓	✓	✓	✓
B.C. Emergency Program Act	Reg	Ministry of Justice and Attorney General, Emergency Management British Columbia	Canada	Multi-agency hazard plans for B.C. are prepared and updated regularly by the Province to ensure an effective strategy is in place to address many possible types of emergencies and disasters. These plans foster cooperation among multiple organizations. They focus on public safety, infrastructure and property protection and management of the aftermath of events. British Columbia's comprehensive emergency management system promotes a coordinated and organized response to all	Aug-2017	Enf	The Provincial Emergency Program (PEP) is a division of the Ministry of Justice and Attorney General, Emergency Management British Columbia, Canada.	http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/oo_96111_01							
Banks Act, 1990 (94/1990)	Reg	South African Reserve Bank	South Africa	To provide for the regulation and supervision of the business of public companies taking deposits from the public; and to provide	Jan-2008	Wat	Banks Act, 1990 (as amended): Reproduced under Government Printer's	http://www.resbank.co.za/RegulationAndSupervision/BankSupervision/BankingRegulation/Pages/BanksAct.aspx	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category							
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	
Basel Committee on Banking Supervision - The Joint Forum - High-level principles for business continuity (August 2006)	Reg	Basel Committee on Banking Supervision	International	The high-level principles set out in this paper are intended to support international standard setting organisations and national financial authorities in their efforts to improve the resilience of financial systems to major operational disruptions.	Aug. 2006	Amb		http://it handbook.ffiec.gov/media/2211/ex_basel_high_princ_bc_a.pdf	✓							
Basel III: A global regulatory framework for more resilient banks and banking systems	Reg	Basel Committee on Banking Supervision	International	This document, together with the document Basel III: International framework for liquidity risk measurement, standards and monitoring, presents the Basel Committee's reforms to strengthen global capital and liquidity rules with the goal of promoting a more resilient banking sector. The objective of the reforms is to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source, thus reducing the risk of spillover from the financial sector to the real economy. This document sets out the rules text and timelines to implement the Basel III framework.	Jun-2011	Wat	In July 2013, the Federal Reserve Board finalized a rule to implement Basel III capital rules in the United States, a package of regulatory reforms developed by the BCBS. The comprehensive reform package is designed to help ensure that banks maintain strong capital positions that will enable them to continue lending to creditworthy households and businesses even after unforeseen losses and during severe economic downturns.	http://www.bis.org/publ/bcbst89.pdf	✓							
BCI Knowledge Bank - Regulations, Standards & Guidelines	Std	BCI (Business Continuity Institute)	International	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.	May-2012	Wat	Lists ISO 22301, BCI Good Practice Guidelines, AZ/NZS 5050:2010, and PAS200	http://www.thebci.org/index.php/regulations-legislation-standards-guidelines	✓	✓	✓	✓	✓	✓	✓	✓
Bill 198 (Canadian SOX)	Reg	Ontario Government	Canada	Bill 198 deals with virtually all of the same issues as Sarbanes-Oxley, including auditor independence, audit committee responsibilities, CEO and CFO accountability for financial reporting and internal controls, faster public disclosure, and stiffer penalties for illegal activities. The most significant difference between the US SOX and C-SOX: - Canadian companies do not have to submit an external auditor	Apr-2003	Enf	Shortly after the bill was passed, Canadian securities commissions issued three additional regulations: Multilateral Instrument (MI) 52-108, MI 52-109 and MI 52-110.	http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=1067	✓							
BS 65000 - Guidance on organizational resilience	Std	Business Standards Institute (BSI) (UK based)	International	The BS 65000 provides clarity and guidance, describing the nature of resilience and ways to build and enhance resilience in your organization. BS 65000 defines organizational resilience as the ability to anticipate, prepare for, respond and adapt to events – both sudden shocks and gradual change. That means being adaptable.	Nov-2014		BS 65000 is intended for anyone responsible for building resilience in their organizations. That includes risk managers and continuity practitioners and those involved with governance, emergency management and supply chain management.	http://shop.bsigroup.com/ProductDetail/?pid=00000000030258792	✓	✓	✓	✓	✓	✓	✓	✓
BSP Circular Letter (2001) - Business Continuity Plan	Reg	The Bangko Sentral ng Pilipinas (BSP) (central bank of the Republic of the Philippines)	Philippines	Requires a comprehensive and updated business continuity plan as an integral part of a the risk management process of all financial institutions. The overall goal of this business continuity plan must be to (1) ensure that there will be minimal disruption of bank operations (2) to minimize financial losses through lost	Oct-2001	Wat		http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=669	✓							

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
BSP Memorandum (2004) - MAB/NBFIs - Establishment of Back-Up Operation Centers and Data Recovery Sites	Reg	The Bangko Sentral ng Pilipinas (BSP) (central bank of the Republic of the Philippines)	Philippines	The board of directors of the concerned institution shall ensure that the institution's overall business continuity plans including the alternate crisis sites and data recovery sites are adequate, fully-capable and well-prepared to meet the contingencies arising from natural and man-made disasters in order to minimize potential business disruptions.	Jan-2004	Enf	Responsibilities on Business Continuity Subject : Back-up Operations Centers and Data Recovery Sites	http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=236	✓						
Business Continuity Management Audit/Assurance	GP	ISACA	International	Main subject areas of the DRI Professional Practices: - Project Initiation and Management - Risk Evaluation and Control	2011	Enf	DRI International established the industry's international first BCM methodology in 1997 when they	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity	✓	✓	✓	✓	✓	✓	✓
Business Continuity Management GOOD PRACTICE GUIDELINES 2013	Std	BCI (Business Continuity Institute)	International	The Good Practice Guidelines (GPG) are the independent body of knowledge for good Business Continuity practice worldwide. They represent current global thinking in good Business Continuity (BC) practice and now include terminology from ISO 22301:2012 Good Practice Guidelines (GPG) 2013 are therefore intended for use by practitioners, consultants, auditors and regulators with a working knowledge of the rationale for BCM and its basic principles.	2013	Wat	GPG available for BCI members and Non-Members. BCI Training and the BCI Certificate examination are both based on the Good Practice Guidelines. The Good Practice Guidelines are available either as a digital download or as a printed book. The GPG is available in English, Arabic, French, German, Italian, Korean, Spanish, US English. Chinese and Japanese will also be available soon.	http://www.thebci.org/index.php/resources/the-good-practice-guidelines	✓	✓	✓	✓	✓	✓	✓
Business Continuity Management Guideline	GP	Autorité des marchés financiers-AMF, Quebec	Canada	This guideline sets out the expectations of the AMF regarding business continuity management for financial institutions operated in Quebec	Apr-10	Amb	The principles of business continuity management proposed by the AMF are based on the frame of reference adopted by Québec's Ministère de la Sécurité publique, which proposes a collective approach to ensure consistency and	http://www.lautorite.qc.ca/files/pdf/reglementation/lignes-directrices-toutes-institutions/2010mars31-ld-gestion-continuee-en.pdf	✓						
Business Continuity Planning (Bank of Japan)	Std	BOJ (Bank of Japan)	Japan	The Bank develops and continually revises business continuity plans for functions such as circulation of banknotes and operation of payment and settlement systems, in order to carry out its responsibilities in times of disaster. The Bank trains its staff and conducts emergency drills on a regular basis to ensure a timely and appropriate response.		Enf		http://www.boj.or.jp/en/about/bcp/	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Business Continuity Planning Resources and Checklists Library	GP	Public Health and Safety, Government of Canada	Canada	Reference Library of links to Business Continuity Planning resources provided by different federal and provincial organizations in Canada	2013	Wat		http://www.phac-aspc.gc.ca/influenza/bcp-eng.php	✓	✓	✓	✓	✓	✓	✓
California SB 1386 - Security of Non-Encrypted Customer Information (July 1, 2003)	Reg	State of California	U.S.A.	Bill requires all agencies, persons or businesses that conduct business in California that owns or licenses computerized data containing personal information to notify the owner or licensee of the information of any breach of security of the data.	Jul-2003	Enf		http://www.legallarchiver.org/sb1386.htm	✓	✓	✓	✓	✓	✓	✓
CAN/CSA-Z 731-03	Std	CSA (Canadian Standards Association)	Canada	Canada's Emergency Preparedness and Response Standards for industry, specifically all organizations that manufacture, use, store, distribute, transport (by pipeline, road, rail, marine, or air), or dispose of dangerous substances.	Oct-2003		Available for purchase in .pdf or printed version	http://shop.csa.ca/en/canada/injury-prevention/z731-03-r2014/invt/z7019912003		✓	✓	✓	✓	✓	
CAN/CSA-Z1600 Emergency management and business continuity programs	Std	CSA (Canadian Standards Association)	Canada	First Canadian standard to include emergency management and business continuity planning for public and private organizations of all sizes. Establishes a common set of criteria for emergency management and business continuity programs Establishes the elements of a continuous improvement process to assess current programs or to develop, implement, and maintain a program that addresses the functions of prevention and mitigation, preparedness, response, and recovery (independently or in combinations).	2012	Enf	Bi-National Harmonization with NFPA 1600; Substantially the same in Technical Content /Scope/ Intent & Purpose Funded by Public Safety Canada; Existing NFPA 1600-based programs should meet the CSA Z1600 standard. The revised standard will be published in 2013 after public beta review in 2012	http://shop.csa.ca/en/canada/z1600-essentials-of-emergency-management-business-continuity-programs-for-health-care-facilities/invt/50066905	✓	✓	✓	✓	✓	✓	✓
Canadian Aviation Security Regulations, 2012 (SOR/2011-318)	Reg	Transport Canada	Canada	The operator of an aerodrome must develop and maintain a business continuity plan that, at a minimum, sets out how the operator will re-establish normal operations and comply with	2012	Enf	The operator of the aerodrome must make its business continuity plan available to the Minister on reasonable	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-318/page_39.html			✓				

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Circular Letter No. 9/30/DPNP - Risk Management in the Use of Information Technology by Commercial Banks (March 31st, 2008)	Reg	Bank Indonesia (Central Bank)	Indonesia	Requires BCP documentation and testing 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. Defines requirements for out-of-state disaster recovery (data) centers.	Mar-2008	Enf	Titled: "Circular Letter No. 9/30/DPNP - Risk Management in the Use of Information Technology by Commercial Banks"	http://www.bi.go.id/en/peraturan/pe-rbankan/Pages/se_093007.aspx PDF Link: http://www.bi.go.id/en/peraturan/pe-rbankan/Documents/86336e7d95464a3585d1e058fc2c11945e_093007.pdf	✓						
Circular to Licensed Corporations - "Business continuity planning against serious communicable diseases"	Std	Securities and Futures Commission of Hong Kong	Hong Kong	Business continuity plans in case of unexpected market conditions and failures. This section also directs to other regulator's business continuity plans.	Aug-2012	Enf	Crisis Management HKEx procedures & guidelines Public Health	http://www.sfc.hk/web/EN/published-resources/business-continuity/	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Civil Contingencies Act 2004 (c.36)	Reg	U.K. Parliament	U.K.	An Act to make provision about civil contingencies. Outlines and defines the duty to assess, plan and advise. – Local arrangements for civil protection - Duty to assess, plan and advise - Advice and assistance to business - Requires persons or bodies listed in the document to assess the risk of an emergency and maintain plans for the purpose of ensuring that if an emergency occurs that the persons or bodies are able to continue to	May-2012	Enf	Amends or repeals older Civil Defense Acts, Emergency Powers Acts, and other related Acts	http://www.legislation.gov.uk/ukpga/2004/36/contents	✓	✓	✓	✓	✓	✓	✓
Civil Defence Emergency Management Act 2002	Reg	Ministry of Civil Defence and Emergency Management	New Zealand	The purpose of this Act is to improve and promote the sustainable management of hazards in a way that contributes to the social, economic, cultural, and environmental well-being and safety of the public and also to the protection of property; and encourage and enable communities to achieve acceptable levels	Oct-2008	Wat	Public Act 2002 No 33	http://www.civildefence.govt.nz/assets/Uploads/publications/cdem-act-2002-introduction-brochure.pdf							
CMS Final CY 2016 Rule Regarding Business Continuity	Reg	CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group	U.S.A.	Centers for Medicare and Medicaid Services (CMS) Business Partners Systems Security Manual Appendix C: An Approach to Business Continuity and Contingency Planning This appendix has been renamed to Medicare Information Technology (IT) Systems Contingency Planning. The title change and associated updates within the appendix reflect a new focus on IT systems when developing and testing contingency	2002	Enf	The Centers for Medicare and Medicaid Services (CMS) requires that its business partners implement information technology (IT) systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters.	https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/downloads/R2SSM.pdf		✓					✓
CMS RMH VII 4.4 Contingency Plan Development	Reg	CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group	U.S.A.	Risk Management Handbook Volume II - Procedure 4.4 Contingency Plan Development The purpose of the Centers for Medicare & Medicaid Services (CMS) Contingency Plan (CP) Development Procedure is to provide CMS Business Owners, Information System Security Officers (ISSOs) and Contingency Plan Coordinators (CPCs) a systematic guide to coordinating.	2014	Enf		https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Vol-II-Procedure-4-4-Contingency-Plan-Development.html		✓					✓
COBIT-Control Objectives for information and related	Std	IT Governance Institute Standards	U.S.A.	COBIT is the the globally accepted framework that provides a comprehensive business view of the governance and management of enterprise IT (GEIT). In	Apr-2012	Enf	COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including	http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx	✓	✓	✓	✓	✓	✓	✓
Computer Fraud and Abuse Act	Reg	FTC (Federal Trade Commission)	U.S.A.	Makes it a federal offense to produce, buy, sell or transfer a credit card or other access devices that are counterfeit, forged, lost or stolen; or to produce, buy, sell, transfer or process equipment used to produce such fraudulent access devices.	Oct-2001	Enf	Section 1030. Fraud and related activity in connection with computers (EXAMPLES OF FINES/PUNISHMENT ASSOCIATED WITH THIS LAW) The	http://www.panix.com/~eck/computer-fraud-act.html	✓	✓	✓	✓	✓	✓	✓
Consumer Credit Protection Act (CCPA)	Reg		U.S.A.	The purpose of this title to provide a basic framework establishing the rights, liabilities, and responsibilities of	Dec-2011	IAI	Takes effect upon the expiration of eighteen months from the date of its	http://www.fdic.gov/regulations/laws/rules/6500-200.html	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
COSO Enterprise Risk Management Framework (September 2015)	Std	COSO (Committee of Sponsoring Organizations of the Treadway Commission)	U.S.A.	Defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.	2015	Enf	Guidance: - Governance & Operational Performance - Internal Controls - Enterprise Risk Mgmt	http://www.coso.org/guidance.htm http://www.coso.org/ERM.htm	✓	✓	✓	✓	✓	✓	✓
Criminal Code Act 1995 (consolidated as of 7 June 2010)	Reg	Australian Government	Australia	WIPO: World Intellectual Property Organization Establishing criminal penalties for officers and directors of organizations that experience a major disaster and fail to have a	Jun-2010	Enf	1995 act has had numerous revisions. Revision 12, Part 2.5 is referenced here Supersedes 1994 Code	http://www.wipo.int/wipolex/en/text.jsp?file_id=205531	✓	✓	✓	✓	✓	✓	✓
Croatian National Bank: Set of CNB Decisions	Reg	Croatian National Bank (CNB)	Croatia	Set of following CNB Decisions: Decision on adequate information system management Decision on risk management Decision on outsourcing Decision on amendments to the Decision on outsourcing	2010	Enf	Documents (EN/HR) available for download	https://www.hnb.hr/en/document-preview?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=527005&_101_type=document https://www.hnb.hr/documents/20182/525873/e-odluka-o-upravljanju-nizicima.pdf/883642e7-d14-429f-a878-d5dd1e30e429 https://www.hnb.hr/en/document-preview?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=527005&_101_type=document	✓						✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Croatian Sabor: Credit Institutions Act	Reg	Croatian National Bank (CNB)	Croatia	Credit Institutions Act	2013	Enf	Document (EN/HR) available for download	https://www.hnb.hr/en/-/zakon-o-kreditnim-institucijama	✓						
CTIA Emergency Preparedness/Disaster Recovery	Std	CTIA - 2013	U.S.A.	<ul style="list-style-type: none"> The CTIA (The Wireless Association) Policy & Initiatives Emergency Preparedness/Disaster Recovery Wireless Emergency Alerts (WEA) Cell on Wheels (COWS) Cell on Light Trucks (COLTS) Generator on Trailer (GOATS) 	Updates 2015	Wat	This certification and industry standard is in the planning phase. CTIA is currently (May 2005) meeting with industry leads to discuss the feasibility of the requirements and verification method.	http://www.ctia.org/policy-initiatives/policy-topics/emergency-preparedness-disaster-recovery						✓	
Derivatives Regulation, RRQ, c I-14.01	Reg	Regulations of Quebec	Canada	<p>DIVISION II.3</p> <p>11.23. Persons who apply for qualification under section 82 of the Act must demonstrate that they meet the obligations under sections 82.1 to 82.3 of the Act as well as the following obligations:</p> <p>...</p> <p>(3) they have developed an emergency and contingency plan to ensure business continuity.</p>	2014	Enf		http://canlii.ca/t/83z1							

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Disaster Management Act 2002	Reg	Ministry for Provincial & Local Government Disaster Management Act, 2002	South Africa	Proposed national disaster management framework. Provides for: · An integrated and coordinated disaster management policy that focuses on preventing and reducing the risk of disasters, mitigating the severity of disasters, emergency preparedness, rapid	Jan-2003	Enf		http://disaster.co.za/index.php?id=25	✓	✓	✓	✓	✓	✓	✓
Disaster Management Act No. 57 of 2002	Reg	Government Gazette; REPUBLIC OF SOUTH AFRICA	South Africa	Proposed national disaster management framework. One of the main reasons for South Africa's DM Act being recognised internationally as a model for disaster risk management best practice is that it gives effect to the concept of mainstreaming disaster risk reduction into development through legislation.	Jun-1905	Enf	A draft bill including amendments to the Disaster Management Act is expected to be presented to Parliament in 2013.	https://www.westerncape.gov.za/Text/2004/10/a57-02.pdf					✓		
Disaster Management Act; 09-10-2015) - South Africa	Reg	Department of Labour (Republic of South Africa)	South Africa	Disaster Management Act (2002) – an integrated and coordinated disaster management policy that focuses on preventing or reducing the risk of disasters, mitigating the severity of disasters, emergency preparedness, rapid and effective response to disasters and post-disaster recovery; the establishment of national, provincial and municipal disaster management centres and disaster management volunteers.	Jul-1905	Enf	Regulation Gazette No. 7122 Vol. 433 Pretoria 30 July 2001 No. 22506 Any person who contravenes or fails to comply with any provision of regulations ... shall be guilty of an offence and on conviction be liable to a fine or to imprisonment for a period of 12 months and, in the case of a continuous offence, to an additional time of ... or	www.gov.za http://www.gov.za/speeches/statement-occasion-disaster-management-institute-southern-africa-held-mosselbay-9-september http://disaster.co.za/index.php?id=25	✓	✓	✓	✓	✓	✓	✓
Draft Malaysian Standard 2- Business Continuity Framework - 2006	Reg	BNM - Bank Malaysia Central Bank	Malaysia	This Malaysian Standard Online was developed by the Working Group on Business Continuity Management under the authority of the Information Technology, Telecommunication and Multimedia Industry Standards Committee.	2007	Enf		http://www.msonline.gov.my/catalog.php file:///C:/Users/wmyers/Downloads/MS-10702007PRE.pdf	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
DRI International "Ten Professional Practices for Business Continuity Professionals"	GP	DRII (Disaster Recovery Institute International)	International	Professional practice letters include developing business continuity management strategies and other contingency planning.	Sep-2013	Wat		https://www.drii.org/certification/professionalprac.php	✓	✓	✓	✓	✓	✓	✓
DRJ GAP Report	Std	DRJ Editorial Advisory Board	International	DRII/BCI Professional Practice Narrative - Establish the need for a Business Continuity Plan (BCP), including obtaining management support and organizing and managing requirements; identifying planning team(s) and action plans; and developing project management and documentation requirements	Mar-2015		Best Practices will be compiled from submittals by experienced Business Continuity Professionals from the public and private sectors, as well as user groups and/or related organizations, in regards to a cross walk of the the industry standards.	http://www.drj.com/GAP/gap.pdf	✓	✓	✓	✓	✓	✓	✓
Earthquake Planning for Business	GP	Emergency Preparedness for Industry and Commerce Council	Canada	This guide is meant to provide practical and reliable earthquake preparedness, response and recovery information for businesses in British Columbia. The guidelines are intended to equip any business owners, managers, supervisors	Nov-2013	Amb	Developed with the assistance from Institute for Catastrophic Loss Reduction and their work towards reducing the risk of earthquake damage in Canada.	http://www.epicc.org/uploadfiles/documents/EPICC%20EARTHQUAKE%20PLANNING%20Nov%2020%202013%20Complete-2.pdf	✓		✓		✓	✓	✓
e-CFR Part 27: Protected Critical Infrastructure Information (as of 03/17/14)	Reg	e-CFR (Electronic Code of Federal Regulations)	U.S.A.	· U.S. Government Publishing Office · Continuity of operations for Critical Infrastructure · Enhance security and resiliency of chemical facilities.	Sep-2015	Wat	The purpose of this part is to enhance the security of our Nation by furthering the mission of the Department as provided in 6 U.S.C. §111(b)(1) and by lowering the risk posed by certain chemical facilities.	http://www.ecfr.gov/cgi-bin/text-idx?SID=a22236216120cb8f2ebc8f7888f44d25&mc=true&node=pt6.1.27&rgn=div5#se6.1.27_1100					✓		
e-CFR Part 29: Protected Critical Infrastructure Information (as of 09/17/2015)	Reg	e-CFR (Electronic Code of Federal Regulations)	U.S.A.	· Continuity of operations for Critical Infrastructure · Disclosure of critical information to the government	Sep-2015	Wat	Uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CI) voluntarily submitted to the Department of Homeland Security (DHS). Title II, Subtitle B, of the	http://www.ecfr.gov/cgi-bin/text-idx?SID=a22236216120cb8f2ebc8f7888f44d25&mc=true&node=pt6.1.29&rgn=div5	✓	✓	✓	✓	✓	✓	✓
Electronic Fund Transfer Act (EFTA)	Reg	OCC	U.S.A.	Business Continuity Planning Booklet Appendix J Update to FFIEC IT Examination Handbook Series. Numerous handbooks are available.	Feb-2015	IAI	[Codified to 15 U.S.C. 1693] effective July 21, 2010	https://www.federalreserve.gov/boariddocs/caletters/2008/0807/0807_attachment.pdf	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Emergency Management Act	Reg	Senate and House of Commons of Canada	Canada	Requires the Minister of Public Safety in Gov.Canada to: establishing policies and programs for the preparation of emergency management plans; control emergency management plans prepared by federal entities; coordinating the federal response to an emergency;	2007	Enf		http://laws-lois.justice.gc.ca/eng/acts/E-4.56/page-1.html							
Emergency Management and Civil Protection Act (EMPCA)	Reg		Canada	Under Provincial legislation, the Emergency Management and Civil Protection Act (EMPCA) , every municipality in Ontario is required to have an Emergency Management Program.	2006	Enf	This Act amended the Emergency Management Act, Employment Standards Act, and Workplace Safety and Insurance Act in order to expand the scope of power provided to the Lieutenant Governor in Council and the Premier to deal with emergencies in Ontario.	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90e09_e.htm							
Emergency Management Planning Guide	GP	Public Safety Canada	Canada	The Emergency Management Planning Guide supports federal institutions in meeting their responsibilities under the Emergency Management Act (2010-2011) to prepare and maintain mandate-specific emergency management plans.			The Guide provides step-by-step instructions of the planning process across the four pillars of Emergency Management Planning: mitigation/prevention; preparedness; response and recovery.	http://www.publicsafety.gc.ca/cnt/rs/rcs/pblctns/mrgnc-mngmnt-pnng/index-eng.aspx							
ERCB Directive 071	Reg	Energy Resources Conservation Board /ERCB	Canada	The ERCB's Directive 071: Emergency Preparedness and Response Requirements for the Upstream Petroleum Industry details emergency preparedness and response requirements that apply to the production, drilling, transportation, and processing of petroleum. It sets out additional requirements specific to sour gas	2009	Enf	The Energy Resources Conservation Board (ERCB) has a stringent regulatory framework that is governed by principles aimed at protecting the public and environment from harm through	http://www.ercb.ca/regulations-and-directives/directives/directive071							
Fair Credit Reporting Act	Reg	FTC (Federal Trade Commission)	U.S.A.	<ul style="list-style-type: none"> Ensures credit information is accurate and up-to-date Designed to promote accuracy and ensure the privacy of the information used in consumer reports 	Jan-2014	IAI	<ul style="list-style-type: none"> Civil penalty of not more than \$2,500 per violation State action of damages of not more than \$1,000 for each willful or negligent violation 	http://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting	✓						
FDICIA –Federal Deposit Insurance Corporation Improvement Act of 1991	Reg	FDIC (Federal Deposit Insurance Corporation)	U.S.A.	Requires at the beginning of the year that all FDIC-insured depository institutions with total assets of \$500 million or more certify that there is effective functioning of their internal controls systems.	Dec-1991	Enf	Last updated December 3, 2009	http://www.fdic.gov/regulations/laws/rules/8000-2400.html	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Federal Acquisition Regulation; Electronic Funds Transfer Final Rule	Reg	SEC	U.S.A.	Addresses the collection of EFT information through the contract process for vendors providing goods and services to the Federal Government	Mar-1999	Enf	Agencies: Department of Defense (DoD), General Service Administration (GSA), and National Aeronautics and Space Administration (NASA).	http://www.fms.treas.gov/eft/regulations/efeft.txt	✓	✓	✓	✓	✓	✓	✓
Federal Continuity Directives (FCDs)	Std	FEMA	U.S.A.	Federal Continuity was developed as a repository of information to guide governmental continuity planning efforts and to share information with private sector stakeholders about the importance of planning. The site provides an overarching framework for US Federal Agencies to develop and deploy actionable continuity strategies. Here you will find descriptions,	May-2013	Wat	Federal Continuity Directives (FCD) 1 and FCD 2 as they are HUGE in the Federal Government (they are the Executive Branch's "COOP Bibles" – 1 being the "what", and 2 being the "how").	http://www.fema.gov/guidance-directives	✓	✓	✓	✓	✓	✓	✓
FEMA 141: Emergency Management Guide for Business & Industry	Std	FEMA	U.S.A.	Designed to provide guidance for business and industry officials to respond and recover from disasters.	Oct-1993	Wat	Links to pdf or text version.	http://www.fema.gov/media-library/assets/documents/3412	✓	✓	✓	✓	✓	✓	✓
FFIEC BCP Handbook: Business Continuity Planning (May 2003) "IT Examination Handbook"	Reg	FFIEC	U.S.A.	- Emphasizes that Business Continuity planning is about maintaining, resuming and recovering the whole Business - planning should occur for a BCP - Business Impact Analysis and Risk assessment are encouraged as the foundation of an effective BCP - Testing	Mar-2008	Enf	Ineffective or incomplete BC plans may lead to qualified examination reports and loss of trust by regulators and financial market	http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/introduction.aspx http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf	✓	✓	✓	✓	✓	✓	✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
File 172-A000-73- 24 April 2002	Reg	National Energy Board	Canada	An Emergency Response Plan (ERP) is required for all oil and gas operations under the jurisdiction of National Energy Board	2002	Enf	As part of its Emergency Management Program, the NEB evaluates the effectiveness of a company's emergency response plans, spill contingency plans, and spill response exercises.	https://www.neb-one.gc.ca/bts/ctr/g/gnbg/prcssngplnt/2002-04-24mr/gncprprdrndssrsps-eng.pdf							
Financial Conduct Authority Handbook	Std	Financial Conduct Authority (FCA)	U.S.A.	REC 3.16 The purpose of REC 3.16 is to ensure that the FSA receives a copy of the UK recognised body's plans and arrangements for ensuring business continuity if there are major problems with its computer systems. External events and other changes (SYSC 13.8)Unexpected changes and business continuity management SYSC 3.2.19 G provides high level guidance on business continuity.	Mar-2013		Breaching a Principle makes a firm liable to disciplinary sanctions. In determining whether a Principle has been breached it is necessary to look to the standard of conduct required by the Principle in question. Under each of the Principles the onus will be on the FCA to show that a firm has been at fault in some way.	https://www.handbook.fca.org.uk/handbook/	✓						
Financial Institutions Reform, Recovery, and Enforcement Act- (FIRREA) of 1989; (P.L. 101-73 1989 HR 1278)	Reg		U.S.A.	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. (pronounced "fie-ree-ah") Federal legislation passed in 1989 in response to the banking and savings and loan crisis, the FDIC bailout, and the bankruptcy of the Federal Savings and Loan Insurance Corporation (FSLIC). It reorganized much of the oversight and regulatory framework for financial institutions and created the Resolution Trust Corporation (now defunct) to receive and liquidate assets from	Jun-2012	IAI	Whoever violates any provision of law to which this section is made applicable by subsection (c) of this section shall be subject to a civil penalty in an amount assessed by the court in a civil action under this section. (b) MAXIMUM AMOUNT OF PENALTY-- (1) GENERALLY-- The amount of the civil penalty shall not exceed \$1,000,000. (2) SPECIAL RULE FOR CONTINUING	http://www.fdic.gov/regulations/laws/rules/8000-3100.html	✓						
FINRA Rule 4370	Reg	Financial Industry Regulatory Authority (FINRA)	U.S.A.	Each Member must create and maintain a written business continuity plan, that must at a minimum, address: (1) Data back-up and recovery (hard copy and electronic); (2) All mission critical systems; (3) Financial and operational assessments;	2009	Enf	Members of FINRA must produce and maintain Business Continuity Plans. Plans must be made available immediately upon request of the FINRA staff. The FINRA rule 4370 is the successor to the	http://finra.complanet.com/en/display/display.html?rbid=2403&element_id=8625	✓						
FINRA Rule 4370 - emergency preparedness rule	Std		U.S.A.	Rule 4370—FINRA's emergency preparedness rule—requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information. This page provides general information related to BCPs for securities firms. Educational info:	Dec-2009	Enf	Replaces NYSE Rule 446. The NYSE, along with NASD, has adopted FINRA Rule 4370. Education	http://www.finra.org/industry/issues/BusinessContinuity/ http://finra.complanet.com/en/display/display_main.html?rbid=2403&element_id=8625	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
FISMA: Federal Information Security Management Act of 2002	Reg	Federal Trade Commission (FTC)	U.S.A.	Title III of the E-Government Act (Public Law 107-347, passed in 2002) entitled the Federal Information Security Management Act (FISMA) and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.	Jan-2003	Enf	May apply to organizations and institutions communicating with, performing work for, on behalf of a federal agency.	http://csrc.nist.gov/groups/SMA/fisma/overview.html https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002	✓	✓	✓	✓	✓	✓	✓
FRB (Federal Reserve Banks) SR 13-1 / CA 13-1 (extends SR 03-5)	Reg	Board of Governors of the Federal Reserve System	U.S.A.	SR 13-1 guidance explains changes over the past several years in banking regulations related to auditor independence and limitations placed on the external auditor. This supplemental policy statement builds upon the 2003 Policy Statement SR 03-5, which remains in effect, and follows the same organizational structure, with a new section entitled "Enhanced Internal Audit Practices" and updates to Parts I-IV of the 2003 Policy Statement. (Extends: Amended Interagency Guidance on the Internal Audit Function and its Outsourcing SR 03-5) (Supersede: Outsourcing of Information and Transaction Processing Cross Reference: SR letter 97-35)	Jan-2013		Reserve Banks are asked to distribute this supplemental guidance to supervised institutions with greater than \$10 billion in total consolidated assets, including state member banks, domestic bank and savings and loan holding companies, and U.S. operations of foreign banking organizations, as well as to their supervisory and examination staff, as appropriate.	http://www.federalreserve.gov/bankinforeg/srletters/sr1301a1.pdf	✓						
FRB (Federal Reserve Banks) SR 13-19 / CA 13-21	Reg	Board of Governors of the Federal Reserve System	U.S.A.	SR 13-19 Guidance on Managing Outsourcing Risk assists financial institutions in understanding and managing the risks associated with outsourcing a bank activity to a service provider to perform that activity, and include Business Continuity and Contingency considerations. This Federal Reserve guidance builds upon the FFIEC Outsourcing Technology Services Booklet (2004) that addresses outsourced information technology services and remains in effect.	Dec-2013		Guidance applies to all financial institutions supervised by the Federal Reserve, including those with \$10 billion or less in consolidated assets. It supplements existing guidance on technology service provider (TSP) risk and applies to service provider relationships where business functions or activities are outsourced. This Guidance is cross-referenced with SR Letter 13-1/CA 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its	http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm	✓						
Gramm-Leach-Bliley Act of 1999, section 501 (b): (P.L. 106-102 1999 S 900)	Reg	Public Law	U.S.A.	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.	Nov-1999	Enf	Effective July 1, 2001; GLB compliance is mandatory; whether a financial institution discloses non-public information or not, there must be a policy in place to protect the information	http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act http://www.ffiec.gov/exam/InfoBase/documents/02-con-	✓						
HIPAA 164.308(a)(7)(i)	Reg	U.S. Department of Health & Human Services	U.S.A.	The HIPAA Security Rule 164.308(a)(7)(i) identifies Contingency Plan as a standard under Administrative Safeguards. HIPAA Contingency plans address the "availability" security principle. The availability principle addresses threats related to business disruption –so that authorized individuals have access to vital systems and information when required.	2013	Enf	Also see: https://www.healthit.gov/safer/guide/sgo03/practice/cpi0p/hipaa	https://www.law.cornell.edu/cfr/text/45/164.308		✓					✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link	Infrastructure Category							
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	
HIPAA Security Requirements	Reg	U.S. Department of Health & Human Services	U.S.A.	Security standards for certain health information. These standards, known as the HIPAA Security Rule.	2013	Enf		http://www.hhs.gov/hipaa/for-professionals/security/index.html		✓						✓
IIROC Rule 17.16 - Business Continuity Plan Requirement	Reg	Investment Industry Regulatory Organization of Canada	Canada	Every Dealer Member shall establish and maintain a business continuity plan identifying the necessary procedures to be undertaken during an emergency or significant business disruption. Such procedures shall be reasonably designed to enable the Dealer Member to stay in business in the event of a future significant business disruption in order to meet obligations to its customers and capital markets counterparts and shall be	Jun-1905	Enf	Following FINRA 4370 Rule The purpose of the rule is to require each 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	http://www.iiroc.ca/industry/member-resources/Pages/Business-Continuity.aspx	✓							
Interagency Paper for Strengthening the Resilience of US Financial System (May 2003; Implementation in 2007)	Reg	FRB (Federal Reserve Bank) OCC (Office of the Comptroller of the Currency) SEC (Securities and Exchange	U.S.A.	During discussions about the lessons learned from September 11, industry participants and others agreed that three business continuity objectives have special importance for all financial firms and the U.S. financial system as a whole: Rapid recovery and timely resumption of critical operations following a wide-scale disruption;	Sep-2002	Enf	For Market Utilities and Core Clearing and Settlement Agencies, goal to meet objectives is end of 2004. For Significant Role Firms, the goal is no later than 2006.	http://www.sec.gov/news/studies/34-47638.htm	✓							
IRS Procedure 91-59 (Superseded IRS Procedure 86-19)	Reg	IRS (Internal Revenue Service)	U.S.A.	o Provides the basic requirements to those institutions that utilize computerized Records o requirements for computer records containing tax information.H22 o Requires off-site protection and documentation of computer records maintaining tax information o The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841	Dec-1997	IAI	See section 6 through 9 of this website	http://www.irs.gov/pub/irs-drop/rp-98-25.pdf	✓	✓	✓	✓	✓	✓	✓	✓
ISO 22301 Business Continuity Management	Std	ISO	International	ISO 22301 is the new international standard for business continuity management. It has been created in response to strong international interest in the original British Standard BS 25999-2 and other regional standards. And if you meet the requirements to gain certification, your organization will be recognized globally.	May-2012	Wat	document available for purchase	http://www.iso.org/iso/catalogue_detail?csnumber=50038	✓	✓	✓	✓	✓	✓	✓	✓
ISO 9000	Std	ISO	International	ISO 9000:2000, Quality management systems - Fundamentals and vocabulary. covers the basics of what quality management systems are and also contains the core language of the ISO 9000 series of standards. Purpose is to determine elements of quality control systems,	Dec-2011	Wat		http://en.wikipedia.org/wiki/ISO_9000					✓			

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category							
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	
ISO 9001	Std	ISO	International	ISO 9001:2000 Quality management systems - Requirements is intended for use in any organization which designs, develops, manufactures, installs and/or services any product or provides any form of service. It provides a number of requirements which an organization needs to fulfill 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.	Dec-2011	Wat		http://en.wikipedia.org/wiki/ISO_9001						✓		
ISO 9002, Quality assurance standard,	Std	ISO	International	Addresses risk management and continuity planning issues for compliance.	Dec-2011	Wat	previous members of the ISO 9000 series 9002 and 9003 have been integrated into 9001	http://en.wikipedia.org/wiki/ISO_9001						✓		
ISO 9004 Quality management systems - Guidelines for performance improvement	Std	ISO	International	ISO 9004:2000 Quality management systems - Guidelines for performance improvements. covers 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	Dec-2011	Wat	Revised by ISO 9004:2009 http://www.iso.org/iso/catalogue_detail?csnumber=41014	http://en.wikipedia.org/wiki/ISO_9004						✓		
ISO Guide 73:2009	GP	ISO	International	Risk management – Vocabulary	Dec-2013	Wat	document available for purchase	http://www.iso.org/iso/catalogue_detail?csnumber=44651						✓		
ISO/IEC 27002:2005	Std	ISO (International Organization for Standardization)	International	the standard contains the following twelve main sections 4. Risk assessment 5. Security policy – management direction 6. Organization of information security – governance of information security 7. Asset management – inventory and classification of information assets 8. Human resources security – security aspects for employees joining, moving and leaving an organization 9. Physical and environmental security – protection of the computer facilities 10. Communications and operations management – management of technical security controls in systems and networks 11. Access control – restriction of access rights to networks, systems, applications, functions and data 12. Information systems acquisition, development and maintenance – building security into applications 13. Information security incident management – anticipating and responding appropriately to information security breaches 14. Business continuity management – protecting, maintaining and recovering business-critical processes and systems 15. Compliance – ensuring conformance with information security	2013	Wat	ISO/IEC 17799:2005: It has subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled Information technology - Security techniques - Code of practice for information security management	http://en.wikipedia.org/wiki/ISO_17799						✓		
ISO/IEC 27005:2008	Std	ISO	International	Continuation of ISO 27000 series standard The purpose of ISO/IEC 27005 is to provide guidelines for information security risk management	2011	Wat	Published June, 2008	http://www.iso27001security.com/html/27005.html http://www.27000.org/	✓	✓	✓	✓	✓	✓	✓	✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
ISO/IEC 31010:2009	GP	ISO	International	Risk management -- Risk assessment techniques	Sep-2015	Wat	document available for purchase	http://en.wikipedia.org/wiki/ISO/IEC_31010					✓		
IT Security Guidelines - G3	Std	Information Technology Services Department - The Government of the Hong Kong Special Administrative	Hong Kong	Introduces general concepts relating to Information Technology Security and elaborates interpretations on the Baseline IT Security Policy. It also provides readers some guidelines and considerations in defining security requirements.	Dec-2013		In this document, government bureau and departments are suggested to consider implementing a BCP/DR as part of business planning. http://www.ogcio.gov.hk/en/information security/policy_and_guidelines/	http://www.ogcio.gov.hk/en/information security/policy_and_guidelines/doc/g3_pub.pdf							
ITIL- IT Infrastructure Library	Std	ITIL (IT Infrastructure Library)	U.S.A.	Global standard in the area of service management. ITIL® (IT Infrastructure Library®) is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. Contains comprehensive publicly accessible specialist documentation on the planning, provision and support of IT services	Aug-2016	Wat		http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library	✓	✓	✓	✓	✓	✓	✓
JCAHO 2010 Hospital Accreditation Standards	GP	Joint Commission on Accreditation of Healthcare Organizations (JCAHO)	U.S.A.	Guidelines for information management established by JCAHO Standard Label: IM.1.20 - The [organization] plans for the continuity of its information management processes.	Mar-2014	Enf		http://www.jointcommission.org/standards_information/joint_commission_requirements.aspx		✓					

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category							
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	
Joint Commission Emergency Management (EM)	GP	Joint Commission	U.S.A.	The Joint Commission's Emergency Management portal. We are launching this portal to provide a valuable source of information from The Joint Commission enterprise and other healthcare organizations related to the topic of Emergency Management. Our goal is to create informed and empowered citizens by bringing relevant and timely information and resources to our community.	2016		The Joint Commission was formerly the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and previous to that the Joint Commission on Accreditation of Hospitals (JCAH).	https://www.jointcommission.org/emergency_management.aspx		✓						
King I Report - 1994 King II Report - 2002 King III 2009	Std	King Committee on Corporate Governance	South Africa	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.	Jun-2016	Wat	The King Committee on Corporate Governance, formed in 1993 by the Institute of Directors in Southern Africa (IoD) was established to investigate the role of boards of directors in South African firms.[1] Chaired by businessman and former judge Mervyn E. King, the committee included Phillip Armstrong,	http://en.wikipedia.org/wiki/King_Committee	✓	✓	✓	✓	✓	✓	✓	
Major Hazard Installations Regulations (2001) - South Africa	Reg	Department of Labour (Republic of South Africa)	South Africa	Major Hazard Installations Regulations [PDF] – regulates employer responsibility for the health and safety of workers as well as the public in or in the vicinity of the workplace.	Jul-2001	Enf	Link is to the South African Legal Information Institute, SAFII http://www.saflii.org/za/legis/consol_reg/ohasa8501993rangnr692716/ Regulation Gazette No. 7122 Vol. 433 Pretoria 30 July 2001 No. 22506	http://www.saflii.org/za/legis/consol_reg/ohasa8501993rangnr692716.pdf	✓	✓	✓	✓	✓	✓	✓	
Malaysia Business Continuity Management Framework 2007	Reg	BNM - Bank Malaysia Central Bank	Malaysia	This Malaysian Standard describes the structured process for developing a Business Continuity Management (BCM) framework. This framework is applicable to any organisation in any sector or industry. This Malaysian Standard describes the structured process for developing a Business Continuity Management (BCM)	Aug-2007	Enf		http://www.msonline.gov.my/download_file.php?file=14038&source=production	✓							
Management, Supervision and Internal Control Guidelines ("The Internal Control Guidelines") For	Std	Securities and Futures Commission of Hong Kong	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	Apr-2013		In section 36 under operational risk: An effective business continuity plan appropriate to the size of the firm is implemented to ensure that the firm is protected from the risk of interruption to its business continuity. Key processes in	Copies of the Guidelines are available at the SFC. They can also be found on the SFC's website at http://www.sfc.hk/sfc/html/EN/	✓							
MAS Business Continuity Management Guidelines (June 2003)	Reg	MAS (Monetary Authority of Singapore)	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 crit	Jun-2003	Enf		http://www.mas.gov.sg/regulations-and-financial-stability/regulations-guidance-and-licensing/securities-futures-and-funds-management/guidelines/2004/business-continuity-management	✓							

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
MAS Guidelines on Outsourcing - Section 6.6 BCM (Oct 2004)	Std	MAS (Monetary Authority of Singapore)	Singapore	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 such that the institution remains able to conduct its business with integrity and competence in the event of disruption, or unexpected termination of the outsourcing or liquidation of the service provider.	2005	Enf	... Response to Feedback on Consultation Paper on Business Continuity Management. (PDF, 84.5KB). Download PDF(84.55 KB). Guidelines on Outsourcing. (PDF, 80.2KB).	http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines.pdf	✓						
MAS Technical Reference for business continuity management (BCM) Replaced by SS ISO 22301:2012 (Replaced by SS 540:2008)	Std	MAS (Monetary Authority of Singapore)	Singapore	Specifies the requirements for organisations intending to build competence, capacity, resilience and readiness to respond to and recover from events which threaten to disrupt normal business operations and activities. Stipulates the requirements to attain and maintain readiness to deal with risks and risk events faced by organisations due to the nature of their businesses, external environment or regulatory requirements.	2012			https://www.singaporestandardseshop.sg/product/product.aspx?id=082e0fce-df3e-420d-9c1a-b30ef4be33e7	✓						
MR-0056: Member Regulation Notice - Business Continuity Planning	Reg	Mutual Fund Dealers Association of Canada	Canada	Provides guidance to Members regarding the development and implementation of business continuity plans.	2006	Enf		http://www.mfda.ca/regulation/notifications/MR-0056.pdf	✓						
MS 1970:2007 BUSINESS CONTINUITY MANAGEMENT FRAMEWORK	Std	MALAYSIAN STANDARD	Malaysia		2007	Enf		http://www.msonline.gov.my/catalog.php?score=checked&istc_id=74	✓	✓	✓	✓	✓	✓	✓
NASD Rule 108 (Sept 9, 02) and SR-NASD-2002-112 (March 10, 03) (Release No. 34-48503; File No. SR-NASD-2002-108)	Reg	NASD (North American Securities Dealers Association)/ SEC	U.S.A.	· Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. · Must update its plan in the event of any material change to the member's operations, structure	Sept - 2003	Enf		http://www.sec.gov/rules/sro/34-48503.htm	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
NASD Rule 3510 has been superseded by FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3510: Business continuity Plans	Reg	NASD	U.S.A.	Requires a Business Continuity Plan addressing: <ul style="list-style-type: none"> · Alternate communications between customers, firm and employees · Business constituent, bank and counter party impact · Regulatory Reporting · Mission Critical Systems · Operational and Finan 	Feb-2015	Enf		http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625	✓						
NASD Rule 3520 has been superseded by FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3520: Emergency Contact Information	Reg	NASD	U.S.A.	NASD Rule 3520 has been superseded by FINRA Rule 4370. Rule 3520 requires NASD members to provide NASD with emergency contact information and to update any information upon the occurrence of a material change. The Rule requires members to designate two emergency contact persons that NASD may contact in the e	Feb-2015	Enf		http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625	✓						
National Instrument 21-101 Marketplace Operation; and National Instrument 31-103 Registration Requirements and Exemptions	Reg	Ontario Securities Commission (OSC)	Canada	Securities regulations require that business continuity plans be tested regularly, to reflect current or potential developments. Subsection 12.1(b) of National Instrument 21-101 Marketplace Operation requires marketplaces to test their business continuity and disaster recovery plans on a reasonably frequent basis and, in any event, at least annually. In addition, subsection 11.1(b) of National Instrument 31-103 Registration Requirements and Exemptions requires a registered firm to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to manage the risks associated with its	Feb-2013	Enf	Only applied to financial institutions registered in Ontario	http://www.osc.gov.on.ca/en/6090.htm	✓						
NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan	Reg	CFTC (Commodity Futures Trading Commission)	U.S.A.	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.	2016	Enf		http://www.nfa.futures.org/nfamanual/NFAMannual.aspx?RuleID=9052&Section=9 http://www.nfa.futures.org/nfa-compliance/NFA-general-compliance-issues/business-continuity-disaster-recovery.HTML	✓						

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
NFPA 111: Standard on Stored Electrical Energy Emergency and Standby Power Systems	Std	NFPA (National Fire Protection Association)	U.S.A.	FPA 111 presents installation, maintenance, operation, and testing requirements as they pertain to the performance of the stored emergency power supply system (SEPPS) up to the load terminals of the transfer switch. Specific topics include definitions of the classification of SEPPS; energy sources, converters, inverters, and accessories; transfer switches and protection; installation and environmental considerations; and routine maintenance and operational testing.	2016	Wat		http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=111&cookie%5Ftest=1	✓	✓	✓	✓	✓	✓	✓
NFPA 232: Standard on Protection of Records	Std	NFPA (National Fire Protection Association)	U.S.A.	Code 232 standard provides requirements for records protection equipment and facilities and records-handling techniques that safeguard records in a variety of media forms from the hazards of fire and its associated effects.	2016	Wat		http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=232	✓	✓	✓	✓	✓	✓	✓
NFPA Standard 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs	Std	NFPA (National Fire Protection Association)	U.S.A.	Establishes minimum criteria for disaster management for the private and public sectors in the development of a program for effective disaster mitigation, preparedness, response and recovery.	2013	Wat		http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf	✓	✓	✓	✓	✓	✓	✓
NIST 800-34	GP	National Institute of Standards and Technology (NIST)	U.S.A.	Contingency Planning Guide for Federal Information Systems - NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide	2010			http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublications800-34r1.pdf							

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
NIST SP 800-34 Contingency Planning Guide	Std	NIST (National Institute of Standards and Technology)	U.S.A.	<ul style="list-style-type: none"> 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. 	Nov-2010	Enf		http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf	✓	✓	✓	✓	✓	✓	✓
NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations	Std	NIST (National Institute of Standards and Technology)	U.S.A.	The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all	Apr-13	Enf		http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf	✓	✓	✓	✓	✓	✓	✓
OCC 2000-14: Infrastructure Threats – Intrusion Risks (May 15, 2000)	Reg	OCC	U.S.A.	This bulletin provides guidance to financial institutions on how to prevent, detect, and respond to intrusions into bank computer systems. Intrusions can originate either inside or outside of the bank and can result in a range of damaging outcomes, including the theft of confidential information, unauthorized transfer of funds, and damage to an institution's reputation.	2000	Enf	This bulletin provides guidance in each of these critical areas and also highlights information-sharing mechanisms banks can use to keep abreast of current attack techniques and potential vulnerabilities.	http://www.occ.gov/news-issuances/bulletins/2000/bulletin-2000-14.html	✓						✓
OCC 2001-47: Third-Party Relationships (November 1, 2001)	Reg	OCC	U.S.A.	This bulletin provides guidance to national banks on managing the risks that may arise from their business relationship with third parties. A third party's inability to deliver products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the bank to transaction risk. Lack of effective business resumption and contingency planning for such situations also increases the bank's transaction risk. The contract should provide for continuation of the business function in the event of	Nov-01	Enf	The bank's own contingency plan should address potential financial problems or insolvency of the third party. As of May 17, 2012, this guidance applies to federal savings associations in addition to national banks	http://it handbook.ffiec.gov/media/resources/3333/occ_bul_2001_47_third_party_relationships.pdf	✓						✓
OCC 2008-6: FFIEC (February 2015)	Reg	OCC	U.S.A.	The Federal Financial Institutions Examination Council (FFIEC) released an updated Business Continuity Planning Booklet (booklet), which is one of 11 that, in total, comprise the FFIEC IT Examination Handbook. The enterprise-wide perspective taken on business risk and human elements makes this booklet a	2015	Enf	This "Business Continuity Planning" booklet is one in a series of booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination	http://it handbook.ffiec.gov/it-booklets/business-continuity-planning.aspx	✓						✓

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link	Infrastructure Category							
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	
OCC Comptroller's Handbooks	GP	Office of the Comptroller	U.S.A.	The Comptroller's Handbook is a collection of booklets that contain the concepts and procedures established by the Office of the Comptroller of the Currency (OCC) for the examination of national banks, federal savings associations, and federal branches and agencies of foreign banks. OCC Comptroller's Handbook	2016	Enf	Listed guidelines are joint publication between: - Board of Governors of the Federal Reserve System - Federal Deposit Insurance Corporation	http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/index-comptrollers-handbook.html	✓							
OSFI Guideline B-10 - Outsourcing of Business Activities, Functions and Processes	Reg	Office of the Superintendent of Financial Institutions Canada (OSFI)	Canada	An FRE's business continuity plan should address reasonably foreseeable situations (either temporary or permanent) where the service provider fails to continue providing service. The business continuity plan and back-up systems should be commensurate with the risk of a service disruption. In particular, the FRE's business continuity plan should ensure that the FRE has in its possession, or can readily access, all records necessary to allow it to sustain business operations, meet its statutory obligations, and provide all information as may be required by OSFI to meet its mandate, in the event the service provider is unable to provide the service.	Mar-09	Enf		http://www.osfi-bsif.gc.ca/Eng/Docs/b10.pdf	✓							
OSFI Guideline B-9 - Earthquake Exposure	Reg	Office of the Superintendent of	Canada	Insurers must have contingency plans in place to ensure continued efficient business operations. The contingency plan	2013	Enf	Document define OSFI's expectations relating to P&C insurers' earthquake	http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/gf-ld/Pages/bg.aspx	✓							
OSHA - Occupational Safety and Health Administration	Reg	OSHA (Occupational Safety and Health Administration)	U.S.A.	Some businesses may be required by regulation to establish Emergency Action Plans meeting certain requirements (see 29 CFR 1910.38 and OSHA's compliance policy). Effective plans should take into account what personal protective equipment workers may require, as well as other resilience resources for emergency responses. Employers should also be aware that some states have	Nov-02	IAI	An emergency action plan must be in writing, kept in the workplace, and available to employees for review. However, an employer with 10 or fewer employees may communicate the plan orally to employees.	https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=5TANDARDS&p_id=9726	✓	✓	✓	✓	✓	✓	✓	
Outsourcing Technology Booklet	GP	FFIEC	U.S.A.	The institution should understand all relevant service provider business continuity requirements, incorporate those requirements within its own business continuity plan, and ensure the service provider tests its plan annually. Management should require the service provider to report all test plan results and to notify the institution after any business continuity plan modifications. The institution should integrate the provider's business continuity plan into its own plan, communicate functions	2004	Wat	The "Outsourcing Technology Booklet" is one of several that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook). The outsourcing risk management program should identify, for Business Continuity Planning (BCP) purposes, the	http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx	✓							

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link	Infrastructure Category						
									Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications
Oversight of the South African National Payment System	Reg	South African Reserve Bank	South Africa	One of the requirements for participation in the SAMOS system is to have sufficient business continuity planning (BCP) and DR facilities in place.	2010	Enf	All participants in the National Payment System are required to have two agreements in place: 1) Redundancy arrangements address failure by one or more of the components that form part of the participant interface infrastructure. 2) DR facilities make provision for a total loss of access to the primary infrastructure and must be in a different location from the primary site. Participants are required to test both these arrangements on a regular basis and to advise the central bank of the test outcomes.	https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Pages/National%20Payment%20System%20(NPS)-Home.aspx	✓						
Risk Management Handbook Volume III Contingency Planning Standard 4.4	Std	CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group	U.S.A.	The CMS Contingency Planning Standard is consistent with the guidance of the National Institute of Standards and Technology (NIST) and most specifically with NIST Special Publication (SP) 800-34 revision 1, Contingency Planning Guide for Federal Information Systems2 dated May 2010.	Feb-2014	Enf		https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_4_4_Contingency_Planning_Standard.pdf		✓					

The content provided was compiled by volunteers of the DRJ EAB Committee, and is as accurate as possible.

Categories (column B):

Standard (Std) Level of quality accepted as norm, typically published by a professional organization of governing body, and is often an auditable standard.

Regulation (Reg) An official rule, law, or order stating what may or may not be done or how something must be done. Issued by a government department or agency.

Good Practice (Leading Practice, Guide, or Guidelines) Recommendation indicating a technique or methodology that, through experience & research, has proven to reliably lead to a desired result. Typically published by a professional organization of government.

Enforcement (column G):

Enforced (Enf) Most frequently enforced for compliance purposes

Ambiguous (Amb) Further clarification regarding strong ties with Business Continuity need to happen

Watch List (Wat) Participating members should be looking for the presence of this item within the coming months/years

Invocation at Incident (IAI) Likely to be invoked or brought to bear as a result of an "incident" occurring involving your organization

Additional Resources:

http://wiki.iso27001standard.com/index.php?title=Laws_and_regulations_on_information_security_and_business_continuity

<http://www.avalution.com/Resources/Standards/Pages/InternationalStandardsandRegulatoryRequirements.aspx>

<http://www.bcifiles.com/LRSG.pdf>

<http://www.bcmpedia.org/wiki/Standards>

<http://www.gartner.com/id=483265>

http://www.geminare.com/pdf/U.S_Regulatory_Compliance_Overview.pdf

Acronym	Country	Definition
ACH	U.S.A.	Automated Clearinghouse Association (of the Federal Reserve Bank)
AICPA	U.S.A.	American Institute of Certified Public Accountants
ANAO	Australia	Australian National Audit Office
ANSI	U.S.A.	American National Standards Institute
APRA	Australia	Australian Prudential Regulation Authority (APRA)
ARMA	U.S.A.	Association of Records Managers and Administrators
BOJ	Japan	Bank of Japan
BSE	India	Bombay Stock Exchange
BSI	U.K.	British Standards Institute
CCPA	U.S.A.	Consumer Credit Protection Act
CFR	U.S.A.	Code of Federal Regulations
CISP	U.S.A.	Customer Information Security Program
CNB	Croatia	Croatian National Bank (Hrvatska Narodna Banka - HNB)
COBIT	U.S.A.	Control Objectives for information and related Technology
COSO	U.S.A.	Committee of Sponsoring Organizations (of the Treadway Commission)
CSA	Canada	Canadian Standards Association
DHS	U.S.A.	Department of Homeland Security (USA)
DRII	International	Disaster Recovery Institute International
EFTA	U.S.A.	Electronic Fund Transfer Act
FCC	U.S.A.	Federal Communications Commission
FDIC	U.S.A.	Federal Deposit Insurance Corporation
FDICIA	U.S.A.	Federal Deposit Insurance Corporation Improvement Act
FFIEC	U.S.A.	Federal Financial Institutions Examination Council
FICOM	Canada	The Financial Institutions Commission (FICOM) is a regulatory agency responsible pension, financial services and real estate sectors in British Columbia.
FINRA	U.S.A.	Financial Industry Regulatory Authority (FINRA) is the largest independent regulator for all securities firms doing business in the United States. http://www.finra.org/AboutFINRA/
FIRREA	U.S.A.	Financial Institutions Reform, Recovery, and Enforcement Act
FISC	Japan	The Center for Financial Industry Information System
FISC	Japan	Financial Industry Information System
FISMA	U.S.A.	Federal Information Security Management Act
FRB	U.S.A.	Federal Reserve Bank
FSA	U.K.	Financial Services Authority
FSSCC	U.S.A.	Financial Services Sector Coordinating Council for Critical Infrastructure Protection
FTC	U.S.A.	Federal Trade Commission
GAO	U.S.A.	General Accounting Office
HIPAA	U.S.A.	Health Insurance Portability and Accountability Act
HKMA	Hong Kong	Hong Kong Monetary Authority
IIROC	Canada	The Investment Industry Regulatory Organization of Canada oversees all investment dealers and trading activities in Canada.
IRS	U.S.A.	Internal Revenue Service
ISO	International	International Organization for Standardization
ITIL	International	Information Technology (IT) Infrastructure Library
MAS	Singapore	Monetary Authority of Singapore
NASD	U.S.A.	North American Securities Dealers Association
NFPA	U.S.A.	National Fire Protection Association
NIST	U.S.A.	National Institute of Standards and Technology, U.S. Department of Commerce
NSE	India	National Stock Exchange
NYSE	U.S.A.	New York Stock Exchange
OCC	U.S.A.	Office of the Comptroller of the Currency
OSC	Canada	Ontario Securities Commission
OSHA	U.S.A.	Occupational Safety and Health Administration
PCAOB	U.S.A.	Public Company Accounting Oversight Board

DRJ's "Obsolete" or "Not Directly Applicable" Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August 19, 2016**

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IA)	Notes /Comments	Link
AS/NZS 4360: 2004 Risk Management Standard; Business Continuity	Std	Standards Association of Australia	Australia, New Zealand	AS/NZS 4360 is a generic guide for risk management so that it applies to all forms of organizations. Risk management" is defined as 'the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.'		Wat	Superseded by AS/NZS ISO 31000:2009	http://www.saiglobal.com/shop/Script/details.asp?docn=AS0733759041A http://www.noweco.com/risk/riske19.htm
AS/NZS 4360: 2004 Risk Management Standard; Business Continuity	Std	Standards Association of Australia	Australia, New Zealand	AS/NZS 4360 is a generic guide for risk management so that it applies to all forms of organizations. Risk management" is defined as 'the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.'	None	Wat	Superseded by AS/NZS ISO 31000:2009	http://www.saiglobal.com/shop/Script/details.asp?docn=AS0733759041A http://www.noweco.com/risk/riske19.htm
AS/NZS 7799.2:2000 (Previously known as 4444.2)	Std	Standards Association of Australia	Australia, New Zealand	This Standard is intended for use by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization and it may be considered as a basis for developing organizational security standards.		Wat	Superseded by AS/NZS 7799.2:2003	http://www.saiglobal.com/shop/Script/details.asp?docn=AS986176255535
AS/NZS 7799.2:2000 (Previously known as 4444.2)	Std	Standards Association of Australia	Australia, New Zealand	This Standard is intended for use by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization and it may be considered as a basis for developing organizational security standards.	None	Wat	Superseded by AS/NZS 7799.2:2003	http://www.saiglobal.com/shop/Script/details.asp?docn=AS986176255535
Australian Commonwealth Criminal Code (1994)	Reg	Australian Government	Australia	Establishing criminal penalties for officers and directors of organizations that experience a major disaster and fail to have a proper business continuity plan in place. Although has no specific reference to business continuity.	None	Enf	Section 5, Corporate criminal responsibility, Part 2.5	www.isrcl.org/Papers/2008/Hinchcliff.pdf
BS (British Standard) 25999	Std	BSI (British Standards Institute)	International	BS 25999-1: Provide a basis for understanding, developing and implementing business continuity within an organization; provide confidence in B2B and B2C relationships BS 25999-2: Specify the requirements for "establishing, operating, monitoring, reviewing, maintaining and improving a documented BCM system within the context of an organization's overall business risks", and for the implementation of continuity controls customized to the needs of specific organization.	May-2012	Enf	Superseded by the international standard ISO22301 in May 2012. Organisations certified to BS25999 should transition themselves to the new international standard by 30th May 2014.	http://www.wjsi.com/xml/
Bulletin R-67 Rescinded 7/10/1989.	Reg	Federal Home Loan Bank	U.S.A.	N/A	None	Enf	Rescinded 7/10/1989. Comptroller of Currency BC-177 (1983, 1987) superceded Federal Home Loan Bank Bulletin R-67.	

DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: **August**

19, 2016

Country	Number of Rules & Regulations Listed by Country	Infrastructure Category								Acromyns
		Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies	
Australia	3	3	1	1	1	1	1	1	1	2
Australia, New Zealand	5	5	3	3	3	3	3	3	3	0
Canada	20	11	4	6	4	5	5	4	7	4
Croatia	2	2	0	0	0	0	0	1	1	1
Hong Kong	3	2	0	0	0	0	0	0	1	1
India	0	0	0	0	0	0	0	0	0	4
Indonesia	1	1	0	0	0	0	0	0	0	0
International	17	10	8	8	8	15	8	8	7	3
Japan	1	1	0	0	0	0	0	0	0	3
Malaysia	3	3	1	1	1	1	1	1	1	0
New Zealand	1	0	0	0	0	0	0	0	1	0
Pakistan	0	0	0	0	0	0	0	0	0	0
Philippines	2	2	0	0	0	0	0	0	0	0
Singapore	3	3	0	0	0	0	0	0	0	1
South Africa	7	6	4	4	4	5	4	4	3	1
Thailand	0	0	0	0	0	0	0	0	0	0
U.K.	1	1	1	1	1	1	1	1	1	2
U.S.A.	53	43	27	20	20	21	20	28	19	34
Total	122									56