# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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<br>1. Crisis management. I. Lindsay, Hugh, 1941- II. Canadian Institute of Chartered Accountants<br>III. Title. IV. Title: Twenty questions directors should ask about crisis management.<br>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<br><br>· An ACH transaction is a batch-processed, value-dated electronic funds transfer between originating and receiving financial institutions | 1/1/2017 Appears to have a 2018 version, available for a subscription | IAI | Login is required to access, but non-member logins are granted and given read-only access.<br><br>Non-compliant fines not more than $10,000 or imprisoned not more than ten years, or both | http://www.achrulesonline.org/ | ✓ | | | | | | |
| Advisory on Business Continuity and Disaster Recovery Planning | GP | CFTC, SEC and FINRA | U.S.A. | The regulators encourage firms to consider implementing the best practices described, which the advisory groups into the following categories:<br>(1) widespread disruption considerations,<br>(2) alternative locations considerations,<br>(3) vendor relationships,<br>(4) telecommunications services and technology considerations,<br>(5) communications plans,<br>(6) regulatory and compliance considerations, and<br>(7) review and testing. | Oct 2012 | Enf | The CFTC, SEC, and FINRA have issued this advisory following their joint investigation into firms' business continuity and disaster recovery plans ("BCPs") in the wake of Hurricane Sandy. | http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/bcpstaffadvisory081613.pdf | ✓ | | | | | | |
| 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:<br>ANAO REPORT NO. 6 OF 2014–2015 Business Continuity Management<br>ANAO REPORT NO. 9 OF 2003–2004 Business Continuity Management and Emergency Management in Centrelink<br>ANAO REPORT NO. 46 OF 2008–2009 Business Continuity Management and Emergency Management in Centrelink<br>ANAO REPORT NO. 53 OF 2002–2003 Business Continuity Management Follow-on Audit<br>ANAO REPORT NO. 16 OF 2008–2009 The Australian Taxation Office's Administration of Business Continuity Management<br>SPEECH Published: Wednesday, February 23, 2000 Business Continuity Management: Opening remarks at a launch of a Better Practice Guide | Nov 2014 | Enf | | https://www.anao.gov.au/work/performance-audit/business-continuity-management#0-0-summary | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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.<br><br>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.<br><br>The Guide will be a useful reference document for boards, chief executives and senior management in public sector entities | Jun 2017 | Wat | Removed from ANAO Website July 1, 2017 - Link to support this removal updated in Column "I"<br><br>Publications from 2007 to 2015 | 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 | ✓ | | | | | | |
| 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 | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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<br><br>Related Guide: Good Management Practice - Information Security Set: 2017 (Nov 2017)<br><br>May be purchased from SAI Global | http://infostore.saiglobal.com/store/Details.aspx?productID=394887<br><br>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 | | | | | | | |
| 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. | Jan 2008 | Wat | Banks Act, 1990 (as amended): Reproduced under Government Printer's Copyright Authority No 10665 dated 19 March 1999 (effective 1 January 2008) | http://www.resbank.co.za/RegulationAndSupervision/BankSupervision/BankingLegislation/Pages/BanksAct.aspx | ✓ | | | | | | |
| 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 | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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:<br>- Canadian companies do not have to submit an external auditor attestation of the adequacy of internal controls.<br>- 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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.<br><br>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.<br><br>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.<br><br>Using agreed terminology, BS 65000:<br>• clarifies the meaning of resilience<br>• highlights the key components of resilience<br>• helps an organization to measure its resilience and make improvements<br>• 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=00000000030258792 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| BSP Circular Letter (2001) - Business Continuity Plan | Reg | The Bangko Sentral ng Pilipinas (BSP) (central bank of the Republic of the Philippines) | Philippines | Requires a comprehensive and updated business continuity plan as an integral part of a the risk management process of all financial institutions. The overall goal of this business continuity plan must be to (1) ensure that there will be minimal disruption of bank operations (2) to minimize financial losses through lost business opportunities or asset deterioration, and (3) to ensure a timely resumption of normal operations.<br><br>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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Business Continuity Management Audit/Assurance Program | GP | ISACA | International | Main subject areas of the DRI Professional Practices:<br>- Project Initiation and Management<br>- Risk Evaluation and Control<br>- Business Impart Analysis<br>- Developing Business Continuity Strategies<br>- Emergency Response and Operations<br>- Developing and Implementing Business Continuity Plans<br>- Awareness Programs and Training<br>- Maintaining and Exercising the Business Continuity Plans<br>- Crisis Communications<br>- 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<br>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.<br><br>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.<br><br>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/fileadmin/lautorite/reglementation/lignes-directrices-toutes-institutions/2010mars31-ld-gestion-continuite-en.pdf | ✓ | | | | | | |
| Business Continuity Planning (Bank of Japan) | Std | BOJ (Bank of Japan) | Japan | The Bank develops and continually revises business continuity plans for functions such as circulation of banknotes and operation of payment and settlement systems, in order to carry out its responsibilities in times of disaster. The Bank trains its staff and conducts emergency drills on a regular basis to ensure a timely and appropriate response.<br><br>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/ | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Business Continuity Planning Resources and Checklists Library | GP | Public Health and Safety, Government of Canada | Canada | Reference Library of links to Business Continuity Planning resources provided by different federal and provincial organizations in Canada | 2013 | Wat | | http://www.phac-aspc.gc.ca/influenza/bcp-eng.php | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| California SB 1386 - Security of Non-Encrypted Customer Information (July 1, 2003) | Reg | State of California | U.S.A. | Bill requires all agencies, persons or businesses that conduct business in California that owns or licenses computerized data containing personal information to notify the owner or licensee of the information of any breach of security of the data. | Jul 2003 | Enf | | http://www.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) | 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 | http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-318/page-39.html | | | ✓ | | | | |
| 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<br><br>http://www.bi.go.id/en/peraturan/perbankan/Documents/86336e7d954642a35851d1e058fc2c1194se_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<br>HKEx procedures & guidelines<br>Public Health | http://www.sfc.hk/web/EN/published-resources/business-continuity/<br><br>http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=H289 | ✓ | | | | | | |
| 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<br>- Duty to assess, plan and advise<br>- Advice and assistance to business<br>- Requires persons or bodies listed in the document to assess the risk of an emergency and maintain plans for the purpose of ensuring that if an emergency occurs that the persons or bodies are able to continue to | May 2012 | Enf | Amends or repeals older Civil Defense Acts, Emergency Powers Acts, and other related Acts | http://www.legislation.gov.uk/ukpga/2004/36/contents | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Civil Defence Emergency Management Act 2002 | Reg | Ministry of Civil Defence and Emergency Management | New Zealand | The purpose of this Act is to improve and promote the sustainable management of hazards in a way<br>that contributes to the social, economic, cultural, and environmental well-being and safety of the public and also to the protection of property; and<br>encourage and enable communities to achieve acceptable levels of risk. | Oct 2008 | Wat | Public Act 2002 No 33 - Reprint as of Aug 2017 | http://www.legislation.govt.nz/act/public/2002/0033/48.0/DLM149789.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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| CMS Final CY 2016 Rule Regarding Business Continuity | Reg | CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group | U.S.A. | Centers for Medicare and Medicaid Services (CMS) Business Partners Systems Security Manual Appendix C: An Approach to Business Continuity and Contingency Planning This appendix has been renamed to Medicare Information Technology (IT) Systems Contingency Planning. The title change and associated updates within the appendix reflect a new focus on IT systems when developing and testing contingency plans. The appendix outlines the steps to be followed by CMS business partner management, IT systems management and staff, and system security persons for recovering and continuing the operation of Medicare systems in an emergency. | 2002 | Enf | The Centers for Medicare and Medicaid Services (CMS) requires that its business partners implement information technology (IT) systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters. | https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/downloads/R2SSM.pdf | | ✓ | | | | | ✓ |
| CMS RMH VII 4.4 Contingency Plan Development | Reg | CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group | U.S.A. | Risk Management Handbook Volume II - Procedure 4.4 Contingency Plan Development The purpose of the Centers for Medicare & Medicaid Services (CMS) Contingency Plan (CP) Development Procedure is to provide CMS Business Owners, Information System Security Officers (ISSOs) and Contingency Plan Coordinators (CPCs) a systematic guide to coordinating, developing, and maintaining CPs. Additionally, this procedure will provide a contingency planning methodology that is integrated with the CMS eXpedited Life Cycle (XLC). Specifically, this procedure will provide guidance for consistently performing the following steps: - Determining IT recovery requirements in the form of Recovery Time Objectives (RTOs)1 and Recovery Point Objectives (RPOs)2 - Determining the most effective recovery strategies. - Developing and maintaining complete and executable CPs. | 2014 | Enf | | https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Vol-II-Procedure-4-4-Contingency-Plan-Development.html | | ✓ | | | | | ✓ |
| COBIT-Control Objectives for information and related Technology | Std | IT Governance Institute Standards | U.S.A. | COBIT is the the globally accepted framework that provides a comprehensive business view of the governance and management of enterprise IT (GEIT). In particular: -Maintain IT-related risk at an acceptable level -Support compliance with relevant laws, regulations, contractual agreements and policies | Apr 2012 | Enf | COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO). | http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Computer Fraud and Abuse Act | Reg | FTC (Federal Trade Commission) | U.S.A. | Makes it a federal offense to produce, buy, sell or transfer a credit card or other access devices that are counterfeit, forged, lost or stolen; or to produce, buy, sell, transfer or process equipment used to produce such fraudulent access devices. | 37165 | Enf | Section 1030. Fraud and related activity in connection with computers<br><br>(EXAMPLES OF FINES/PUNISHMENT ASSOCIATED WITH THIS LAW) The punishment for an offense under subsection (a) or (b) of this section is (A)...a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section..... (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) | http://www.panix.com/~eck/computer-fraud-act.html | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Consumer Credit Protection Act (CCPA) of 1992, Section 2001 Title IX- Electronic Funds Transfer | Reg | | U.S.A. | The purpose is to promote the availability of credit to all creditworthy applicants without regard to race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract); to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The regulation prohibits creditor practices that discriminate on the basis of any of these factors. The regulation also requires creditors to notify applicants of action taken on their applications; to report credit history in the names of both spouses on an account; to retain records of credit applications; to collect information about the applicant's race and other personal characteristics in applications for certain dwelling-related loans; and to provide applicants with copies of appraisal reports used in connection with credit transactions. | Dec 2011 | IAI | · Takes effect upon the expiration of eighteen months from the date of its enactment, except that sections 909 and 911 take effect upon the expiration of ninety days after the date of enactment<br><br>· Non-compliant fines not more than $10,000 or imprisoned | https://www.fdic.gov/regulations/laws/rules/6000-1350.html#fdic6000titlexeft | ✓ | | | | | | |
| COSO Enterprise Risk Management Framework (September 2015) | Std | COSO (Committee of Sponsoring Organizations of the Treadway Commission) | U.S.A. | Defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management. | 2017 | Enf | Guidance:<br>- Governance & Operational Performance<br>- Internal Controls<br>- Enterprise Risk Mgmt | http://www.coso.org/guidance.htm<br><br>http://www.coso.org/-ERM.htm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Criminal Code Act 1995 (consolidated as of 7 June 2010) | Reg | Australian Government | Australia | WIPO: World Intellectual Property Organization<br>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. | Jun 2010 | Enf | 1995 act has had numerous revisions. Revision 12, Part 2.5 is referenced here Supersedes 1994 Code | http://www.wipo.int/wipolex/en/text.jsp?file_id=205531 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Croatian National Bank: Set of CNB Decisions | Reg | Croatian National Bank (CNB) | Croatia | Set of following CNB Decisions:<br>Decision on adequate information system management<br>Decision on risk management<br>Decision on outsourcing<br>Decision on amendments to the Decision on outsourcing | 2010 | Enf | Documents (EN/HR) available for download | https://www.hnb.hr/en/document-preview?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=527005&_101_type=document<br><br>https://www.hnb.hr/documents/20182/525873/e-odluka-o-upravljanju-rizicima.pdf/883642e7-7d14-429f-a878-d5dd1e30e429<br><br>https://www.hnb.hr/en/document-preview?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=527411&_101_type=document<br><br>https://www.hnb.hr/en/-/odluka-o-izmjenama-i-dopunama-odluke-o-eksternalizaciji | ✓ | | | | | | ✓ |
| Croation Sabor: Credit Institutions Act | Reg | Croatian National Bank (CNB) | Croatia | Credit Institutions Act | 2013 & 2015 | Enf | Document (EN/HR) available for download | https://www.hnb.hr/en/-/zakon-o-kreditnim-institucijama | ✓ | | | | | | |
| CTIA Emergency Preparedness/Disaster Recovery | Std | CTIA - 2013 | U.S.A. | · The CTIA (The Wireless Association)Policy & Initiatives Emergency Preparedness/Disaster Recovery<br>- Emergency Preparedness<br>and<br>PDF with a Emergency Preparedness Wireless Tips card. | Updates 2015 | Wat | This certification and industry standard is in the planning phase. CTIA is currently (May 2005) meeting with industry leads to discuss the feasibility of the requirements and verification method. | https://www.ctia.org/consumer-resources/emergency-preparedness<br><br>https://www.ctia.org/docs/default-source/default-document-library/ctia-emergency-preparedness-tips-v2.pdf | | | | | | | ✓ |
| Derivatives Regulation, RRQ, c I-14.01 | Reg | Regulations of Quebec | Canada | DIVISION II.3<br>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:<br>...<br>(3) they have developed an emergency and contingency plan to ensure business continuity. | Oct 2016 | Enf | | http://www.legisquebec.gouv.qc.ca/en/ShowDoc/cr/I-14.01,%20r.%201 | ✓ | | | | | | |
| Disaster Management Act 2002 | Reg | Ministry for Provincial & Local Government Disaster Management Act, 2002 | South Africa | Proposed national disaster management framework.<br><br>Provides for:<br><br>· An integrated and coordinated disaster management policy that focuses on preventing and reducing the risk of disasters, mitigating the severity of disasters, emergency preparedness, rapid | Jan 2003 | Enf | | http://disaster.co.za/index.php?id=25 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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. | Dec 2002 | Enf | A draft bill including amendments to the Disaster Management Act is expected to be presented to Parliament in 2013. | https://www.westerncape.gov.za/Text/2004/10/a57-02.pdf | | | | | ✓ | | |
| Disaster Management Act; 09-10-2015) - South Africa | Reg | Department of Labour (Republic of South Africa) | South Africa | Disaster Management Act (2002) – an integrated and 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<br>Vol. 433 Pretoria 30 July 2001 No. 22506<br><br>About South Africa ==========><br><br>DMISA is the professional body for Disaster Mmanagement in South Africa. | www.gov.za<br><br>http://www.gov.za/speeches/statement-occasion-disaster-management-institute-southern-africa-held-mosselbay-9-september<br><br>http://disaster.co.za/index.php?id=25 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Draft Malaysian Standard 2- Business Continuity Framework - 2006 | Reg | BNM - Bank Malaysia Central Bank | Malaysia | This Malaysian Standard Online was developed by the Working Group on Business Continuity Management under the authority of the Information Technology, Telecommunication and Multimedia Industry Standards Committee. | 2007 | Enf | | http://www.jsm.gov.my/standards;jsessionid=MpSSbaByJ7pNNeq+iumVnXn6.AS2-INSTANCE-01#.Woczdu_ruHthttp://www.jsm.gov.my/standards?p_p_auth=upXJr8de&p_p_id=77&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_77_struts_action=%2Fjournal_content_search%2Fsearch"<br><br>http://www.jsm.gov.my/standards?p_p_auth=upXJr8de&p_p_id=77&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_77_struts_action=%2Fjournal_content_search%2Fsearch | ✓ | | | | | | |
| DRI International<br><br>"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 | D | https://www.drii.org/certification/professionalprac.php | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| DRJ GAP Report | Std | DRJ Editorial Advisory Board | International | DRII/BCI Professional Practice Narrative<br>- 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 | Mar 2015 | | Best Practices will be compiled from submittals by experienced Business Continuity Professionals<br>from the public and private sectors, as well as user groups and/or related organizations, in regards to a cross walk of the the industry standards. | http://www.drj.com/GAP/gap.pdf | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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:<br>- Offering guidance and a standard approach to earthquake planning<br>- Providing a framework with which to prepare your organization for its specific earthquake vulnerabilities<br>- 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 | e-CFR (Electronic Code of Federal Regulations) | U.S.A. | · U.S. Govennment Publishing Office<br>- Continuity of operations for Critical Infrastructure<br>· Enhance security and resiliency of chemical facilities. | Aug 2018 | Wat | The purpose of this part is to enhance the security of our Nation by furthering the mission of the Department as provided in 6 U.S.C. §111(b)(1) and by lowering the risk posed by certain chemical facilities. | http://www.ecfr.gov/cgi-bin/text-idx?SID=a22236216120cb8f2ebc8f7888f44d25&mc=true&node=pt6.1.27&rgn=div5#se6.1.27_1100 | | | | | ✓ | | |
| e-CFR Part 29: Protected Critical Infrastructure Information (as of 08/16/2015) | Reg | e-CFR (Electronic Code of Federal Regulations) | U.S.A. | · Continuity of operations for Critical Infrastructure<br>· 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=a22236216120cb8f2ebc8f7888f44d25&mc=true&node=pt6.1.29&rgn=div5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Electronic Fund Transfer Act (EFTA) | Reg | OCC | U.S.A. | Business Continuity Planning Booklet Appendix J Update to FFIEC IT Examination 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 | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Emergency Management Act | Reg | Senate and House of Commons of Canada | Canada | Requires the Minister of Public Safety in Gov.Canada to:<br>establishing policies and programs for the preparation of emergency management plans;<br>control emergency management plans prepared by federal entities;<br>coordinating the federal response to an emergency;<br>coordinating federal and provincial emergency management activities<br>coordinating the provision of assistance to a province;<br>promoting a common approach to emergency management, including the adoption of standards and best practices; and<br>conducting exercises and providing emergency management education and training. | 5-Jul-18 | Enf | | http://laws-lois.justice.gc.ca/eng/acts/E-4.56/page-1.html | | | | | | | |
| Emergency Management and Civil Protection Act (EMPCA) | Reg | | Canada | Under Provincial legislation, the Emergency Management and Civil Protection Act (EMPCA) , every municipality in Ontario is required to have an Emergency Management Program. | 2009 | 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. | http://www.ercb.ca/regulations-and-directives/directives/directive071 | | | | ✓ | | | |
| Fair Credit Reporting Act | Reg | FTC (Federal Trade Commission) | U.S.A. | · Ensures credit information is accurate and up-to-date<br>· Designed to promote accuracy and ensure the privacy of the information used in consumer reports | 2016 | IAI | · Civil penalty of not more than $2,500 per violation<br>· 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 | Mar 1999 | 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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Federal Continuity Directives (FCDs) | Std | FEMA | U.S.A. | Federal Continuity was developed as a repository of information to guide governmental continuity planning efforts and to share information with private sector stakeholders about the importance of planning. The site provides an overarching framework for US Federal Agencies to develop and deploy actionable continuity strategies. Here you will find descriptions, documents, guidance, and worksheets necessary to comply with Federal Continuity mandates and to achieve a high level of preparedness. | May 2013 | Wat | Federal Continuity Directives (FCD) 1 and FCD 2 as they are HUGE in the Federal Government (they are the Executive Branch's "COOP Bibles" – 1 being the "what", and 2 being the "how").<br><br>Includes links to:<br>National Security Presidential Directive-51/Homeland Security Presidential Directive-20<br>National Continuity Policy Implementation Plan<br>National Communications System Directive (NCSD) 3-10<br>Federal Continuity Directive (FCD) 1<br>Federal Continuity Directive (FCD) 2<br>Continuity Guidance Circular (CGC) 1<br>Continuity Guidance Circular (CGC) 2<br>FEMA Continuity Planning Guidance | http://www.fema.gov/guidance-directives | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| FEMA 141: Emergency Management Guide for Business & Industry | Std | FEMA | U.S.A. | Designed to provide guidance for business and industry officials to respond and recover from disasters. 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)<br><br>"IT Examination Handbook" | Reg | FFIEC | U.S.A. | - Emphasizes that Business Continuity planning is about maintaining, resuming and recovering the whole Business<br>- planning should occur for a BCP<br>- Business Impact Analysis and Risk assessment are encouraged as the foundation of an effective BCP<br>- Testing | Feb 2015 | 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<br><br>http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Financial Conduct Authority Handbook | Std | Financial Conduct Authority (FCA) | U.S.A. | REC 3.16 The purpose of REC 3.16 is to ensure that the FSA receives a copy of the UK recognised body's plans and arrangements for ensuring business continuity if there are major problems with its computer systems.<br><br>External events and other changes (SYSC 13.8)Unexpected changes and business continuity management SYSC 3.2.19 G provides high level guidance on business continuity.<br><br>Outsourcing (SYSC 13.9)and 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. | Jan 2016 | | 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.<br><br>FSA is now 2 separate regulatory authorities - Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA). | https://www.handbook.fca.org.uk/handbook/ | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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. | Apr 2014 | IAI | Whoever violates any provision of law to which this section is made applicable by subsection (c) of this section shall be subject to a civil penalty in an amount assessed by the court in a civil action under this section.<br>(b) MAXIMUM AMOUNT OF PENALTY–<br>(1) GENERALLY– The amount of the civil penalty shall not exceed $1,000,000.<br>(2) SPECIAL RULE FOR CONTINUING VIOLATIONS– In the case of a continuing violation, the amount of the civil penalty may exceed the amount described in paragraph (1) but may not exceed the lesser of $1,000,000 per day or $5,000,000. | 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:<br>(1) Data back-up and recovery (hard copy and electronic);<br>(2) All mission critical systems;<br>(3) Financial and operational assessments;<br>(4) Alternate communications between customers and the member;<br>(5) Alternate communications between the member and its employees;<br>(6) Alternate physical location of employees;<br>(7) Critical business constituent, bank, and counter-party impact;<br>(8) Regulatory reporting;<br>(9) Communications with regulators; and<br>(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. The FINRA rule 4370 is the successor to the NASD rule 3510. | http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625 | ✓ | | | | | | |
| FINRA Rule 4370 - emergency preparedness rule | Std | Financial Industry Regulatory Authority (FINRA) | U.S.A. | Rule 4370—FINRA's emergency preparedness rule—requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information. This page provides general information related to BCPs for securities firms.<br>Educational Info:<br>FINRA Business Continuity Planning Template (podcast) - July 19, 2010<br>Pandemic Preparedness - Part II (podcast) - December 21, 2009<br>Pandemic Preparedness - Part I (podcast) - November 23, 2009<br>Small Firm Emergency Partner Program (podcast) - October 16, 2007<br>Business Continuity Planning: Recent Survey Findings (podcast) - February 1, 2007 | Feb 2015 | Enf | Replaces NYSE Rule 446. The NYSE, along with NASD, has adopted FINRA Rule 4370.<br><br>Education | http://www.finra.org/Industry/Issues/BusinessContinuity/<br><br>http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=8625 | ✓ | | | | | | |

# DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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. | Nov 3 2015 | Enf | New for Fall 2018:<br><br>Adopted by SR-FINRA-2015-046 eff. Nov. 3, 2015. | http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=12111 | ✓ | | | | | | |
| FISMA: Federal Information Security Management Act of 2002 | Reg | Federal Trade Commission (FTC) | U.S.A. | Title III of the E-Government Act (Public Law 107-347, passed in 202) 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.<br><br>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. | Jan 2003 | Enf | May apply to organizations and institutions communicating with, performing work for, on behalf of a federal agency. Link is for NIST site, which addresses FISMA requirements.<br><br>The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include:<br>FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems<br>FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems<br>SP 800-18: Guide for Developing Security Plans for Federal Information Systems and Organizations<br>SP 800-30: Guide for Conducting Risk Assessments<br>SP 800-37, Revision 1: Guide for Applying | https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002<br><br>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.<br>(Extends: Amended Interagency Guidance on the Internal Audit Function and its Outsourcing SR 03-5)<br>(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<br>banks, domestic bank and savings and loan holding companies, and U.S. operations of foreign<br>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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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 | ✓ | | | | | | |
| Gramm-Leach-Bliley Act of 1999, section 501 (b): (P.L. 106-102 1999 S 900) | Reg | Public Law | U.S.A. | Guidelines in this section address standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information. | Nov 1999 | Enf | Effective July 1, 2001; GLB compliance is mandatory; whether a financial institution discloses non-public information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity. | http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act<br><br>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.healthit.gov/safer/guide/sgo03/practice/cp10p/hipaa | 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 | | ✓ | | | | | ✓ |
| 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.<br><br>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 | | ✓ | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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.<br>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<br>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.<br><br>after July 31, 2006 all member firms must comply with this rule.<br><br>The Corporation, in its discretion, may require an annual review to be performed by a qualified third party. | 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)<br><br>OCC (Office of the Comptroller of the Currency)<br><br>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:<br><br>Rapid recovery and timely resumption of critical operations following a wide-scale disruption;<br><br>Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location; and<br><br>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.<br><br>For Significant Role Firms, the goal is no later than 2006. | http://www.sec.gov/news/studies/34-47638.htm | ✓ | | | | | | |

# DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| IRS Procedure 91-59<br><br>(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<br>o requirements for computer records containing tax information.H22<br>o Requires off-site protection and documentation of computer records maintaining tax information<br>o The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841 | Dec 1997 | IAI | | https://www.thefreelibrary.com/Record+retention+under+rev.+proc.+91-59%3a+a+checklist+approach.-a0139843355 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ISO 22301 Business Continuity Management | Std | ISO | International | ISO 22301 is the new international standard for business continuity management. It has been created in response to strong international interest in the original British Standard BS 25999-2 and other regional standards. And if you meet the requirements to gain certification, your organization will be recognized globally. Currently under review and will be replaced by ISO/CD22301 | 8/15/2018 | Wat | Document available for purchase. | http://www.iso.org/iso/catalogue_detail?csnumber=50038 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ISO 9000 | Std | ISO | International | ISO 9000:2000, Quality management systems - Fundamentals and vocabulary. covers the basics of what quality management systems are and also contains the core language of the ISO 9000 series of standards.<br><br>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. | Sep 2015 | Wat | | http://en.wikipedia.org/wiki/ISO_9000 | | | | | ✓ | | |
| ISO 9001 | Std | ISO | International | ISO 9001:2000 Quality management systems - Requirements is intended for use in any organization which designs, develops, manufactures, installs and/or services any product or provides any form of service. It provides a number of requirements which an organization needs to fulfill if it is to achieve customer satisfaction through consistent products and services which meet customer expectations. This is the only implementation for which third-party auditors may grant certifications. | Aug 2018 | Wat | | http://en.wikipedia.org/wiki/ISO_9001 | | | | | ✓ | | |
| ISO 9002, Quality assurance standard, | Std | ISO | International | Addresses risk management and continuity planning issues for compliance. | Sep 2015 | Wat | previous members of the ISO 9000 series 9002 and 9003 have been integrated into 9001 | http://en.wikipedia.org/wiki/ISO_9001 | | | | | ✓ | | |
| ISO 9004 Quality management sysetms - Guidelines for performance improvement | Std | ISO | International | ISO 9004:2000 Quality management systems - Guidelines for performance improvements. covers continual improvement. This gives you advice on what you could do to enhance a mature system. This standard very specifically states that it is not intended as a guide to implementation | Sep 2015 | Wat | Revised by ISO 9004:2009<br><br>http://www.iso.org/iso/catalogue_detail?csnumber=41014 | http://en.wikipedia.org/wiki/ISO_9004 | | | | | ✓ | | |
| ISO Guide 73:2009 | GP | ISO | International | Risk management -- Vocabulary | Jan 2016 | Wat | document available for purchase | http://www.iso.org/iso/catalogue_detail?csnumber=44651 | | | | | ✓ | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| ISO/IEC 27002:2005 | Std | ISO (International Organization for Standardization) | International | the standard contains the following twelve main sections<br>4. **Risk assessment**<br>5. **Security policy** – management direction<br>6. Organization of information security – **governance** of information security<br>7. **Asset management** – inventory and classification of information assets<br>8. **Human resources security** – security aspects for employees joining, moving and leaving an organization<br>9. **Physical and environmental security** – protection of the computer facilities<br>10. **Communications and operations management** – management of technical security controls in systems and networks<br>11. **Access control** – restriction of access rights to networks, systems, applications, functions and data<br>12. **Information systems acquisition, development and maintenance** – building security into applications<br>13. Information security **incident management** – anticipating and responding appropriately to information security breaches<br>14. **Business continuity management** – protecting, maintaining and recovering business-critical processes and systems<br>15. **Compliance** – ensuring conformance with information security policies, standards, laws and regulations<br><br>Within each section, information security controls and their objectives are specified and outlined. The information security controls are generally regarded as best practice means of achieving those objectives.<br><br>Areas reviewed include:<br><br>· Was BS17799 originally and proposed as ISO 7799. | 2013 | Wat | ISO/IEC 17799:2005: It has subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled Information technology - Security techniques - Code of practice for information security management | http://en.wikipedia.org/wiki/ISO_17799 | | | | ✓ | | | |
| ISO/IEC 27005:2011 | Std | ISO | International | Continuation of ISO 27000 series standard The purpose of ISO/IEC 27005 is to provide guidelines for information security risk management | 2011 | Wat | Published 2011 | http://www.iso27001security.com/html/27005.html http://www.27000.org/ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 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.<br><br>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.<br>http://www.ogcio.gov.hk/en/information_security/policy_and_guidelines/<br><br>V4.1 November 2008<br>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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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.<br><br>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.<br>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.<br>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 | | ✓ | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| King I Report - 1994<br>King II Report - 2002<br>King III 2009<br>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:<br><br>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.<br><br>The committee has released three King reports on corporate governance in South Africa:<br><br>1994 King I<br>2002 King II<br>2009 King III<br>2016 King IV | http://en.wikipedia.org/wiki/King_Committee<br><br>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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Malaysia Business Continuity Management Framework 2007 | Reg | BNM - Bank Malaysia Central Bank | Malaysia | This Malaysian Standard describes the structured process for developing a Business Continuity Management (BCM) framework. This framework is applicable to any organisation in any sector or industry. This Malaysian Standard describes the structured process for developing a Business Continuity Management (BCM) framework. This framework is applicable to any organisation in any sector or industry.<br><br>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<br><br>http://www.cybersecurity.my/data/content_files/13/169.pdf | ✓ | | | | | | |
| 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 | | 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 | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| MAS Business Continuity Management Guidelines (June 2003) | Reg | MAS (Monetary Authority of Singapore) | Singapore | 7 Guiding Principles on Senior Management responsibilities for BCM; embedding BCM into Business-as-usual activities, incorporating sound practices; testing BCP regularly, completely and meaningfully; developing recovery strategies and setting RTO for crit | Jun 2003 | Enf | | http://www.mas.gov.sg/regulations-and-financial-stability/regulations-guidance-and-licensing/securities-futures-and-funds-management/guidelines/2004/business-continuity-management-guidelines.aspx | ✓ | | | | | | |
| 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. …" | http://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.singaporestandardseshop.sg/product/product.aspx?id=082e0fce-df3e-420d-9c1a-b30ef4be33e7 | ✓ | | | | | | |
| 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.msonline.gov.my/catalog.php?score=checked&istc_id=74 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| NASD Rule 108 (Sept 9, 02) and SR-NASD-2002-112 (March 10, 03)<br><br>(Release No. 34-48503; File No. SR-NASD-2002-108) | Reg | NASD (North American Securities Dealers Association)/<br><br>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.<br><br>· 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 | ✓ | | | | | | |

# 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| NASD Rule 3510 has been superseded by FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3510: Business continuity Plans | Reg | NASD | U.S.A. | Requires a Business Continuity Plan addressing:<br>· Alternate communications between customers, firm and employees<br>· Business constituent, bank and counter party impact<br>· Regulatory Reporting<br>· Mission Critical Systems<br>· Operational and Finan | Feb-2015 | Enf | | http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625 | ✓ | | | | | | |
| NASD Rule 3520 has been superseded by FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3520: Emergency Contact Information | Reg | NASD | U.S.A. | NASD Rule 3520 has been superseded by FINRA Rule 4370. Rule 3520 requires NASD members to provide NASD with emergency contact information and to update any information upon the occurrence of a material change. The Rule requires members to designate two emergency contact persons that NASD may contact in the e | Feb-2015 | Enf | | http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=8625 | ✓ | | | | | | |
| National Instrument 21-101 Marketplace Operation; and<br><br>National Instrument 31-103 Registration Requirements and Exemptions | Reg | Ontario Securities Commission (OSC) | Canada | Securities regulations require that business continuity plans be tested regularly, to reflect current or potential developments. Subsection 12.1(b) of National Instrument 21-101 Marketplace Operation requires marketplaces to test their business continuity and disaster recovery plans on a reasonably frequent basis and, in any event, at least annually. In addition,subsection 11.1(b) of National Instrument 31-103 Registration Requirements and Exemptions requires a registered firm to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to manage the risks associated with its 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/6090.htm | ✓ | | | | | | |
| NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan | Reg | CFTC (Commodity Futures Trading Commission) | U.S.A. | Requires all National Futures Association members to establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant disruption. | 2016 | Enf | | http://www.nfa.futures.org/nfamanual/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. | 2016 | Wat | | http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=111&cookie%5Ftest=1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| NFPA 232: Standard on Protection of Records | Std | NFPA (National Fire Protection Association | U.S.A. | Code 232 standard provides requirements for records protection equipment and facilities and records-handling techniques that safeguard records in a variety of media forms from the hazards of fire and its associated effects. | 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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| NFPA Standard 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs | Std | NFPA (National Fire Protection Association | U.S.A. | Establishes minimum criteria for disaster management for the private and public sectors in the development of a program for effective disaster mitigation, preparedness, response and recovery. | 2016 | 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.<br><br>· 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 2001-47: Third-Party Relationships (November 1, 2001) | Reg | OCC | U.S.A. | This bulletin provides guidance to national banks on managing the risks that may arise from their business relationship with third parties. A third party's inability to deliver products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the bank to transaction risk. Lack of effective business resumption and contingency planning for such situations also increases the bank's transaction risk. The contract should provide for continuation of the business function in the event of problems affecting the third party's perations, including system breakdown and natural (or man-made) disaster. | Nov 2001 | | The bank's own contingency plan should address potential financial problems or insolvency of the third party.<br><br>As of May 17, 2012, this guidance applies to federal savings associations in addition to national banks | http://ithandbook.ffiec.gov/media/resources/3333/occ-bul_2001_47_third_party_relationships.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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| OCC 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 | ✓ | | | | | | ✓ |
| 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<br>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. | 2001 | 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/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b9.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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| 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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 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. | 2004 | Wat | NOTE: Although the webpage indicates 2007 as the previous revision, one of the Word versions (when opened) states 2011.<br><br>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.<br><br>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.<br><br>The Business Continuity Institute's lifecycle model consists of the following elements:<br>BCM policy and programme management<br>Embedding BCM in the organisation's culture<br>Understanding the organisation<br>Determining BCM strategy<br>Developing and implementing a BCM response<br>Exercising, maintaining and reviewing | 2010 | Enf | | https://www.resbank.co.za/AboutUs/RiskManagement/Pages/RiskManagementApproachAndMethodology-.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 informati
please go directly to the source. Revision Date: September 14, 2018

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link | Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Banking & Finance | Public Health & Healthcare | Transportation & Shipping | Energy (including nuclear) | Industry | Agriculture, Food Supply & Water | Information Distribution & Communications |
| Risk Management Handbook Volume III Contingency Planning Standard 4.4 | Std | CENTERS for MEDICARE & MEDICAID SERVICES (CMS) Enterprise Information Security Group | U.S.A. | The CMS Contingency Planning Standard is consistent with the guidance of the National Institute of Standards and Technology (NIST) and most specifically with NIST Special Publication (SP) 800-34 revision 1, Contingency Planning Guide for Federal Information Systems2 dated May 2010. | Feb- 2014 | Enf | | https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_4-4_Contingency_Planning_Standard.pdf | | ✓ | | | | | |

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

## Categories (column B):

Standard (Std) Level of quality accepted as norm, typically published by a professional organization of governing body, and is often an auditable standard.
Regulation (Reg) An official rule, law, or order stating what may or may not be done or how something must be done. Issued by a government department or agency.
Good Practice (Leading Practice, Guide, or Guidelines) Recommendation indicating a technique or methodology that, through experience & research, has proven to reliably lead to a desired result. Typically published by a professional organization of 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

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

# 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 14, 2018**

| 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<br><br>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<br><br>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<br>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 14, 2018**

| Title | Category (Reg, Std, GP) | Governing Body | Country | Summary / Description | Last Revision Date | Enforcement (Enf, Amb, Wat, IAI) | Notes /Comments | Link |
|---|---|---|---|---|---|---|---|---|
| Bulletin R-67<br>**Rescinded 7/10/1989.** | Reg | Federal Home Loan Bank | U.S.A. | N/A | None | Enf | **Rescinded 7/10/1989.**<br><br>Comptroller of Currency BC-177 (1983, 1987) superceds Federal Home Loan Bank Bulletin R-67. | |

# DRJ's Rules & Regulations

The content provided was compiled by volunteers of the DRJ EAB R&R Committee, and is as accurate as possible. Please contact the DRJ with any updates or suggestions. The content is subject to change without notice. For the most timely information please go directly to the source. Revision Date: September 14, 2018

| 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 | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 |
| Australia, New Zealand | 5 | 5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 0 |
| Canada | 18 | 11 | 2 | 4 | 4 | 3 | 3 | 3 | 6 | 5 |
| Croatia | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Hong Kong | 3 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| India | - | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 |
| Indonesia | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| International | 17 | 10 | 8 | 8 | 8 | 15 | 8 | 8 | 7 | 3 |
| Japan | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| Malaysia | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| New Zealand | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| Pakistan | - | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Philippines | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Singapore | 3 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| South Africa | 7 | 6 | 4 | 4 | 4 | 5 | 4 | 4 | 3 | 1 |
| Thailand | - | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| U.K. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 |
| U.S.A. | 54 | 44 | 28 | 20 | 20 | 21 | 20 | 29 | 20 | 34 |
| **Total** | **121** | | | | | | | | | **56** |