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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
AS/NZS 5050:2010 Business continuity - Managing disruption-related risk	Std	Standards Association of Australia	Australia, New Zealand	Provides a generic guide for Business continuity - Managing disruption-related risk. It may be applied to a wide range of activities or operations of any public, private or community enterprise, or group.	Jun 2010		Wat	document may be purchased; supersedes DR 09013; governance, risk and compliance regulatory developments in Australia reference this standard	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	✓	✓	✓	✓	✓	✓	✓	✓
2017 ACH Rules Online - Operating Rules & Guidelines	Reg	ACH (Federal Reserve's Automated Clearinghouse Association)	U.S.A.	· Requires 6 year file retention on all ACH transactionsx · An ACH transaction is a batch-processed, value-dated electronic funds transfer between originating and receiving financial institutions	Appears to have a 2019 version, available for a subscription		IAI	Login is required to access, but non-member logins are granted and given read-only access. Non-compliant fines not more than $10,000 or imprisoned not more than ten years, or both	http://www.achrulesonline.org/	✓							
87/600/Euratom: Council Decision of 14 December 1987 on Community arrangements for the early exchange of information in the event of a radiological emergency	Reg	The Council of the European Union	European Union	These arrangements shall apply to the notification and provision of information whenever a Member State decides to take measures of a wide-spread nature in order to protect the general public in case of a radiological emergency following: (a) an accident in its territory involving facilities or activities from which a significant release of radioactive material occurs or is likely to occur; or (b) the detection, within or outside its own territory, of abnormal levels of radioactivity which are likely to be detrimental to public health in that Member State; or (c) accidents other than those specified in (a) involving facilities or activities from which a significant release of radioactive material occurs or is likely to occur; or (d) other accidents from which a significant release of radioactive materials occurs or is likely to occur. Member States shall take the measures necessary to comply with this Decision within three months of the date of its notification.	1987		Enf		https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:31987D0600		✓	✓	✓	✓			✓
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, (3) vendor relationships, (4) telecommunications services and technology considerations, (5) communications plans, (6) regulatory and compliance considerations, and (7) review and testing.	Aug. 2013		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/bcpstaffadvisory081613.pdf and/or http://finra.complinet.com/net_file_store/new_rulebooks/f/i/FINRANotice13-25.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
AFMA KRI Definitions & Guidelines	GP	Australian National Audit Office (ANAO)	Australia	Multiple publsked 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	Nov 2014		Enf	Audit Report: The objective of the audit was to assess the adequacy of selected Australian Government entities' practices and procedures to manage business continuity. To conclude against this objective, the ANAO adopted high-level criteria relating to the entities' establishment, implementation and review of business continuity arrangements.	https://www.anao.gov.au/work/performance-audit/business-continuity-management#0-0-summary	✓							
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. This Guide has been produced following consultation with Australian Government and private sector entities. The Guide provides a refreshed version of a previous ANAO Guide. The new version is presented in a more user-friendly format, and includes contemporary practical advice, case studies and references as well as exploring issues within the business continuity environment that have arisen since the previous ANAO publication. The Guide will be a useful reference document for boards, chief executives and senior management in public sector entities	8//2018		Wat	Have to request a copy from the National Librarian of Australia. The document addresses Crisis Management, Business Planning, and Emergency Response.	https://www.anao.gov.au/work/better-practice-guide/review-anao-better-practice-guides	✓	✓	✓	✓	✓	✓	✓	✓
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	Jul 2010		Enf	This site allows you to order documents at a specific price.	http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2fARMA+5-2010	✓	✓	✓	✓	✓	✓	✓	✓
APRA - Prudential Standard CPS 232 Business Continuity Management	Std	Australian Prudential Regulation Authority (APRA)	Australia	This Prudential Standard requires each APRA-regulated institution and Head of a group to implement a whole-of-business approach to business continuity management that is appropriate to the nature and scale of the operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the institution's or group's business operations, reputation, profitability, depositors, policyholders and other stakeholders.	Aug 2018		Enf		https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-232-Business-Continuity-Management-%28July-2017%29.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
AS/NZS Good Management Practice - Business Continuity Management	Std	Standards Association of Australia	Australia, New Zealand	Business continuity management is a process that helps an organisation better understand and prioritise threats in the event of a crisis, reduce the likelihood of those threats, and ensure good recovery. Business continuity management is part of a business's overall approach to effective risk management. The set provides guidance on societal security, business continuity management, information technology security techniques as well as planning for emergencies and disruption.	Jun 2017		Wat	The comprehensive set includes: - AS ISO 22301:2017 Societal security - Business continuity management systems – Requirements - AS ISO 22313:2017 Societal security - Business continuity management systems – Guidance - AS/NZS 5050:2010 Business continuity - Managing disruption-related risk - AS 3745-2010 Planning for emergencies in facilities	https://infostore.saiglobal.com/en-us/Standards/Good-Management-Practice-Business-Continuity-Management-Set-2017-99247_SAIG_AS_AS_208671/	✓	✓	✓	✓	✓	✓	✓	✓
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.	Jul 2009		Wat	Supersedes AS/NZS 4360; 2004 Non-government employees may 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 - Information security management systems - Requirements	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 (ISMIS). This Standard can be used in order to assess conformance by interested internal or external parties.	Jun 2006		Wat	Superceded by AS ISO/IEC 27001:2015 Related Guide: Good Management Practice - Information Security Set: 2017 (Nov 2017) May be purchased from SAI Global	http://infostore.saiglobal.com/store/Details.aspx?productID=394887 https://infostore.saiglobal.com/en-us/Standards/Good-Management-Practice-Information-Security-Set-2017-1947001/	✓							
ASIS American National Standard - Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard (2009)	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 enviroments. It is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and repond to a disruptive incident (emergency, crisis, or disaster). It enhances an organization's capacity to manage and survive the event, and take all appropriate actions to help ensure the organization's continued viability. Regardless of the organization, its leadership has a duty to stakeholders to plan for its survival. The body of this document provides generic auditable criteria to establish, chec, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.	Mar 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 emergency incidents and disasters. The structure provides the framework for a standardized emergency response in the province.	Mar 2018		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/00_96111_01								✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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 for matters connected therewith.	1996		Wat	Banks Act, 1990 (as amended): Reproduced under Government Printer's Copyright Authority No 10665 dated 19 March 1999 (effective 1 January 2008)	https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/2591/Banks+Amendment+Act+2007[1].pdf	✓							
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		https://www.bis.org/publ/joint17.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/bcbs189.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 attestation of the adequacy of internal controls. - Canadian companies are supposed to deliver a " reasonable assurance " of preventing risk of material misstatement. And to give that assurance, the companies are supposed to show high level of commitment, care and meticulousness for reviewing and documenting their internal controls.	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	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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, competitive, agile and robust. One way to improve resilience is by integrating and coordinating the various operational disciplines in an organization, so BS 65000 draws on other standards relating to these disciplines. Most organizations work within a complex web of interactions. The standard recognises that it is essential to build resilience not only within an organization but across networks and in partnership with others. Using agreed terminology, BS 65000: • clarifies the meaning of resilience • highlights the key components of resilience • helps an organization to measure its resilience and make improvements • identifies good practice found in other disciplines and defined in existing standards	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=000000000030258792	✓	✓	✓	✓	✓	✓	✓	✓
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 business opportunities or asset deterioration, and (3) to ensure a timely resumption of normal operations. Requires submission and validation of business continuity plan by all Non-Bank Financial Institutions With Quasi-Banking Functions (NBQBs), Investment Houses (IHs) With Trust Functions, Non-Stock Savings And Loan Associations (NSSLAs), AND All Other Non-Bank Financial Institutions (NBFIs) Which are Subsidiaries or Affiliates of Banks or NBQBs.	37167		Wat		http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=669	✓							
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	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Building the UK Financial Sector's Operational Resilience DISCUSSION PAPER		Bank of England (BOE) Prudential Regulation Authority (PRA) Financial Conduct Authority (FCA)	U.K.	"This discussion paper seeks to commence a dialogue with the financial services industry on achieving a step change in the operational resilience of firms and FMIs and generate debate about the expectations regulators and the wider public might have of the operational resilience of our financial services institutions." "The supervisory authorities are considering the extent to which they might supplement existing policies to improve the resilience of the system as a whole, and to increase the focus on this area within individual firms. They are reviewing exisiting policies, including those on...business continuity plans, to ensure that these continue to be effective...."	Jul 2018		Wat	NEW FOR Spring 2019 Not a rule or regulation, but a discussion paper describing a key new focus for UK regulatory oversight of financial services industry operational resilience. The regulators have invited financial services firms to provide feedback on the paper	https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A	✓							
Business Continuity Management Audit/Assurance Program	GP	ISACA	International	Main subject areas of the DRI Professional Practices: - Project Initiation and Management - Risk Evaluation and Control - Business Impart Analysis - Developing Business Continuity Strategies - Emergency Response and Operations - Developing and Implementing Business Continuity Plans - Awareness Programs and Training - Maintaining and Exercising the Business Continuity Plans - Crisis Communications - Coordination with External Agencies	2011		Enf	DRI International established the industry's international first BCM methodology in 1997 when they published the Professional Practices for Business Continuity Planners. Currently $45.00 USD to purchase	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx	✓	✓	✓	✓	✓	✓	✓	✓
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.	2018		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	40269		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 complementarily in the management of business continuity.	https://lautorite.qc.ca/en/professionals/regulations-and-obligations/public-consultations/topic/insurance-and-financial-planning/finished/7/#consultation_583 https://lautorite.qc.ca/fileadmin/lautorite/consultations/lignes-directrices/ld-bus-conti-manag-2009-06-22-cq.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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. The Bank also coordinates with relevant parties for effective business continuity planning at payment and settlement systems, at the market level, and in the financial system as a whole. For example, the Bank tests contingency procedures with market participants and with related administrative institutions, based on various scenarios including large-scale earthquakes.	2016		Enf	added the year of last revision 2016	http://www.boj.or.jp/en/about/bcp/	✓							
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 Consumer Privacy Act (CCPA)	Reg	California Constitution 1798.100 to 1798.198	U.S.A.	The California Consumer Privacy Act (CCPA) is a data privacy act that goes into effect Jan 1, 2020. Every Company that does business in California and collects personal information must abide by the law.	Jun-18		Enf	The intention of the Act is to provide California residents with the right to: •Know what Personal Data is being collected about them •Know whether their personal data is sold or disclosed and to whom •Say no to the sale of personal data •Access their personal data	https://cal-privacy.com/ https://www.cmswire.com/customer-experience/what-is-the-california-consumer-privacy-act-of-2018-and-how-does-it-affect-marketers/	✓	✓	✓	✓	✓	✓	✓	
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.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf	✓	✓	✓	✓	✓	✓	✓	✓
Canadian Aviation Security Regulations, 2012 (SOR/2011-318) Section 452.27 1,2,4; Section 325 1,2,4; Section 169 1,2,4; Section 63 1,2,4	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 section 324 in the event that the operator is unable to use its restricted area access control process to comply with that section.	2012		Enf	The operator of the aerodrome must make its business continuity plan available to the Minister on reasonable notice given by the Minister of Justice Laws Website	https://laws-lois.justice.gc.ca/eng/regulations/		✓						
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"	https://www.bi.go.id/en/peraturan/perbankan/Pages/se_093007.aspx http://www.bi.go.id/en/peraturan/perbankan/Documents/86336e7d95464a3585d1e058fc2c1194se_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.	Dec 2014		Enf	Crisis Management HKEx procedures & guidelines Public Health	http://www.sfc.hk/web/EN/published-resources/business-continuity/ http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=H289	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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	✓	✓	✓	✓	✓	✓	✓	✓
Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations	Reg	The Council of the European Union	European Union	This Directive shall apply to any civilian nuclear installation subject to a licence. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 22 July 2011.	2014		Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1412848109512&uri=CELEX:32009L0071		✓	✓	✓	✓			✓
Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom	Reg	The Council of the European Union	European Union	This Directive applies to any planned, existing or emergency exposure situation which involves a risk from exposure to ionising radiation which cannot be disregarded from a radiation protection point of view or with regard to the environment in view of long-term human health protection. EU Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 6 February 2018.	2014		Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1550067952603&uri=CELEX:32013L0059		✓	✓	✓	✓	✓		✓
Croation Sabor: Credit Institutions Act	Reg	Croatian National Bank (CNB)	Croatia	Credit Institutions Act	Feb-19		Enf	Act on Amendments to the Credit Institutions Act (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.	The CTIA represents the U.S. wireless communication industry; advocates for legislative and regulatory policies, works with members to develop test plans and certification processes and building awareness. CTIA advocates on behalf of America's wireless industry for legislative and regulatory policies that foster greater innovation, investment and economic growth.	2019		Wat	Consumer resources include: Emergency Preparedness, Protecting Your Data, Protecting Your Privacy	https://www.ctia.org/consumer-resources/emergency-preparedness Additional URL's: https://www.youtube.com/watch?v=uNqCB4wajo8&feature=youtu.be ctia.org ready.org (REMOVE THIS LINK - NOT WORKING) INSTEAD ADD ready.gov							✓	

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC Text with EEA relevance	Reg	The European Parliament and the Council of the European Union	European Union	1. This Decision lays down rules on epidemiological surveillance, monitoring, early warning of, and combating serious cross-border threats to health, including preparedness and response planning related to those activities, in order to coordinate and complement national policies. 2. This Decision aims to support cooperation and coordination between the Member States in order to improve the prevention and control of the spread of severe human diseases across the borders of the Member States, and to combat other serious cross-border threats to health in order to contribute to a high level of public health protection in the Union. 3. This Decision also clarifies the methods of cooperation and coordination between the various actors at Union level.	2013		Enf		https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013D1082	✓	✓	✓	✓	✓	✓	✓	✓
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism	Reg	The European Parliament and the Council of the European Union	European Union	1. The Union Civil Protection Mechanism ("the Union Mechanism") shall aim to strengthen the cooperation between the Union and the Member States and to facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters. 2. The protection to be ensured by the Union Mechanism shall cover primarily people, but also the environment and property, including cultural heritage, against all kinds of natural and man-made disasters, including the consequences of acts of terrorism, technological, radiological or environmental disasters, marine pollution, and acute health emergencies, occurring inside or outside the Union. In the case of the consequences of acts of terrorism or radiological disasters, the Union Mechanism may cover only preparedness and response actions. This Decision shall enter into force on the day following that of its publication in the Official Journal of the European Union. It shall apply from 1 January 2014.	2013		Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013D1313	✓	✓	✓	✓	✓	✓	✓	✓
Derivatives Regulation, RRQ, c I-14.01	Reg	Regulations of Quebec	Canada	DIVISION II.3 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: ... (3) they have developed an emergency and contingency plan to ensure business continuity.	Jun 2019		Enf	This Act seeks to foster honest, fair, efficient and transparent derivatives markets and to protect the public from unfair, improper or fraudulent practices and market manipulation. It also seeks to ensure that the public, and more particularly, market participants and their clients, have access to adequate, true and clear information, tailored to the level of financial knowledge and experience of those for whom it is intended.	http://www.legisquebec.gouv.qc.ca/en/ShowDoc/cs/I-14.01/	✓							
Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks	Reg	The European Parliament and the Council of the European Union	European Union	Directive 2007/60/EC on the assessment and management of flood risks entered into force on 26 November 2007. This Directive now requires Member States to assess if all water courses and coast lines are at risk from flooding, to map the flood extent and assets and humans at risk in these areas and to take adequate and coordinated measures to reduce this flood risk. With this Directive also reinforces the rights of the public to access this information and to have a say in the planning process.	2007		Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32007L0060	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance	Reg	The European Parliament and the Council of the European Union	European Union	This Directive lays down rules for the prevention of major accidents which involve dangerous substances, and the limitation of their consequences for human health and the environment, with a view to ensuring a high level of protection throughout the Union in a consistent and effective manner. EU Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 May 2015. They shall apply those measures from 1 June 2015.	2012		Enf		https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32012L0018		✓	✓	✓	✓	✓	✓	✓
Disaster Management Act 2002	Reg	Ministry for Provincial & Local Government Disaster Management Act, 2002	South Africa	The Disaster Management institute of Southern Africa (DMISA) was founded in 1985 and still maintains its position as the premium professional association for Disaster Management professionals and associated disciplines in Southern Africa. DMISA is the SAQA-approved professional body for Disaster Management in South Africa and manages the SAQA-approved Disaster Management Professional (PrDM), Disaster Management Practitioner (DMPc), Disaster Management Associate (DMA) and Disaster Management Technician (DMT) designation. DMISA is committed to providing learning, networking and alignment opportunities for the Disaster Management / Disaster Risk Reduction community of practice in Southern Africa. We encourage interaction between practitioners, researchers, legislators, stakeholders and leadership across Southern Africa to build capacity and resilience, reduce risk, and improve our common understanding of disaster risk. Our common goal is to reduce the impact of disasters on society and to build future ready sustainable communities.	Jan 2003		Enf		http://disaster.co.za/?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.	Aug 2019		Enf	The proposed constitutional amendments were discussed by the DMISA Council on 18 September 2018 and subsequently at the extraordinary general meeting held on 21 September 2018, where the amended Constitution was officially adopted.	http://disaster.co.za/?id=25					✓			✓
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 co-ordinated 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.	2015		Enf	Regulation Gazette No. 7122 Vol. 433 Pretoria 30 July 2001 No. 22506 DMISA is the professional body for Disaster Management in South Africa.	https://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	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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 plannint team(s) and action plans; and developing project management and documentation requirements 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.	Mar 2015			GAP is an acronym meaning "Generally Accepted Practice"	http://www.drj.com/GAP/gap.pdf	✓	✓	✓	✓	✓	✓	✓	✓
Earthquake Planning for Business	GP	Emergency Preparedness for Industry and Commerce Council EPICC	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 and employees with the tools to develop earthquake preparedness and response plans and procedures by: - Offering guidance and a standard approach to earthquake planning - Providing a framework with which to prepare your organization for its specific earthquake vulnerabilities - Providing a template for developing your organization's emergency plans	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: Chemical Facility Anti-Terrorism Standards (as of 08/16/2017)	Reg	Dept. of Homeland Security	U.S.A.	· U.S. Govennment Publishing Office - Continuity of operations for Critical Infrastructure · Enhance security and resiliency of chemical facilities.	Feb 2019		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					✓			

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
e-CFR Part 29: Protected Critical Infrastructure Information (as of 08/16/2015)	Reg	Dept. of Homeland Security	U.S.A.	· Continuity of operations for Critical Infrastructure · Disclosure of critical information to the government	Aug 2018		Wat	Uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Department of Homeland Security (DHS). Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act). Consistent with the statutory mission of DHS to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, DHS will encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is, as necessary, securely shared with State and local government	http://www.ecfr.gov/cgi-bin/text-idx?SID=a2223621620cb8f2ebc8f7888f44d25&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 Handbood Series. Numerous handbooks are available.	Feb 2015		IAI	[Codified to 15 U.S.C. 1693] effective July 21, 2010	https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf	✓							
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; coordinating federal and provincial emergency management activities coordinating the provision of assistance to a province; promoting a common approach to emergency management, including the adoption of standards and best practices; and conducting exercises and providing emergency management education and training.	3-Aug-07		Enf	Per website, Act confirmed current to 2019-06-20	http://laws-lois.justice.gc.ca/eng/acts/E-4.56/page-1.html								✓
Emergency Management and Civil Protection Act (EMPCA)	Reg	Government of Ontario	Canada	Under Provincial legislation, the Emergency Management and Civil Protection Act (EMPCA) , every municipality in Ontario is required to have an Emergency Management Program.	29-Aug-19		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.	January 31 2018			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/rsrcs/pblctns/mrgnc-mngmnt-pnnng/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 wells, sour gas production facilities and associated gathering systems, high vapour pressure pipelines, spills, and natural gas storage.	2017		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 responsible petroleum operations.	https://aer.ca/regulating-development/rules-and-directives/directives/directive-071 http://exterramonitoring.com/files/ERCB_Directive_071.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Fair Credit Reporting Act	Reg	FTC (Federal Trade Commission)	U.S.A.	· Ensures credit information is accurate and up-to-date · Designed to promote accuracy and ensure the privacy of the information used in consumer reports	2019		IAI	· 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.	Apr 2014		Enf	Last updated April 20, 2014	http://www.fdic.gov/regulations/laws/rules/8000-2400.html	✓							
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	May 2019		Enf	Agencies: Department of Defense (DoD), General Service Adminisration (GSA), and National Aeronautics and Space Administration (NASA).	http://www.fms.treas.gov/eft/regulations/fareft.txt	✓	✓	✓	✓	✓	✓	✓	✓
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. Provides advice on how to create and maintain a comprehensive emergency management program.	Oct 1993		Wat	Links to pdf or text version of the guides, available for download.	http://www.fema.gov/media-library/assets/documents/3412	✓	✓	✓	✓	✓	✓	✓	✓
FFIEC BCP Handbook: Business Continuity Planning (Feb 2015) "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	Aug 2018		Enf	Ineffective or incomplete BC plans may lead to qualified examination reports and loss of trust by regulators and financial market. This link is for the FFIEC IT Examination Infobase site that has multiple booklets available for download.	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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Financial Conduct Authority Handbook	Std	Financial Conduct Authority (FCA)	U.K.	SYSC 4.1.6 - 4.1.8: Business continuity requirements for firms SYSC 3.2.19G: High level guidance on business continuity REC 3.16: Ensure that the FSA receives a copy of the UK recognised body's plans and arrangements for business continuity if there are major problems with its computer systems SYSC 13.8: Unexpected changes and business continuity management SYSC 13.9 (Outsourcing): Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms … the extent to which a service provider will provide business continuity for outsourced operations.	Feb 2019		Wat	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. What constitutes "fault" varies between different Principles. FSA is now 2 separate regulatory authorities - Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).	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 failed financial institutions.	Aug 2017		IAI	SEC. 1123. EMERGENCY EXCEPTION FOR DISASTER AREAS. (a) IN GENERAL.--Each Federal financial institutions regulatory agency may, by regulation or order, make exceptions to this title, and to standards prescribed pursuant to this title, for transactions involving institutions for which the agency is the primary Federal regulator with respect to real property located within a disaster area if the agency-- (1) makes the exception not later than 30 months after the date on which the President determines, pursuant to section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, that a major disaster exists in the area; and (2) determines that the exception-- (A) would facilitate recovery from the major disaster; and (B) is consistent with safety and soundness. (b) 3-YEAR LIMIT ON EXCEPTIONS.--Any exception made under this section shall expire not later than 3 years after the date of the determination referred to in subsection (a)(1). (c) PUBLICATION REQUIRED.--Any Federal financial institutions regulatory agency shall publish in the Federal Register a statement that-- (1) describes any exception made under this section; and	http://www.fdic.gov/regulations/laws/rules/8000-3100.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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 failed financial institutions.	Aug 2017		IAI	SEC. 1123. EMERGENCY EXCEPTION FOR DISASTER AREAS. (a) IN GENERAL.--Each Federal financial institutions regulatory agency may, by regulation or order, make exceptions to this title, and to standards prescribed pursuant to this title, for transactions involving institutions for which the agency is the primary Federal regulator with respect to real property located within a disaster area if the agency-- (1) makes the exception not later than 30 months after the date on which the President determines, pursuant to section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, that a major disaster exists in the area; and (2) determines that the exception-- (A) would facilitate recovery from the major disaster; and (B) is consistent with safety and soundness. (b) 3-YEAR LIMIT ON EXCEPTIONS.--Any exception made under this section shall expire not later than 3 years after the date of the determination referred to in subsection (a)(1). (c) PUBLICATION REQUIRED.--Any Federal financial institutions regulatory agency shall publish in the Federal Register a statement that-- (1) describes any exception made under this section; and	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; (4) Alternate communications between customers and the member; (5) Alternate communications between the member and its employees; (6) Alternate physical location of employees; (7) Critical business constituent, bank, and counter-party impact; (8) Regulatory reporting; (9) Communications with regulators; and (10) How the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.	Feb-15		Enf	Members of FINRA must produce and maintain Business Continuity Plans. Plans must be made available immediately upon request of the FINRA staff. FINRA Rule 4370 is the successor to NYSE Rule 446 and NASD Rule 3510	http://finra.complinet.com/en/display/display.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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; (4) Alternate communications between customers and the member; (5) Alternate communications between the member and its employees; (6) Alternate physical location of employees; (7) Critical business constituent, bank, and counter-party impact; (8) Regulatory reporting; (9) Communications with regulators; and (10) How the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.	Feb 2015		Enf	Members of FINRA must produce and maintain Business Continuity Plans. Plans must be made available immediately upon request of the FINRA staff. FINRA Rule 4370 is the successor to NYSE Rule 446 and NASD Rule 3510	http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625	✓							
FINRA Rule 4370 - Overview	Std	Financial Industry Regulatory Authority (FINRA)	U.S.A.	(a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption... (b) Each member must update its plan in the event of any material change to the member's operations, structure, business or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location. (c) The elements that comprise a business continuity plan are flexible and may be tailored to the size and needs of a member. Each plan, however, must at a minimum, address... (d) Members must designate a member of senior management to approve the plan and he or she shall be responsible for conducting the required annual review. The member of senior management must also be a registered principal. (e) Each member must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must be made in writing to customers at account opening, posted on the member's Web site (if the member maintains a Web site), and mailed to customers upon request.	Feb-15		Enf		http://www.finra.org/Industry/Issues/BusinessContinuity/	✓							
FINRA Rule 4370 - Overview	Std	Financial Industry Regulatory Authority (FINRA)	U.S.A.	General information related to Rule 4370 (Business Continuity Plans and Emergency Contact Information) and links to BCP resources for firms subject to the Rule	Feb 2015		Enf		http://www.finra.org/Industry/Issues/BusinessContinuity/	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3510: Business continuity Plans	Reg	NASD	U.S.A.	Requires a Business Continuity Plan addressing: · Alternate communications between customers, firm and employees · Business constituent, bank and counter party impact · Regulatory Reporting	Feb-2015		Enf	When approved in 2009, FINRA Rule 4370 consolidated NYSE Rule 446 and NASD Rules 3510 and 3520. The rule requires that member firms "establish and maintain business continuity plans that are reasonably designed to enable the firm to meet its obligations to clients in the event of a sudden business disruption."	https://www.finra.org/rules-guidance/rulebooks/finra-rules/4370	✓							
FINRA Rule 4380 - Mandatory participation in FINRA BC/DR Testing under Regulation SCI	Reg	Financial Industry Regulatory Authority (FINRA)	U.S.A.	Rule 4380 - FINRA Mandatory Participation rule indicates that FINRA will designate members that will be required to participate in FINRA's periodic scheduled testing of its BC/DR plan. Members designated will be notified at least 90 days prior to the date, and members may be required to fulfill certain testing requirements determined necessary and appropriate by FINRA, and may be required to satisfy related reporting requirements. Regulation SCI requires that FINRA, as an SCI entity, establish, maintain, and enforce written policies and procedures that address, among other things, "[b]usiness continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse…." In addition, Regulation SCI contains a separate, corresponding requirement that each SCI entity, including FINRA, designate firms that must participate in the testing of the entity's BC/DR plans.	Mar 2018		Enf	New guidance (Notice 18-09) issued March 2018 for firms reporting U.S. Treasury Securities to TRACE to participate in FINRA's Business Continuity/Disaster Recovery Testing	http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=12111 http://www.finra.org/industry/notices/18-09	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
FISMA: The Federal Information Security Modernization Act of 2014)	Reg	Department of Homeland Security (DHS)	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. The Federal Information Security Modernization Act of 2014 (link: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text) amends the Federal Information Security Management Act of 2002 (FISMA) provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents.	Dec 2014		Enf	May apply to organizations and institutions communicating with, performing work for, on behalf of a federal agency. This FISMA act has been amended by The Federal Information Security Moderization Act of 2014 (FISMA 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521 Link is for NIST site, which addresses FISMA requirements. The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include: FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems SP 800-18: Guide for Developing Security Plans for Federal Information Systems and Organizations SP 800-30: Guide for Conducting Risk Assessments SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	https://www.dhs.gov/fisma https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002 https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
FISMA: The Federal Information Security Modernization Act of 2014)	Reg	Department of Homeland Security (DHS)	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. The Federal Information Security Modernization Act of 2014 (link: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text) amends the Federal Information Security Management Act of 2002 (FISMA) provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents. The FISMA publications are developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. The FISMA publications are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.	Dec 2014		Enf	May apply to organizations and institutions communicating with, performing work for, on behalf of a federal agency. This FISMA act has been amended by The Federal Information Security Moderization Act of 2014 (FISMA 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521 Link is for NIST site, which addresses FISMA requirements. The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include: FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems SP 800-18: Guide for Developing Security Plans for Federal Information Systems and Organizations SP 800-30: Guide for Conducting Risk Assessments SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	https://www.dhs.gov/fisma 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-13			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 13-1 / 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	✓							

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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 Outsourcing".	http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm	✓							
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.	Sep 2014			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 Outsourcing".	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.	Gramm-Leach-Bliley Bill Section 501(b) FINANCIAL INSTITUTIONS SAFEGUARDS. In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.	Nov-99		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 from foreseeable threats in security and data integrity.	http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act http://www.ffiec.gov/exam/InfoBase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf	✓							
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; GLBA compliance is mandatory; whether a financial institution discloses non-public information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.	https://en.wikipedia.org/wiki/Gramm–Leach–Bliley_Act http://www.ffiec.gov/exam/InfoBase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf	✓							
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.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf	https://www.law.cornell.edu/cfr/text/45/164.308		✓					✓	✓
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		✓					✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
HITECH Act Enforcement Interim Final Rule	Reg	U.S. Department of Health & Human Services	U.S.A.	The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. It mandates audits of health care providers to investigate and determine if they are in compliance with the HIPAA privacy and security rules. These two laws reinforce each other, and HITECH established data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI" (patient health information).	Jun 2017		Enf	This act applies more to the cybersecurity space but it is tied in with HIPAA and relates to data privacy/PHI. The breach notification requirement could translate to reputation risk, BC and CM etc.	https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/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 derived from the Dealer Member's assessment of its critical business functions and required levels of operation during and following a disruption. Every Dealer Member must also conduct an annual review and test of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.	Jul 2006		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 and other capital markets counterparts.The objective of such a plan is to ensure, at a minimum, clients' access to their assets in the event of significant business interruption. after July 31, 2006 all member firms must	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 Commission)	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; Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location; and A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible. Firms that Play Significant Roles in Critical Financial Markets (As a guideline, the agencies consider a firm significant in a particular critical market if it consistently clears or settles at least five percent of the value of transactions in that critical market.)	Apr-03		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 Revenue Procedure 98-25; 1998-1 C.B. 689 (Supersedes Rev. Proc. 91-59, 1991-2 C.B. 841)	Reg	IRS (Internal Revenue Service)	U.S.A.	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)	Mar 1998		IAI		https://www.irs.gov/businesses/automated-records	✓	✓	✓	✓	✓	✓	✓	

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
ISO 22301 Business Continuity Management	Std	ISO	International	ISO 22301 is the 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. Currently under review and will be replaced by ISO/DIS 22301.	2/25/2019		Wat	Document available for purchase.	http://www.iso.org/iso/catalogue_detail?csnumber=50038	✓	✓	✓	✓	✓	✓	✓	✓
ISO 9000	Std	ISO	International	ISO 9000: family of 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, especially maintenance of records and verification standards. While business continuity planning is not required by statute, vendors report that records retention and data availability are issues with their customers, and that they are specifically asked about their plans.	2/12/2019		Wat	Article has multiple issues including technical language, and multiple references to primary sources.	http://en.wikipedia.org/wiki/ISO_9000					✓				
ISO 9001	Std	ISO (International Organization for Standardization)	International	ISO 9001:2015 - Quality management systems - Requirements This standard specifies requirements for a quality management system when an organization: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.	Sep 2015		Wat	JDN : Old Link - http://en.wikipedia.org/wiki/ISO_9001 JDN Comment: Both ISO/TC 176, Quality Standards Technical Committee, and ANSI list ISO 9001:2015 as the current version.	https://committee.iso.org/home/tc176sc2 https://webstore.ansi.org/sdo/ISO					✓			
ISO 9004 Quality management sysetms - Guidelines for performance improvement	Std	ISO (International Organization for Standardization)	International	ISO 9004:2018 - Quality management - Quality of an organization - Guidance to achieve sustained success ISO 9004:2018 gives guidelines for enhancing an organization's ability to achieve sustained success. This guidance is consistent with the quality management principles given in ISO 9000:2015. ISO 9004:2018 provides a self-assessment tool to review the extent to which the organization has adopted the concepts in this document.	Apr 2018		Wat	JDN: Recommend using ISO TC/176 and ANSI as primary links rather than Wikipedia.	https://committee.iso.org/home/tc176sc2 https://webstore.ansi.org/sdo/ISO					✓			
ISO Guide 73:2009 - Risk management – Vocabulary	GP	ISO (International Organization for Standardization)	International	ISO/Guide 73:2009 (en) - Risk management — Vocabulary This Guide provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk. This Guide is intended to be used by: — those engaged in managing risks, — those who are involved in activities of ISO and IEC, and — developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk.	2009		Wat	JDN : Old Link - http://www.iso.org/iso/catalogue_detail?csnumber=44651 JDN Comment: Both ISO/TC 176, Quality Standards Technical Committee, and ANSI list ISO Guide 73:2009 as the current version.	https://www.iso.org/standard/44651.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	Std	ISO (International Organization for Standardization)	International	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: 1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; 2. implement commonly accepted information security controls; 3. develop their own information security management guidelines.	Oct 2013		Wat	JDN: Recommend using ISO and ANSI as primary links rather than Wikipedia.	https://www.iso.org/standard/54533.html https://webstore.ansi.org/Standards/ISO/ISOIEC270022013					✓			
ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management	Std	ISO (International Organization for Standardization)	International	ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management ISO 27005:2018 supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.	July 2018		Wat		https://www.iso.org/standard/75281.html https://webstore.ansi.org/Standards/ISO/ISOIEC270052018	✓	✓	✓	✓	✓	✓	✓	✓
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 Region	Hong Kong	This document elaborates policy requirements and sets implementation standard on the security requirements specified in the Baseline IT Security Policy, and provides implementation guidance for effective implementation of corresponding security measures. The materials included in this document are prepared irrespective of computer platforms.	Dec 2016			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/ V4.1 November 2008 Version 7, 9/2012	https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/G3.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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	Feb 2018		Wat	ITIL advocates that IT services are aligned to the needs of the business and support its core processes. It provides guidance to organizations and individuals on how to use IT as a tool to facilitate business change, transformation and growth. ITIL is mapped in ISO 20000 Part 11. This recognizes the way that ITIL can be used in order to meet the requirements set out for ISO 20000 certification and the interdependent nature with ITIL. It's the first such mapping that ISO (the International Organization for Standardization) has allowed to be part of their standards. ITIL's IT Service Management Best Practice is supported by a certification scheme that enables practitioners to demonstrate their abilities in adopting and adapting the framework to address their specific needs.	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		✓						
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 King IV 2016	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	From Wikipedia: 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, Nigel Payne, and Richard Wilkinson. The committee has released three King reports on corporate governance in South Africa: 1994 King I 2002 King II 2009 King III 2016 King IV	http://en.wikipedia.org/wiki/King_Committee http://www.ecgi.org/codes/documents/king_i_sa.pdf	✓	✓	✓	✓	✓	✓	✓	
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		http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=60182	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Malaysia Business Continuity Management Framework 2007	Std	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) framework. This framework is applicable to any organisation in any sector or industry. The scope of this Malaysian Standard is limited to identifying the processes involved in developing a BCM framework, the recommended sequence of steps and the minimum deliverables expected from each process.	Aug 2007		Enf	The first link provided is to the a pdf file of the standard, the second is a supporting article discussing BCM in Malaysia	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwiP_bOMuf_cAhVCS60KHbPeBvUQFjADegQICBAC&url=https%3A%2F%2Fwww.msonline.gov.my%2Fdownload_file.php%3Ffile%3D14038%26source%3Dproduction&usg=AOvVaw1gueCcMoXGgV6DbzfX2CnT http://www.cybersecurity.my/data/content_files/13/169.pdf	✓	✓	✓	✓	✓	✓	✓	✓
Malaysian Standard - Business Continuity Framework - 2007	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.	2019		Enf		https://docplayer.net/13835994-Malaysian-standard-information-and-documentation-records-management-part-2-guidelines.html	✓							
Management, Supervision and Internal Control Guidelines ("The Internal Control Guidelines") For Persons Licensed By OR Registerd With The Securities and Futures Commission	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 arisin	Apr 2013		Enf	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.	http://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/management,-supervision-and-internal-control-guidelines-for-persons-licensed/Management,%20Supervision%20and%20Internal%20Control%20Guidelines%20for%20Persons%20Licensed%20by%20or%20Registered%20with%20the%20Securities%20and%20Futures%20Commission.pdf	✓							
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		www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/BCMGuidelines.pdf	✓							
MAS Guidelines on Outsourcing - Section 5.7 Business Continuity Management (27 Jul 2016)	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.	2016		Enf	"... An institution should ensure that its business continuity is not compromised by outsourcing arrangements, in particular, of the operation of its critical systems as stipulated under the Technology Risk Management Notice. An institution should adopt the sound practices and standards contained in the Business Continuity Management ("BCM") Guidelines issued by MAS, in evaluating the impact of outsourcing on its risk profile and for effective BCM. ..."	www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.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.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/BCMGuidelines.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
MO-002-2017	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	2017		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://apps.neb-one.gc.ca/REGDOCS/Item/Filing/A81701				✓				
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.	Oct - 2006		Enf		http://mfda.ca/notice/msn-0056/	✓							
MS 1970:2007 BUSINESS CONTINUITY MANAGEMENT FRAMEWORK	Std	MALAYSIAN STANDARD	Malaysia	MS 1970:2007 BUSINESS CONTINUITY MANAGEMENT-FRAMEWORK available for purchase from site	2007		Enf		http://www.bki.my/standards/ms-1970-business-continuity-management-framework	✓	✓	✓	✓	✓	✓	✓	✓
NASD Rule 108 (Sept 9, 02) and SR-NASD-2002-112 (March 10, 03) Business Continuity Plans and Emergency Contact Information (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	Note: While the link is still valid, it is our understanding that NASD was replaced by FINRA. Working to confirm what replaced this besides usual 4370 rule.	http://www.sec.gov/rules/sro/34-48503.htm	✓							
National Continuity Programs	Std	FEMA	U.S.A.	The Federal Emergency Management Agency's National Continuity Programs (NCP) serves the public by coordinating the federal programs and activities that preserve our nation's essential functions across a wide range of potential threats and emergencies. On behalf of the White House, the Secretary of Homeland Security, and the FEMA Administrator, NCP guides and assists the planning and implementation of continuity programs that enable federal, state, tribal, territorial, and local governments to deliver critical services to survivors throughout all phases of a disaster. Continuity and sustainment of essential functions is a shared responsibility of the whole community. Development and maintenance of continuity capabilities helps build and sustain a more resilient nation equipped to sustain essential functions, deliver critical services, and supply core capabilities under all conditions.	Aug 2019		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"). Includes links to: National Security Presidential Directive-51/Homeland Security Presidential Directive-20 National Continuity Policy Implementation Plan National Communications System Directive (NCSD) 3-10 Federal Continuity Directive (FCD) 1 Federal Continuity Directive (FCD) 2 Continuity Guidance Circular (CGC) 1 Continuity Guidance Circular (CGC) 2 FEMA Continuity Planning Guidance	https://www.fema.gov/national-conti	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
National Instrument 21-101 Marketplace Operation; and National Instrument 31-103 Registration Requirements and Exemptions	Reg	Ontario Securities Commission (OSC)	Canada	Part 12 of NI 21-101 addresses marketplace systems and business continuity planning. It requires that each system operated by or on behalf of the marketplace that supports order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing must develop and maintain business continuity plans in accordance with business practices at least once a year. It also states that the regulator must be promptly notified of any material systems failure, malfunction, delay or security breach along with timely updates on status. Subsection 12.1(a,b,c) of National Instrument 21-101 Marketplace Operation requires marketplaces to develop and maintain an adequate system of internal controls and information technology controls over the systems and auxillary systems. It also requires prompt notification to the regulator its regulation service provider of any material systems failures. Subsection 12.2 requires that the marketplace to annual engage a specified party to conduct independent systems review and prepare a report in accordance with audit standards. The report must be provided to its board of directors and the regulator. Subsection 12.3 requires the marketplace to make publically available all technology requirements regarding interfacing and accessing the marketplace in its final form. Subsection 12.4 requires the marketplace to provide uniform test symbols. Subsection 12.5 requires the marketplace to develop, maintain, and test reasonable business continuity plans to include disaster recovery plans. 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 business in accordance with prudent business practices.	Feb-2013		Enf	Only applied to financial institutions registered in Ontario	http://www.osc.gov.on.ca/en/13537.htm http://www.osc.gov.on.ca/en/SecuritiesLaw_31-103.htm	✓							
NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan	Reg	CFTC (Commodity Futures Trading Commission)	U.S.A.	Requires each member to: a) 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. b) provide NFA with, and keep current, the name and contact information for all key management employees. c) provide NFA with the name of and contact information for an individual who NFA can contact in the event of an emergency.	2016		Enf		http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=RULE 2-38&Section=4	✓							
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 (SEPSS) up to the load terminals of the transfer switch. Specific topics include definitions of the classification of SEPSS; energy sources, converters, inverters, and accessories; transfer switches and protection; installation and environmental considerations; and routine maintenance and operational testing.	2019		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 minimal 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. The standard provides requirements for a variety of categories of records storage environments. The standard also provides the requirements for the application of the types of records protection equipment.	2017		Wat		https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=232	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
NFPA Standard 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs	Std	NFPA (National Fire Protection Association	U.S.A.	NFPAA Standard 1600 establishes a common set of criteria for all hazards disaster/emergency management and business continuity programs. The standard includes government at distict levels, commercial business and industry, not-for-profit, and nongovernental organizations as well as individual citizens.	2019		Wat		https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600	✓	✓	✓	✓	✓	✓	✓	✓
NIST SP 800-34 Contingency Planning Guide for Federal Information Systems	Std	NIST (National Institute of Standards and Technology)	U.S.A.	· 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.	May 2010		Enf		http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf	✓	✓	✓	✓	✓	✓	✓	✓
NIST SP 800-53 r5 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 components9 of an information system that process, store, or transmit federal information. The guidelines have been developed to achieve more secure information systems and effective risk management within the federal government	Aug 2017		Enf		https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.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 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 valuable tool to the entire organization in addition to the information technology department.	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 Handbook. This booklet provides guidance to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.	http://ithandbook.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
OCC 2013-29: Third-Party Relationships - Risk Management Guidance (October 30, 2013)	Reg	OCC	U.S.A.	This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise 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 problems affecting the third party's perations, including system breakdown and natural (or man-made) disaster.	Oct 2013				https://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.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.	2009		Enf		http://www.osfi-bsif.gc.ca/Eng/Docs/b10.pdf	✓							
OSFI Guideline B-9 - Earthquake Exposure Sound Practices	Reg	Office of the Superintendent of Financial Institutions Canada (OSFI)	Canada	Insurers must have contingency plans in place to ensure continued efficient business operations. The contingency plan should address the key elements of claims management, such as emergency communications links, availability and adequacy of claims and adjustment service personnel, and off-site systems back-up, that also includes reinsurance records.	2013		Enf	Document define OSFI's expectations relating to P&C insurers' earthquake exposure risk management. This guideline outlines the framework for quantifying earthquake exposures for regulatory purposes and assessing insurers' capacity and financial preparedness to meet contractual obligations that may arise from a major earthquake.	http://www.osfi-bsif.gc.ca/Eng/Docs/b9.pdf	✓							
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 OSHA-approved occupational safety and health plans that may have more stringent requirements than what Federal OSHA requires.	Nov 2002		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=STANDARDS&p_id=9726	✓	✓	✓	✓	✓	✓	✓	

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
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 to the appropriate personnel, and maintain and periodically review the combined plan.	2015		Wat	NOTE: Although the webpage indicates 2007 as the previous revision, one of the Word versions (when opened) states 2015. 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 specific responsibilities of all parties, particularly in the areas of information security and business continuity planning.	http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx	✓							
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. Business continuity risk management - The Bank's business continuity management (BCM) programme is based on the BCM lifecycle model, as defined by the Business Continuity Institute UK. This is widely recognised as the international good practice guideline for BCM development and management. The Business Continuity Institute's lifecycle model consists of the following elements: BCM policy and programme management Embedding BCM in the organisation's culture Understanding the organisation Determining BCM strategy Developing and implementing a BCM response Exercising, maintaining and reviewing	2010		Enf		https://www.resbank.co.za/AboutUs/RiskManagement/Pages/RiskManagementApproachAndMethodology-.aspx https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Documents/Oversight/Oversight.pdf	✓							
Procedure of Implementation of Prevention of Emergencies	Reg	Government of the Republic of Lithuania	Lithuania	The procedure of implementation of prevention of emergencies shall regulate the procedure of establishment, planning, implementation and control of emergency preparedness measures of state and municipal institutions and agencies, economic entities and other agencies that are designed to eliminate emergencies or reduce the possibility of their occurrence and, in the event of an emergency, to mitigate its consequences.	2017		Enf		https://e-seimas.lrs.lt/rs/legalact/TAD/702d015216b811e6aa14e8b63147ee94/format/ISO_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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Recommendations for National Risk Assessment for Disaster Risk Management in EU	GP	The Joint Research Centre is the European Commission's science and knowledge service	European Union	The Disaster Risk Management Centre has produced in the collaboration with more than 20 scientists the Science for Policy Report titled "Recommendations for National Risk Assessment for Disaster Risk Management in EU: Approaches for identifying, analysing and evaluating risks, Version 0". This Science for Policy report aims to provide scientific support to the Union Civil Protection Mechanism Participating States and national authorities in charge of the preparation of National Risk Assessment process.	2019		Enf	This Science for Policy Report contributes to common understanding on what risk is and how to quantify it for different hazards. This Science for Policy Report collects the instructions for robust and usable approaches for the risk assessment process in the context of National Risk Assessment and to inform Disaster Risk Management planning. Nine Joint Research Centre expert groups provided their insight on tools and methods for specific risk assessment related to certain hazards and assets: drought, earthquakes, floods, terrorist attacks, biological disasters, critical infrastructures, chemical accidents, nuclear accidents and Natech accidents. The overall aim is to maximize the national capacity of a country in achieving the objectives National Risk Assessment process. NRAs should define the relative importance of different risks (potential impacts) in the country as well as identify disaster risk drivers to address a range of measure to reduce risk.	https://drmkc.jrc.ec.europa.eu/knowledge/science-for-drm/recommendations-for-national-risk-assessment-for-disaster-risk-management-in-eu	✓	✓	✓	✓	✓	✓	✓	✓
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.	19-Jan		Enf		https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-6-Contingency-Planning.pdf		✓						✓
Science for Disaster Risk Management 2017: Knowing better and losing less	GP	The Joint Research Centre is the European Commission's science and knowledge service	European Union	This report will present the state of science in DRM. The narrower purpose is to show practical use of scientific knowledge in DRM actions in Europe. The report shall provide reviews of the scientific evidence base and its practical use in various areas of disaster risk management, in a format that is intended to be accessible to the well-informed practitioner. The reviews of the scientific evidence base are summaries of (1) recent advances/outcomes of EU research projects, (2) relevant national work and (3) relevant international work.The final scope of the report is naturally divided into three distinct parts: understanding risk, communicating risk and managing risk. The report is one of the most visible objectives of DRMKC aiming to bridge science and policy as well operatoin communities. It is the first in a series and therefore comprehensive in scope but selective in topic. It will fill the gap in preparation for Sendai framework for DRR and show posibilites to strengthen society's resilience by using science and technology.	2017		Enf		https://ec.europa.eu/jrc/en/publication/science-disaster-risk-management-2017-knowing-better-and-losing-less	✓	✓	✓	✓	✓	✓	✓	✓

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
SEC Adviser Business Continuity and Transition Planning PROPOSED Rule	Reg	Securities and Exchange Commission (SEC)	U.S.A.	PROPOSED new rule and rule amendments under the Investment Advisers Act of 1940 ("Advisers Act") that would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations.	Jun-16		Wat	NEW for Spring 2019: The SEC has invited feedback on the proposed rule. Below is an excerpt from the rule: "Proper planning and preparation for possible distress and other significant disruptions in an adviser's operations is essential so that, if an entity has to exit the market, it can do so in an orderly manner, with minimal or no impact on its clients. As discussed above, an adviser's fiduciary duty obligates it to take steps to protect client interests from being placed at risk as a result of the adviser's inability to provide advisory services and, thus, it SEC-registered advisers should be required to adopt and implement a written business continuity and transition plan that is tailored to the risks associated with the adviser's operations and includes certain components, reflecting its critical role as an agent for its clients."	https://www.sec.gov/rules/proposed/2016/ia-4439.pdf	✓							
SEC Adviser Business Continuity and Transition Planning PROPOSED Rule	Reg	Securities and Exchange Commission (SEC)	U.S.A.	PROPOSED new rule and rule amendments under the Investment Advisers Act of 1940 ("Advisers Act") that would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations.	Jul 2016		Wat	NEW for Spring 2019: The SEC has invited feedback on the proposed rule. Below is an excerpt from the rule: "Proper planning and preparation for possible distress and other significant disruptions in an adviser's operations is essential so that, if an entity has to exit the market, it can do so in an orderly manner, with minimal or no impact on its clients. As discussed above, an adviser's fiduciary duty obligates it to take steps to protect client interests from being placed at risk as a result of the adviser's inability to provide advisory services and, thus, it SEC-registered advisers should be required to adopt and implement a written business continuity and transition plan that is tailored to the risks associated with the adviser's operations and includes certain components, reflecting its critical role as an agent for its clients."	https://www.sec.gov/rules/proposed/2016/ia-4439.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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost (will be ready by April 2020)	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when ckicking on the cell, please try copying the link to your web browser)	Infrastructure Category: Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
SEC Regulation SCI	Reg	Securities and Exchange Commission (SEC)	U.S.A.	**Background** The U.S. Securities and Exchange Commission adopted Regulation Systems Compliance and Integrity and Form SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. Specifically, the rules are designed to: Reduce the occurrence of systems issues; Improve resiliency when systems problems do occur; Enhance the Commission's oversight and enforcement of securities market technology infrastructure. **Who Regulation SCI applies to** Regulation SCI applies to "SCI entities," a term which includes self-regulatory organizations ("SROs"), including stock and options exchanges, registered clearing agencies, FINRA and the MSRB, alternative trading systems ("ATSs"), that trade NMS and non-NMS stocks exceeding specified volume thresholds, disseminators of consolidated market data ("plan processors"), and certain exempt clearing agencies. **What Regulation SCI applies to** Regulation SCI applies primarily to the systems of SCI entities that directly support any one of six key securities market functions - trading, clearance and settlement, order routing, market data, market regulation, and market surveillance ("SCI systems"). Subject to certain exceptions, the compliance date of Regulation SCI was nine months after the effective date of the regulation, or November 3, 2015.	Nov 2014		Enf	The SEC designed Regulation SCI in response to securities markets being increasingly dependent on technology and automated systems. Regulation SCI strives to reduce the number of market disturbances stemming from this reliance on technology, as well as speed up recovery when disturbances do occur.	This is the location of the published final rule: Securities and Exchange Commission -- SEC Final Rules 2014 https://www.sec.gov/rules/final/finalarchive/finalarchive2014.shtml Select Release 34-73639 (Nov 19, 2014) for a pdf of the rule This is the location of the rule correction: Securities and Exchange Commission -- SEC Final Rules 2015 https://www.sec.gov/rules/final/finalarchive/finalarchive2015.shtml Select Release 34-73639A (Dec 22, 2015) for a pdf of the rule correction	✓							

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: September 22, 2019

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 governing body.

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:

www.avalution.com/business-continuity-standards-regulations
www.avalution.com/iso-22301
https://www.thebci.org/uploads/assets/uploaded/c203e090-8f23-4f3a-8b7f6f67c62c3a50.pdf
www.bcmpedia.org/wiki/Standards
www.gartner.com/doc/483265/laws-influence-business-continuity-disaster
www.gartner.com/id=483265
www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses
www.informit.com/articles/article.aspx?p=777896

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
CMS	U.S.A.	Centers for Medicare and Medicaid Servicess
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)
DMISA	South Africa	Disaster Management in South Africa, is the professional body for SA.
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
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
GAP	U.S.A.	Generally Accepted Practice
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
MFDA	Canada	Mutual Fund Dealer Association (of Canada)
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
RBI	India	Reserve Bank of India
SAMOS	South Africa	South African Multiple Option Settlement (SAMOS) system is South African's Real Time Gross Settlement (RTGS) System.
SAS	U.S.A.	Statement on Auditing Standards
SEBI	India	Securities & Exchange Board of India
SEC	U.S.A.	Securities and Exchange Commission
SIFMA	U.S.A.	Securities Industry and Financial Markets Association

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: September 22, 2019

Country	Number of Rules & Regulatuons 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	2	0	2	0	0	0	0	0	0	2
Australia, New Zealand	6	0	6	4	4	4	4	4	4	0
Canada	18	0	11	3	3	4	3	3	3	5
Croatia	1	0	1	0	0	0	0	0	0	1
European Union	9	0	5	9	9	9	9	7	6	0
Hong Kong	3	0	2	0	0	0	0	0	0	1
India	-	0	0	0	0	0	0	0	0	4
Indonesia	1	0	1	0	0	0	0	0	0	0
International	16	0	10	8	8	8	14	8	8	3
Japan	1	0	1	0	0	0	0	0	0	2
Lithuania	1	0	1	1	1	1	1	1	1	0
Malaysia	3	0	3	2	2	2	2	2	2	0
Philippines	2	0	2	0	0	0	0	0	0	0
Singapore	3	0	3	0	0	0	0	0	0	1
South Africa	7	0	6	4	4	4	5	4	4	2
U.K.	3	0	3	1	1	1	1	1	1	2
U.S.A.	56	0	48	25	19	19	20	19	25	36
Total	**132**									**59**

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	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=AS0733759041AT 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=AS0733759041AT 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/Hinchcliffe.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.w3j.com/xml/

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
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) superceds Federal Home Loan Bank Bulletin R-67.	
Business Continuity Planning Committee Best Practice Guidelines (April 2011)	Std	ISIA (International Securities Industry Association)	International	Presents guidelines that can assist in the establishment of a comprehensive business continuity program. It is not intended to be an outline of a business continuity plan or as a single best approach, but rather it should be viewed as a summary of significant components that an organization may wish to consider when developing a full business continuity program.	Apr-2011	Wat	As of March 2016, no longer found, only remaining tace is an article from 2002 annoucing it: http://www.wallstreetandtech.com/risk-management/sia-releases-business-continuity-planning-best-practices/d/d-id/1255508	http://www.sifma.org/uploadedfiles/services/bcp/sifma-bc-practices-guidelines2011-04.pdf
Croation Sabor: Set of related laws	Reg	Croatian Sabor (Parliament)	Croatia	Set of following Croatian Laws: Law on Minimum Protection Measures in Dealing with Cash and Valuables Law on Personal Data Protection Law on Safety at Work Law on Fire Protection Law on Protection and Rescue	2013	Enf	September 2016 - These laws may still be enforce, but no link could be found. IF anyone can provide links to these it may be added back to the R&R data base.	http://www.hnb.hr/propisi/hpropisi.htm
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.	2002	Enf	A draft bill including amendments to the Disaster Management Act is expected to be presented to Parliament in 2013. September 2016 - These laws may still be enforce, but no link could be found. IF anyone can provide links to these it may be added back to the R&R data base.	http://disaster.co.za/index.php?id=25

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
FFIEC Policy SP-5	Reg	FFIEC	U.S.A.	Policy mandating corporate-wide contingency planning, including the development of recovery alternatives for distributed processing and service bureau information processing.	Mar-1997	Enf	With the issuance of the new FFIEC Information Technology Examination Handbook, several Supervisory Policies (SP) found in Chapter 25 of the 1996 Handbook have been rescinded, including SP-5, Interagency Policy on Contingency Planning for Financial Institutions. Issued July 1989.	http://www.bankersonline.com/security/sec_ffiecsp5.html
Foreign Corrupt Practices Act of 1977: (P.L. 95-213) Section 13 (b) (2).	Reg	US Dept of Justice	U.S.A.	Policy states that Directors and Officers can be held liable for "failure to enact standards of care" and should they fail to document their assessment processing determining not to develop a contingency plan. Since 1977, the anti-bribery provisions of the FCPA have applied to all U.S. persons and certain foreign issuers of securities. With the enactment of certain amendments in 1998, the anti-bribery provisions of the FCPA now also apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States.	1998	~~IAI~~	Foreign Corrupt Practices Act of 1977 · Civil penalties can range from $5000 to $100,000 for individuals and from $50,000 to $500,000 for business entities · Criminal sanctions may be imposed against anyone who knowingly violates the statute: up to $2 million in fines	http://www.justice.gov/criminal/fraud/fcpa/
FRB (Federal Reserve Banks) SR 96-22 - Inactive		Board of Governors of the Federal Reserve System	U.S.A.	Inactive: Reviews and enforces the FFIEC's Interagency Supervisory Statement on Risk Management of Client/Server Systems SP-12. · The statement addresses concerns for security and the controls that should be associated with client/server computing for the officer in charge of each federal reserve bank, including: · Management should ensure that systems and operations are recoverable after an event causing disruption in service. · Management should determine that database management system has adequate recovery capabilities	Jul-2012		April 12, 2012 - Federal Reserve Board staff have identified certain previously issued guidance that should now be inactive. Forty-three SR letters have been determined to be inactive and no longer applicable to the Federal Reserve's supervision program.	"http://www.federalreserve.gov/bankinforeg/srletters/sr1206.pdf" FILE HAS BEEN REMOVED
GAO Supplier Requirements	Reg	GAO (Government Accountability Office)	U.S.A.	Requirements for federal agencies to include the requirement for contingency plans in contracts with private sector organizations providing data processing services.	1998	~~Enf~~	Will apply to all organizations providing suppliers or services to GAO or Federal Agencies	http://www.gao.gov/special.pubs/bcpguide.pdf

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
Guidance Note on the Use of Internet for Insurance Activities (GN8)	Reg	Office of the Commissioner of Insurance - The Government of the Hong Kong Special Administrative Region	Hong Kong	Point 11 address the issue of security in which service providers are advised to take all practicable steps to ensure a number of items including the integrity of data stored in the system hardware, whilst in transit and as displayed on the website (a), a	2001	~~Enf~~	The scope of this Guidance Note covers the internet insurance activities of all service providers to the extent that such activities fall within the jurisdiction of Hong Kong.	http://www.oci.gov.hk/download/gn8-eng.pdf
HB 221:2004 Handbook Business Continuity Management	GP	Jointly published by Standards Australia and Standards New Zealand	Australia, New Zealand	The objective of this Handbook is to outline a broad framework and core processes that should be included in a comprehensive business continuity process. Sets out a definition and process for business continuity management, and provides a workbook that may be used by organisations to assist in implementation.	2004	~~IAI~~	**Withdrawn Date: 19 Aug 2013** supersedes HB 221: 2003. Aligned with the 2004 edition of AS/NZS 4360, Risk management.	http://infostore.saiglobal.com/store/Details.aspx?docn=AS0733762506AT
HB 293—2006 Executive Guide to Business Continuity Management	Std	Standards Association of Australia	Australia, New Zealand	The executive guide to business continuity management (BCM) provides senior management with an overview of the key concepts and processes that are required to implement and maintain an integrated, robust business continuity management program. This document was prepared as a summary and a navigational tool for HB 292, A practitioners guide to business continuity management.	Jun-1905	Wat	The link is to a 6 page sample of the document which may be purchased from SAI Global at http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB293-2006.pdf	http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB293-2006.pdf
HKMA Supervisory Policy Manual, BCP TM-G-2 V.1 02.12.02	Reg	Hong Kong Monetary Authority	Hong Kong	Enforced by onsite examinations, requires need for BCP documentation and testing at least annually, planning for different scenarios and prolong outages.		Enf	BCP organization & governance structure Approach to business continuity planning Documentation DR site & vendor management	http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/circulars/2002/20021202-1.shtml
HKMA Supervisory Policy Manual, General Principles for Technology Risk Management TM-G-1 V.1 24.06.03	Reg	Hong Kong Monetary Authority	Hong Kong	Refers to TM-G-2 on BCP on the need to provide continuous service.	Jun-1905	Enf	Link references same website as above. Need to provide alternative service	http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/circulars/2003/20030624-1.shtml

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
Homeland Security Strategy for Critical Infrastructure Protection in Financial Services Sector (May 2004)	Std	FSSCC (Financial Services Sector Coordinating Council for Critical Infrastructure Protection)	U.S.A.	Ensuring the resiliency of the nation to minimize the damage and expedite the recovery from attacks that do occur. ~~https://www.fsscc.org/fsscc/reports/2006/Bank_Finance_SSP_061213.pdf~~	Wat		TO BE DELETED: This is generic reference to "Homeland Security Strategy for Critical Infrastructure Protection in Financial Services Sector" and currently has been replaced by SIFMA BCP Expanded Practices Guidelines (already included in our list)	http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-7844:1 http://www.sifma.org/services/business_continuity/pdf/NationalStrategy.pdf (THIS PAGE WAS NOT FOUND)
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-97	IAI		https://www.thefreelibrary.com/Record+retention+under+rev.+proc.+91-59%3a+a+checklist+approach.-a013984355
ISO/TS 9002:2016 Quality management systems - Guidelines for the application of ISO 9001:2015	Std	ISO (International Organization for Standardization)	International	ISO 9001:2015 - Quality management systems - Guidelines for the application of iso 9001. ISO/TS 9002:2016 provides guidance on the intent of the requirements in ISO 9001:2015, with examples of possible steps an organization can take to meet the requirements. It does not add to, subtract from, or in any way modify those requirements. ISO/TS 9002:2016 does not prescribe mandatory approaches to implementation, or provide any preferred method of interpretation.	Nov 2016	Wat	**ISO 9002 is obsolete.** The three standards (ISO 9001, ISO9002, and ISO 9003) were combined into ISO 9001 in the year 2000 revision (ISO 9001:2000) which was replaced by ISO 9001:2008. ISO 9002:1987 Model for quality assurance in production, installation, and servicing had basically the same material as ISO 9001 but without covering the creation of new products.	https://committee.iso.org/home/tc176sc2 https://webstore.ansi.org/sdo/ISO

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
MAS SPRING Singapore BCM Fact Sheet 2006	Reg	MAS (Monetary Authority of Singapore)	Singapore	Rule 3.5.4(1) requires Clearing Members to maintain adequate business continuity arrangements, and document such arrangements in a business continuity plan.		Enf	Not found on site	http://info.sgx.com/SGXRuleb.nsf/VwCPForm_CDP_CLEARING_RULES_Download/CDP%20Clearing%20Rules%20Practice%20Note%2003.05.04%20-%20Business%20Continuity%20Requirements.pdf
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 create and maintain a written business continuity plan that identifies procedures related to an emergency or significant business disruption. The plan must be updated in the event of any material change to operations, structure, business, or location. Any annual review must be conducted of the business continuity plan to determine any modifications that are necessary. Each plan must address, at a minimum, the 10 elements listed in the rules. NASD members must designate a member of the senior management to approve the plan and disclose to their customers how its business continuity plan addresses significant business interruptions. Each NASD member must provide FINRA 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 FINRA may contact in the emergency. FINRA Rule 4370: Business Continuity Plans and Emergency Contact Information.	Feb-2015		Enf	
NYSE Rule 446: Business Continuity and Contingency Planning	Reg	NYSE (New York Stock Exchange)	U.S.A.	· Members and member organizations must develop and maintain a written business continuity and contingency plan establishing procedures to be followed in the event of an emergency or disruption. · Yearly review must be conducted of the business continuity - Amended in September, 2008.		Enf	NYSE Rule 446 is no longer current. The NYSE, along with NASD, has adopted FINRA Rule 4370.	http://www.sec.gov/rules/sro/34-48502.htm

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
OCC 2013-29: Third-Party Relationships (October 30, 2013)	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 problems affecting the third party's perations, including system breakdown and natural (or man-made) disaster.	Oct 2013		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	https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
OCC 99-9: Infrastructure	Reg	OCC	U.S.A.	· Identifies and raises awareness of vulnerabilities and threats of cyber terrorism to the financial services industry, including ensuring that these threats are taken into account when preparing and testing a disaster recovery/business contingency · Exp		Enf		http://www.occ.treas.gov/ftp/bulletin/99-9.txt
Prudent Man Concept	Reg	Common Law - Negligence Liability	International	· As per the Uniform Commercial Code, legal standard used to determine whether appropriate action was taken in a particular situation.		IAI	Uniform Commercial Code Any company, regardless of its industry, is expected to exercise due-care to implement and maintain security mechanisms and practices that protect the company, its employees, customers, and partners., Due-Care can be compared to the "prudent man" concept. A prudent man is seen as responsible, careful, cautious, and practical. A company practicing due-care is seen in the same light by State and Federal Courts.	http://www.oecd.org/finance/private-pensions/2763540.pdf
Public Finance Management Act, 1999- DRAFT Treasury Relations	Reg		South Africa	Unable to find anything specific to BC or DR… "availability of financial information" was included…				"http://www.acts.co.za/public_fin_man/index.htm" PAGE OR FILE HAS BEEN REMOVED

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: September 22, 2019

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link
Publicly Available Specification (PAS) 56- Guide to Business Continuity Management	Std	BSI (British Standards Institute)	U.K.	Publicly Available Specification, PAS 56, is an 'informal standard' that was published by the BSI in 2003.	2003	Enf	PAS56 has been replaced with BS 25999.	http://en.wikipedia.org/wiki/PAS_56
Publicly Available Specification (PAS) 56- Guide to Business Continuity Management	Std	BSI (British Standards Institute)	U.K.	Publicly Available Specification, PAS 56, is an 'informal standard' that was published by the BSI in 2003.	2003	Enf	PAS56 has been replaced with BS 25999.	http://en.wikipedia.org/wiki/PAS_56
Telecommunications Act of 1996	Reg	FCC - Federal Communications Commission	U.S.A.	The act was intended to promote competition in the telecommunications industry. Section 256 gives the FCC the right to oversee that telecommunications networks "seamlessly and transparently transmit and receive information between and across telecommunications networks."		~~Enf~~	The FCC's Network Reliability and Interoperability Council provides best practices for business continuity and disaster recovery in the telecommunications industry. (www.nric.org)	http://www.drj.com/article-archives/communications/the-impact-of-the-telecommunications-act-on-business-continuity-plans.html FILE OR PAGE HAS BEEN REMOVED