DRJ 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: Sept. 9, 2023

Title	Category (Reg, Std, GP)	Governing Body	Country	Summary / Description	Last Revision Date	Associated Cost	Enforcement (Enf, Amb, Wat, IAI)	Notes /Comments	Link (if link doesn't work when clicking on the cell, please try copying the link to your web browser)	Infrastructure Category							
										Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
AFMA KRI Definitions & Guidelines	GP	Australian National Audit Office (ANAO)	Australia	Multiple published documents provided by the ANAO on the topic of business continuity, including: ANAO REPORT NO. 6 OF 2014–2015 Business Continuity Management ANAO REPORT NO. 9 OF 2003–2004 Business Continuity Management and Emergency Management in Centrelink ANAO REPORT NO. 36 OF 2009-2010 Emergency Management and Community Recovery Assistance in Centrelink ANAO REPORT NO. 46 OF 2008–2009 Business Continuity Management and Emergency Management in Centrelink ANAO REPORT NO. 53 OF 2002–2003 Business Continuity Management Follow-on Audit ANAO REPORT NO. 16 OF 2008–2009 The Australian Taxation Office's Administration of Business Continuity Management SPEECH Published: Wednesday, February 23, 2000 Business Continuity Management:	dates vary	No charge	Amb		https://www.anao.gov.au/work?query=BCM	✓	✓	✓	✓	✓	✓	✓	✓
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.	Jul 2017	No charge	IAI		https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-232-Business-Continuity-Management-%28July-2017%29.pdf	✓							
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.	Oct 2020	$85.09 US	Wat		http://infostore.saiglobal.com/store/details.aspx?ProductID=1409610	✓	✓	✓	✓	✓	✓	✓	✓
ANAO Better Practice Guide: Business Continuity Management - Building resilience in public sector entities. June 2009	Std	ANAO (Australian National Audit Office)	Australia, New Zealand	Business continuity management is an essential component of good public sector governance. It is part of an entity's overall approach to effective risk management, and should be closely aligned to the entity's incident management, emergency response management and IT disaster recovery. Successful business continuity management requires a commitment from the executive to raising awareness and implementing sound approaches to build resilience. This Guide has been produced following consultation with Australian Government and private sector entities. The Guide provides a refreshed version of a previous ANAO Guide. The new version is presented in a more user-friendly format, and includes contemporary practical advice, case studies and references as well as exploring issues within the business continuity environment that have arisen since the previous ANAO publication. The Guide will be a useful reference document for boards, chief executives and senior management in public sector entities	Aug 2018	No charge	Enf		Better practice guides | Australian National Audit Office (anao.gov.au)		✓	✓	✓	✓			✓
AS/NZS Good Management Practice - Business Continuity Management	Std	Standards Association of Australia	Australia, New Zealand	Business continuity management is a process that helps an organisation better understand and prioritise threats in the event of a crisis, reduce the likelihood of those threats, and ensure good recovery. Business continuity management is part of a business's overall approach to effective risk management. The set provides guidance on societal security, business continuity management, information technology security techniques as well as planning for emergencies and disruption.	Mar 2013	No charge	Enf		Australian Business Continuity Management Standard AS/NZS 5050:2010 – A Risk Perspective – Complispace (wordpress.com)	✓							
AS/NZS ISO 31000:2018 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. NOTE: An update to ISO 31000:2009 was added in early 2018. The update is different in that "ISO 31000:2018 provides more strategic guidance than ISO 31000:2009 and places more emphasis on both the involvement of senior management and the integration of risk management into the organization."	2018	Copyright - Can only be printed by employees or NIWA members	Enf	Audit Report: The objective of the audit was to assess the adequacy of selected Australian Government entities' practices and procedures to manage business continuity. To conclude against this objective, the ANAO adopted high-level criteria relating to the entities' establishment, implementation and review of business continuity arrangements.	https://www.iso.org/standard/65694.html	✓	✓	✓	✓	✓	✓	✓	✓
AS/NZS ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements	Std	Standards Association of Australia	Australia, New Zealand	ISO/IEC 27001:2022 is a robust information security management system (ISMS) standard applicable to any business in any sector. It addresses the people, processes, and technologies that process protected information/data. Its companion document, ISO 27002:2022, provides guidance on how to implement security controls. Any business in any industry can apply the ISO 27001 requirements to better protect critical data. ISO 27001 applies a comprehensive set of security controls (which has been updated since the 2013 version), Annex A, that includes information security best practices, control areas, and control objectives. It mitigates threats to information confidentiality, integrity, and availability (CIA) to ensure business security and continuity.	Oct 2022	No charge	Enf		https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en	✓	✓	✓	✓	✓	✓	✓	✓

20 Questions Directors Should Ask about Crisis Management	GP	Intitute for Crisis Management	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.	2008	No charge	Enf		20 Questions Directors Should Ask About Crisis Management 2008 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.	Nov 2022		Wat	The comprehensive set includes: - AS ISO 22301:2017 Societal security - Business continuity management systems – Requirements - AS ISO 22313:2017 Societal security - Business continuity management systems – Guidance - AS/NZS 5050:2010 Business continuity - Managing disruption-related risk - AS 3745-2010 Planning for emergencies in facilities	https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_96111_01	✓	✓	✓	✓	✓	✓	✓	✓
Bill 198 (Canadian SOX)	Reg	Ontario Government	Canada	Bill 198 deals with virtually all of the same issues as Sarbanes-Oxley, including auditor independence, audit committee responsibilities, CEO and CFO accountability for financial reporting and internal controls, faster public disclosure, and stiffer penalties for illegal activities. The most significant difference between the US SOX and C-SOX: - Canadian companies do not have to submit an external auditor attestation of the adequacy of internal controls. - Canadian companies are supposed to deliver a " reasonable assurance " of preventing risk of material misstatement. And to give that assurance, the companies are supposed to show high level of commitment, care and meticulousness for reviewing and documenting their internal controls.	Jul 2023		Wat	Emergency Program Act	https://rsmcanada.com/what-we-do/services/consulting/risk-advisory/internal-audit-and-controls-services/bill-198-sarbanes-oxley-compliance.html	✓	✓	✓	✓	✓	✓	✓	✓
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	Jan 2020		Wat		https://www.canada.ca/en/services/policing/emergencies/continuity.html	✓							
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. Checklist of recommended sections of a business continuity plan.	2013		Wat		https://www.bdc.ca/en/Documents/businesscontinuityplanning/checklist.pdf	✓							
Canadian Aviation Security Regulations, 2012 (SOR/2011-318) Section 452.27 1,2,4; Section 325 1,2,4; Section 169 1,2,4; Section 63 1,2,4	Reg	Transport Canada	Canada	The operator of an aerodrome must develop and maintain a business continuity plan that, at a minimum, sets out how the operator will re-establish normal operations and comply with section 324 in the event that the operator is unable to use its restricted area access control process to comply with that section.	Oct 2022		Wat	Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard(ASIS SPC.1-2009); document may be purchased	Canadian Aviation Security Regulations, 2012 (justice.gc.ca)	✓	✓	✓	✓	✓	✓	✓	✓
Derivatives Regulation, RRQ, c I-14.01	Reg	Regulations of Quebec	Canada	DIVISION II.3 11.23. Persons who apply for qualification under section 82 of the Act must demonstrate that they meet the obligations under sections 82.1 to 82.3 of the Act as well as the following obligations: ... (3) they have developed an emergency and contingency plan to ensure business continuity.	Jun 2022		Enf	The Provincial Emergency Program (PEP) is a division of the Ministry of Justice and Attorney General, Emergency Management British Columbia, Canada.	I-14.01, r. 1 - Derivatives Regulation (gouv.qc.ca)								✓
Earthquake Planning for Business	GP	Emergency Preparedness for Industry and Commerce Council EPICC	Canada	This guide is meant to provide practical and reliable earthquake preparedness, response and recovery information for businesses in British Columbia. The guidelines are intended to equip any business owners, managers, supervisors and employees with the tools to develop earthquake preparedness and response plans and procedures by: - Offering guidance and a standard approach to earthquake planning - Providing a framework with which to prepare your organization for its specific earthquake vulnerabilities - Providing a template for developing your organization's emergency plans	Nov 2013		Wat		Earthquake Planning Guide for Business (iclr.org)	✓							
Emergency Management Act	Reg	Senate and House of Commons of Canada	Canada	Requires the Minister of Public Safety in Gov.Canada to: establishing policies and programs for the preparation of emergency management plans; control emergency management plans prepared by federal entities; coordinating the federal response to an emergency; coordinating federal and provincial emergency management activities coordinating the provision of non-finaincial assistance to a province and any declarations; participating in international emergency managment activities; establishing arrangements for continuity of government; promoting a common approach to emergency management, including the adoption of standards and best practices; and conducting exercises and providing emergency management education and training.	August 2021		Amb	The Emergency Management Act is a law established by the Canadian government that outlines the Minister of Public Safety and Emergency Preparedness as it relates to Canada, the United States and in general.	Emergency Management Act (justice.gc.ca)	✓							
Emergency Management and Civil Protection Act (EMPCA)	Reg	Government of Ontario	Canada	Under Provincial legislation, the Emergency Management and Civil Protection Act (EMPCA) , every municipality in Ontario is required to have an Emergency Management Program.	June 2011		Wat		http://www.bis.org/publ/bcbs189.pdf	✓							
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.	2010-2011		Wat		Emergency Management Planning Guide (publicsafety.gc.ca)	✓	✓	✓	✓	✓	✓	✓	✓
Third-Party Risk Management Guideline	GP	Office of the Superintendent of Financial Institutions (OFSI)	Canada	Federally regulated financial institutions (FRFIs) engage in business and strategic arrangements with external parties—entities or individuals—to perform business activities, functions, and services or obtain goods in support of their own operations or their business strategy.	April 2023	N/A	Amb	This Guideline sets out OSFI's expectations for managing risks associated with third-party arrangements. This Guideline applies to all FRFIs, excluding foreign bank branches and foreign insurance company branches. OSFI's expectations for foreign bank branches and	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx								

Technology and Cyber Risk Management	GP	Office of the Superintendent of Financial Institutions (OFSI)	Canada	This Guideline establishes OSFI's expectations related to technology and cyber risk management and applies to all federally regulated financial institutions (FRFIs). These expectations aim to support FRFIs in developing greater resilience to technology and cyber risks.	July 2022	N/A	Amb	There is no one-size-fits-all approach for managing climate-related risks given the unique risks and vulnerabilities that will vary with a FRFI's size, nature, scope, and complexity of its operations, and risk profile. The Guideline should be read, and implemented, from a risk-based perspective that allows the FRFI to compete	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx								
Climate Risk Management	GP	Office of the Superintendent of Financial Institutions (OFSI)	Canada	The Guideline establishes OSFI's expectations related to the FRFI's management of climate-related risks. It aims to support FRFIs in developing greater resilience to, and management of, these risks. The Guideline applies to all FRFIs except foreign bank branche	March 2023	N/A	Amb	There is no one-size-fits-all approach for managing climate-related risks given the unique risks and vulnerabilities that will vary with a FRFI's size, nature, scope, and complexity of its operations, and risk profile. The Guideline should be read, and implemented, from a risk-based perspective that allows the FRFI to compete	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b15-dft.aspx								
Operationa Risk Management	GP	Office of the Superintendent of Financial Institutions (OFSI)	Canada	This Guideline sets out OSFI's expectations for the management of operational risk and is applicable to all federally regulated financial institutions (FRFIs).	June 2016	N/A	Amb	OSFI recognizes that FRFIs may have different operational risk management practices depending on their: size; ownership structure; nature, scope and complexity of operations; corporate strategy and risk profile.	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21.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.	February 2023		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. Amended in 2023	Emergency Preparedness and Response Requirements for the Petroleum Industry (aer.ca)	✓							
IIROC Rule 17.16 - Business Continuity Plan Requirement	Reg	Investment Industry Regulatory Organization of Canada	Canada	Every Dealer Member shall establish and maintain a business continuity plan identifying the necessary procedures to be undertaken during an emergency or significant business disruption. Such procedures shall be reasonably designed to enable the Dealer Member to stay in business in the event of a future significant business disruption in order to meet obligations to its customers and capital markets counterparts and shall be derived from the Dealer Member's assessment of its critical business functions and required levels of operation during and following a disruption. Every Dealer Member must also conduct an annual review and test of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.	Sep 2021	NA		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.	Rule 17 - Dealer Member Minimum Capital, Conduct of Business and Insurance (iiroc.ca) file:///C:/Users/chuber2/Downloads/RulesCollated_090121_en.pdf https://www.iiroc.ca/members/dealer-member-compliance/business-continuity	✓	✓	✓	✓	✓	✓	✓	✓
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	June 2018	NA	Wat		https://www.cer-rec.gc.ca/en/about/acts-regulations/cer-act-regulations-guidance-notes-related-documents/processing-plant/2002-04-24mrgncprprdnssrspns-eng.pdf https://docs2.cer-rec.gc.ca/ll-eng/llisapi.dll/fetch/2000/90463/3119405/3186080/A81701%2D3_NEB_Amended_Order_AO%2D001%2DMO%2D002%2D2017_Compelling_Publication_of_Emergency_Management_Program_Informati	✓							
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.	October 2006	NA	Enf	Responsibilities on Business Continuity: Back-up Operations Centers and Data Recovery Sites	https://mfda.ca/notice/msn-0056/	✓							
National Instrument 21-101 Marketplace Operation; and National Instrument 31-103 Registration Requirements and Exemptions	Reg	Ontario Securities Commission (OSC)	Canada	Part 12 of NI 21-101 addresses marketplace systems and business continuity planning. It requires that each system operated by or on behalf of the marketplace that supports order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing must develop and maintain business continuity plans in accordance with business practices at least once a year. It also states that the regulator must be promptly notified of any material systems failure, malfunction, delay or security breach along with timely updates on status. Subsection 12.1(a,b,c) of National Instrument 21-101 Marketplace Operation requires marketplaces to develop and maintain an adequate system of internal controls and information technology controls over the systems and auxillary systems. It also requires prompt notification to the regulator its regulation service provider of any material systems failures. Subsection 12.2 requires that the marketplace to annual engage a specified party to conduct independent systems review and prepare a report in accordance with audit standards. The report must be provided to its board of directors and the regulator. Subsection 12.3 requires the marketplace to make publically available all technology requirements regarding interfacing and accessing the marketplace in its final form. Subsection 12.4 requires the marketplace to provide uniform test symbols. Subsection 12.5 requires the marketplace to develop, maintain, and test reasonable business continuity plans to include disaster recovery plans. In addition,subsection 11.1(b) of National Instrument 31-103 Registration Requirements and Exemptions requires a registered firm to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to manage the risks associated with its business in accordance with prudent business practices.	Sep 2020	NA	Wat		https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-101/national-instrument-21-101-marketplace-operation https://www.osc.ca/en/securities-law/instruments-rules-policies/3/31-103	✓							
OSFI Guideline B-10 - Third Party Risk Guidelines	Reg	Office of the Superintendent of Financial Institutions Canada (OSFI)	Canada	FRFI third-party arrangements have a variety of forms, which include but are not limited to, critical services for the FRFI, minor support arrangements, and strategic arrangements where no service is actually being provided. OSFI expects FRFIs to consider risk and criticality when examining third-party arrangements to determine the intensity with which to apply the expectations set out in this Guideline. For example, an exit or contingency plan may not be needed for a low-risk arrangement, nor will subcontracting risk be a significant factor in managing every third-party arrangement. Similarly, a legal review may not be necessary for a low-risk, short-term arrangement. Fundamental to applying this Guideline in a prudent manner is identifying the type and	April 2023	$45	Enf	Updated in 2023 and replaced Business Continuity guidelines for 3rd parties.	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx#toca1	✓	✓	✓	✓	✓	✓	✓	✓

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	NA	Wat		Earthquake Exposure Sound Practices (osfi-bsif.gc.ca)	✓	✓	✓	✓	✓	✓	✓	✓
Croation Sabor: Credit Institutions Act	Reg	Croatian National Bank (CNB)	Croatia	Credit Institutions Act	May 1, 2023	N/A	Enf	Act on Amendments to the Credit Institutions Act (EN/HR) available for download	https://www.hnb.hr/en/-/zakon-o-kreditnim-institucijama	✓							✓
87/600/Euratom: Council Decision of 14 December 1987 on Community arrangements for the early exchange of information in the event of a radiological emergency	Reg	The Council of the European Union	European Union	These arrangements shall apply to the notification and provision of information whenever a Member State decides to take measures of a wide-spread nature in order to protect the general public in case of a radiological emergency following: (a) an accident in its territory involving facilities or activities from which a significant release of radioactive material occurs or is likely to occur; or (b) the detection, within or outside its own territory, of abnormal levels of radioactivity which are likely to be detrimental to public health in that Member State; or (c) accidents other than those specified in (a) involving facilities or activities from which a significant release of radioactive material occurs or is likely to occur; or (d) other accidents from which a significant release of radioactive materials occurs or is likely to occur. Member States shall take the measures necessary to comply with this Decision within three months of the date of its notification.	2006	N/A	Enf		https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:31987D0600 https://op.europa.eu/en/publication-detail/-/publication/7921d3b2-a6c0-4915-a828-96e162123ede/language-en/format-HTML/source-search		✓	✓	✓	✓			✓
Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations	Reg	The Council of the European Union	European Union	This Directive shall apply to any civilian nuclear installation subject to a licence. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 22 July 2011.	2014	N/A	Enf	http://data.europa.eu/eli/dir/2014/87/oj	https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1412848109512&uri=CELEX:32009L0071		✓	✓	✓	✓			✓
Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom	Reg	The Council of the European Union	European Union	This Directive applies to any planned, existing or emergency exposure situation which involves a risk from exposure to ionising radiation which cannot be disregarded from a radiation protection point of view or with regard to the environment in view of long-term human health protection. EU Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 6 February 2018.	2014	N/A	Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1550067952603&uri=CELEX:32013L0059		✓	✓	✓	✓	✓		✓
Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC Text with EEA relevance	Reg	The European Parliament and the Council of the European Union	European Union	This Decision establishes rules on epidemiological surveillance, monitoring, early warning of, and combating, serious cross-border threats to health, including preparedness and response planning related to those activities, in order to coordinate and complement national policies. It also aims to support cooperation and coordination between the Member States in order to improve the prevention and control of the spread of severe human diseases across the borders of the Member States, and to combat other serious cross-border threats to health in order to contribute to a high level of public health protection in the Union. Finally, the Decision clarifies the methods of cooperation and coordination between the various actors at Union level.	2013	N/A	Enf		https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013D1082	✓	✓	✓	✓	✓	✓	✓	✓
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism	Reg	The European Parliament and the Council of the European Union	European Union	1. The Union Civil Protection Mechanism ("the Union Mechanism") shall aim to strengthen the cooperation between the Union and the Member States and to facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters. 2. The protection to be ensured by the Union Mechanism shall cover primarily people, but also the environment and property, including cultural heritage, against all kinds of natural and man-made disasters, including the consequences of acts of terrorism, technological, radiological or environmental disasters, marine pollution, and acute health emergencies, occurring inside or outside the Union. In the case of the consequences of acts of terrorism or radiological disasters, the Union Mechanism may cover only preparedness and response actions.	2021	N/A	Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013D1313	✓	✓	✓	✓	✓	✓	✓	✓
Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks	Reg	The European Parliament and the Council of the European Union	European Union	Directive 2007/60/EC on the assessment and management of flood risks entered into force on 26 November 2007. This Directive now requires Member States to assess if all water courses and coast lines are at risk from flooding, to map the flood extent, assets and humans at risk in these areas, and to take adequate and coordinated measures to reduce this flood risk. This Directive also reinforces the rights of the public to access this information and to have a say in the planning process.	2007	N/A	Enf		https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32007L0060	✓	✓	✓	✓	✓	✓	✓	✓

Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance	Reg	The European Parliament and the Council of the European Union	European Union	This Directive lays down rules for the prevention of major accidents which involve dangerous substances, and the limitation of their consequences for human health and the environment, with a view to ensuring a high level of protection throughout the Union in a consistent and effective manner. EU Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 May 2015. They shall apply those measures from 1 June 2015.	2012	N/A	Enf		https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32012L0018		✓	✓	✓	✓	✓	✓	✓
Recommendations for National Risk Assessment for Disaster Risk Management in EU, Version 1	GP	The Joint Research Centre is the European Commission's science and knowledge service	European Union	The purpose of Version 1 of the Recommendations for NRA for Disaster Risk Management, prepared by 50 scientists, is to encourage the use of the new "Reporting Guidelines on Disaster Risk Management, Art. 6(1) of Decision No.1313/2013/EU2019/C 428/07" by relevant authorities of the Participating States to the EUCPM. The final scope of this collective effort is to support establishment of an appropriate risk governance that is flexible, adaptable to new evidences, knowledge and situations. It is designed to encourage risk assessment processes as proper evidence to drive disaster risk management planning and the implementation of adequate measures all along the risk management cycle, from adaptation and mitigation to response and recovery phases.	2021	N/A	Enf		https://drmkc.jrc.ec.europa.eu/knowledge/science-for-drm/recommendations-for-national-risk-assessment-for-disaster-risk-management-in-eu	✓	✓	✓	✓	✓	✓	✓	✓
Science for Disaster Risk Management 2017: Knowing better and losing less	GP	The Joint Research Centre is the European Commission's science and knowledge service	European Union	This report will present the state of science in DRM. The narrower purpose is to show practical use of scientific knowledge in DRM actions in Europe. The report shall provide reviews of the scientific evidence base and its practical use in various areas of disaster risk management, in a format that is intended to be accessible to the well-informed practitioner. The reviews of the scientific evidence base are summaries of (1) recent advances/outcomes of EU research projects, (2) relevant national work and (3) relevant international work.The final scope of the report is naturally divided into three distinct parts: understanding risk, communicating risk and managing risk. The report is one of the most visible objectives of DRMKC aiming to bridge science and policy as well operatoin communities. It is the first in a series and therefore comprehensive in scope but selective in topic. It will fill the gap in preparation for Sendai framework for DRR and show posibilites to strengthen society's resilience by using science and technology.	2017	N/A	Enf		https://ec.europa.eu/jrc/en/publication/science-disaster-risk-management-2017-knowing-better-and-losing-less	✓	✓	✓	✓	✓	✓	✓	✓
Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)	Reg	The European Parliament and the Council of the European Union	European Union	Known as Solvency II, this directive requires insurance companies to hold enough financial resources. It also sets out management and supervisory rules. The directive covers non-life insurance, life insurance and reinsurance companies. An insurance company can conduct its activities after having obtained an authorisation from the supervisor of its country. The authorisation is valid throughout the EU.	2021		Enf		https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0138	✓							
Circular re "Business Continuity Planning"	Std	Securities and Futures Commission of Hong Kong	Hong Kong	The HKMA conducted a self-assessment exercise involving 25 AIs in Hong Kong to gain an understanding of the effectiveness of their business continuity plans (BCPs) impacted by large events (i.e., 9/11, fire, etc.) affecting core sites	Aug 2011		Enf		Hong Kong Monetary Authority - Business Continuity Planning (hkma.gov.hk)	✓							
Circular to Licensed Corporations concerning Effective Business Continuity Plans	Std	Securities and Futures Commission of Hong Kong	Hong Kong	"An effective business continuity plan is essential to the operations of all licensed corporations. You are expected to establish and maintain appropriate internal controls and risk management measures to protect your key business functions and recover them in a timely fashion in the event of operational disruptions."	Jun 2014		Wat		https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/ https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC32 https://www.sfc.hk/en/faqs/business-continuity-contingency-information	✓						✓	
Bank Indonesia Regulation Number 9/15/PBI/2007 Concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks	Reg	Bank Indonesia (Central Bank)	Indonesia	Requires BCP documentation and testing at least annually. Requires Internal Audit to conduct an audit at least annually and provide report to Bank Indonesia.	Dec 2016		Enf		Bank Indonesia Regulation Concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks (ojk.go.id) https://www.ojk.go.id/en/regulasi/Documents/Pages/Bank-Indonesia-Regulation-Number-9.15.PBI.2007/pbi091507_eng_1392373937.pdf	✓							
Basel Committee on Banking Supervision - The Joint Forum - High-level principles for business continuity (August 2006)	Reg	Basel Committee on Banking Supervision	International	The high-level principles set out in this paper are intended to support international standard setting organisations and national financial authorities in their efforts to improve the resilience of financial systems to major operational disruptions.	Aug. 2006		Enf		https://www.bis.org/publ/joint17.htm https://www.bis.org/publ/joint14.pdf	✓							✓	

Basel III: A global regulatory framework for more resilient banks and banking systems	Reg	Basel Committee on Banking Supervision	International	This document, together with the document Basel III: International framework for liquidity risk measurement, standards and monitoring, presents the Basel Committee's reforms to strengthen global capital and liquidity rules with the goal of promoting a more resilient banking sector. The objective of the reforms is to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source, thus reducing the risk of spillover from the financial sector to the real economy. This document sets out the rules text and timelines to implement the Basel III framework.	Jun 2011		Enf		https://www.bis.org/publ/bcbs189.htm https://www.bis.org/publ/bcbs189.pdf	✓							
BS 65000 - Guidance on organizational resilience	Std	Business Standards Institute (BSI) (UK based)	International	BS 65000 is a revised British Standard that helps organizations understand what resilience means and provides the necessary guidance to help them build a more resilient future. As the latest version, BS 65000:2022 is no longer just a guidance document, but a code of practice. It supplies updated terminology and approaches, and covers a wider scope of resilience across industries, sectors and organizational types and sizes. Who is BS 65000 – Organizational resilience for? • Compliance officers • Resilience managers • Business continuity managers • Cyber managers • Human resources managers • Resilience officers and those responsible for resilience in their organization • CFOs, CEOs and board chairs • Risk managers, analysts and officers • Risk operations managers • Security officers • Facility managers • Those responsible for governance of the organization	Aug 2022		Enf		https://www.bsigroup.com/en-GB/standards/bs-650002022/ https://knowledge.bsigroup.com/products/organizational-resilience-code-of-practice/standard?_ga=2.8515185.538937092.1668097744-742569559.1668097744		✓	✓	✓	✓	✓	✓	✓
Business Continuity Management Audit Program	GP	ISACA	International	In addition to scenario planning, the audit program provides controls and testing in the areas of: • Governance/Monitoring • Business Impact Analysis • Workforce • Location • Applications and Systems • Emergency Preparedness/Communications • Scenario Planning/DR Testing • Continuous Improvement & Reports	Aug 2021	free to members, membership est. < $200 USD	Enf		https://www.isaca.org/ https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoEfEAK	✓	✓	✓	✓	✓	✓	✓	
The BCI Good Practice Guidelines	Std	BCI (Business Continuity Institute)	International	The Good Practice Guidelines (GPG) 2018 Edition is the definitive guide for business continuity and resilience professionals. The GPG is used as an information source for individuals and organizations seeking an understanding of business continuity as part of their awareness raising campaigns and training schedules. The GPG takes a collaborative approach to business continuity, ensuring organizations and individuals understand how to work with related management disciplines to successfully implement their business continuity solutions. The Good Practice Guidelines draw on the knowledge of practitioners from all over the world as well as information within International Standards. As a result, the GPG is globally recognised as the go-to publication for good practice.	Nov 2017		Enf		https://www.thebci.org https://www.thebci.org/training-qualifications/good-practice-guidelines.html					✓			✓
DRI International "Ten Professional Practices for Business Continuity Professionals"	GP	DRII (Disaster Recovery Institute International)	International	As part of DRI International's ongoing efforts to maintain the relevance and utility of the Professional Practices, an extensive revision of substance, form, and function was undertaken starting in mid-2015 and finishing in the beginning of 2017. The goals were to provide information that would include: • Advances in technology • Cyber threat considerations • Utilizing insurance as a risk transfer tool • Strategies for manufacturing • Supply chain processing • Risk management concepts • Legal and regulatory concerns	2017		Enf		https://drii.org/ https://drii.org/resources/professionalpractices/EN	✓	✓	✓	✓	✓	✓	✓	✓
ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements	Std	ISO	International	This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.	Oct 2019			This standard has been revised by ISO 22301:2019	ISO - ISO 22301:2012 - Societal security — Business continuity management systems — Requirements	✓	✓	✓	✓	✓	✓	✓	✓
ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management	GP	ISO	International	This document gives guidelines for incident management, including — principles that communicate the value and explain the purpose of incident management, — basic components of incident management including process and structure, which focus on roles and responsibilities, tasks and management of resources, and — working together through joint direction and cooperation. This document is applicable to any organization involved in responding to incidents of any type and scale. This document is applicable to any organization with one organizational structure as well as for two or more organizations that choose to work together while continuing to use their own organizational structure or to use a combined organizational structure.	Jan 2018				ISO - ISO 22320:2018 - Security and resilience — Emergency management — Guidelines for incident management								✓

ISO 9000 FAMILY - QUALITY MANAGEMENT	Std	ISO	International	ISO 9000: family of quality management systems, fundamentals and vocabulary. Covers the basics of what quality management systems are and also contains the core language of the ISO 9000 series of standards. Purpose is to determine elements of quality control systems, especially maintenance of records and verification standards. While business continuity planning is not required by statute, vendors report that records retention and data availability are issues with their customers, and that they are specifically asked about their plans.	2/12/2019		Amb		ISO - ISO 9000 family — Quality management	✓		✓		✓	✓	✓	
ISO 9001:2015 Quality management systems — Requirements	Std	ISO (International Organization for Standardization) - the correct link for ISO is: https://www.iso.org/home.html	International	ISO 9001:2015 specifies requirements for a quality management system when an organization: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.	Jan 2021		Wat		ISO - ISO 9001:2015 - Quality management systems — Requirements					✓			
ISO 9004:2018 Quality management — Quality of an organization — Guidance to achieve sustained success	Std	ISO (International Organization for Standardization)	International	ISO 9004:2018 gives guidelines for enhancing an organization's ability to achieve sustained success. This guidance is consistent with the quality management principles given in ISO 9000:2015. ISO 9004:2018 provides a self-assessment tool to review the extent to which the organization has adopted the concepts in this document. ISO 9004:2018 is applicable to any organization, regardless of its size, type and activity.	Jan 2020		Wat		ISO - ISO 9004:2018 - Quality management — Quality of an organization — Guidance to achieve sustained success	✓	✓	✓	✓	✓	✓	✓	✓
ISO Guide 73:2009 - Risk management -- Vocabulary	GP	ISO (International Organization for Standardization)	International	ISO/Guide 73:2009 (en) - Risk management — Vocabulary This Guide provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk. This Guide is intended to be used by: — those engaged in managing risks, — those who are involved in activities of ISO and IEC, and — developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk. For principles and guidelines on risk management, reference is made to ISO 31000:2009.	2009		IAI		https://www.iso.org/standard/44651.html	✓							
ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	Std	ISO (International Organization for Standardization)	International	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: 1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; 2. implement commonly accepted information security controls; 3. develop their own information security management guidelines.	Feb 2022		Enf	This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organisations: (a) within the context of an information security management system (ISMS) based on ISO/IEC27001; (b) for implementing information security controls based on internationally recognized best practices; [and] (c) for developing organisation-specific information security management guidelines. Source: ISO/IEC 27002:2022	https://www.iso27001security.com/html/27002.html							✓
ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management Emergency Management and Civil Protection Act, R.S.O. 1990, c. E.9	Std	ISO (International Organization for Standardization) Emergency Management and Civil Protection Act	International	ISO/IEC 27005:2018 provides guidelines for information security risk management. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.	Jul 2019		Enf		https://www.iso.org/standard/75281.html								✓
Business Continuity Planning (Bank of Japan)	Std	BOJ (Bank of Japan)	Japan	The Bank develops and continually revises business continuity plans for functions such as circulation of banknotes and operation of payment and settlement systems, in order to carry out its responsibilities in times of disaster. The Bank trains its staff and conducts emergency drills on a regular basis to ensure a timely and appropriate response. The Bank also coordinates with relevant parties for effective business continuity planning at payment and settlement systems, at the market level, and in the financial system as a whole. For example, the Bank tests contingency procedures with market participants and with related administrative institutions, based on various scenarios including large-scale earthquakes.	2016		Enf		https://www.boj.or.jp/en/about/bcp/index.htm	✓							

Procedure of Implementation of Prevention of Emergencies	Reg	Government of the Republic of Lithuani - Minister of the Interior Republic of LithuaniaGovernment of the	Lithuania	This document outlines the procedures for prevention, planning, and implementation of emergency procedures. Additional information on policies can be found at: CoR - Lithuania Civil protection (europa.eu)	2017	N/A	Enf	The PDF is no longer valid. The following link provides information on the on the Law on the State of Emergency for Lithuania - https://IX-938 Republic of Lithuania Law on a State of Emergency (lrs.lt)	https://e-seimas.lrs.lt/rs/legalact/TAD/702d015216b811e6aa14e8b63147ee94/format/ISO_PDF/	✓	✓	✓	✓	✓	✓	✓	✓
Malaysia Business Continuity Management Requirements	Tech Code	MCMC - Malaysian Communications and Multimedia Commission	Malaysia	This Malaysian standard was developed to fill a need that existed at that time. The practice of business continuity management was being popularise in the country but there was no clear or generally accepted guidelines for the malaysian consumer to follow. And the guidelines there were required in some industrial sector were either too control driven or vague. Knowing that there were standards being developed in other countries and at the international level, the committee responsible for developing MS 1970 decided to a document which will guide the reader in developing and implementing a business continuity management framework. This document provides the reader with clear method and recommended steps. It also provides the reader with the minimum expected outcomes for each process. This standard was intended for use by organizations of all types and sizes may it be private, government or commercial.	15 October 2018 Bhd (MTSFB) via its Trust and Privacy Sub Working Group. It defines the general requirements to establish, maintain and implement effective business continuity plan as an extension to the document 'MCMC MTSFB		Enf		extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G014_2018_BUSINESS-CONTINUITY-MANAGEMENT-(BCM)-REQUIREMENTS.pdf	✓	✓	✓	✓	✓	✓	✓	
Manual of Regulations for Banks (MORB) Section E. Risk Management	Reg	The Bangko Sentral ng Pilipinas (BSP) (central bank of the Republic of the Philippines)	Philippines	Cojtains the followig: Section141Supervision by Risk Section142Risk Governance Framework Section143Credit Risk Management Section144Market Risk Management Section145Liquidity Risk Management Section145-ALiquidity Coverage Ratio (LCR) Section146Operational Risk Management Section147Bank Protection Section148Information Technology Risk Management Section149Business Continuity Management Section150Social Media Risk Management Section151Guidelines on the Conduct of Stress Testing Exercises	2018		Enf		E. Risk Management – Manual of Regulations for Banks (bsp.gov.ph)	✓							
MAS Business Continuity Management Guidelines (June 2003)	Reg	MAS (Monetary Authority of Singapore)	Singapore	The Monetary Authority of Singapore published its Business Continuity Management guidelines in 2003. These guidelines consist of sound BCM principles that businesses should adopt in order to ensure business recovery and preparedness in case of any disruption to their operations. Business Continuity Management According to the guidelines, Business Continuity Management or BCM is an overarching framework that that aims to minimize the impact to businesses due to operational disruptions. It not only addresses the restoration of IT infrastructure, but also focuses on the rapid recovery and resumption of critical business functions for the fulfillment of business obligations. A BCM framework should include:	June 2022		IAI		Monetary Authority of Singapore – Business Continuity Management Guidelines: Overview and Summary of Requirements - ComplianceOnline.com	✓							
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.	Oct 2018	NA	IAI		Outsourcing Guidelines_Jul 2016 revised on 5 Oct 2018.pdf (mas.gov.sg)	✓							
SS540 – Singapore Business Continuity Standard	Std	Economic Development Board (EDB) with the collaboration of Singapore Business Federation (SBF)	Singapore	The SS540:2008 structure is based on a matrix BCM framework. It allows potential gaps in an organization's BCM efforts to be identified and located. For example, the implications of selecting a particular recovery strategy should be linked to the corresponding policies set forth by Executive Management. Implementation of the recovery strategy should be supported by corresponding infrastructure, training of recovery personnel and establishing the associated recovery processes.	Oct 2008	NA	Enf		SS540 – Singapore Business Continuity Standard (dcag.com)	✓							

SS ISO 22301:2020 Security and resilience – Business continuity management systems – Requirements	Std	Singapore Standards Council	Singapore	Specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. Requirements are generic and intended to be applicable to all organisations, or parts thereof, regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity. Is applicable to all types and sizes of organisations that: a) implement, maintain and improve a BCMS; b) seek to ensure conformity with stated business continuity policy; c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; d) seek to enhance their resilience through the effective application of the BCMS.	Apr 2020	NA	Enf		https://www.singaporestandardseshop.sg	✓	✓	✓	✓	✓	✓	✓	✓
Monetary Authority of Singapore -BCM Guidelines	Std	Monetary Authority of Singapore	Singapore	This set of MAS BCM Guidelines (hereafter referred as "the Guidelines") contains sound BCM principles that FIs are encouraged to adopt. Financial Instituitions (FIs) are ultimately responsible for their business continuity preparedness and recovery from operational disruptions. FIs should establish policies, plans and procedures to ensure that their critical business services and functions can be promptly resumed following a disruption.	Jun 2022	NA			https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management	✓	✓	✓	✓	✓	✓	✓	✓
Act No. 16 of 2015: Disaster Management Amendment Act, 2015	Reg	Ministry for Provincial & Local Government Disaster Management Act, 2002	South Africa	To amend the Disaster Management Act, 2002, so as to substitute and insert certain definitions; to clarify policy focus on rehabilitation and functioning of disaster management centres; to align the functions of the National Disaster Management Advisory Forum to accommodate the South African National Platform for Disaster Risk Reduction; to provide for the South African National Defence Force, South African Police Service and any other organ of state to assist the disaster management structures; to provide for an extended reporting system by organs of state on information regarding occurrences leading to the declarations of disasters, expenditure on response and recovery, actions pertaining to risk reduction and particular problems experienced in dealing with disasters; to strengthen reporting on implementation of policy and legislation relating to disaster risk reduction and management of allocated funding to	12/15/2015	NA	Enf	Disaster Management Amendment Act 16 of 2015 (www.gov.za)	Disaster Management Amendment Act 16 of 2015 [www.gov.za]	✓	✓	✓	✓	✓	✓	✓	✓
Disaster Management Act 2002	Reg	Ministry for Provincial & Local Government Disaster Management Act, 2002	South Africa	To provide for- * 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 manage ment centres; * disaster management volunteers; and * matters incidental thereto.	Jan 2003	NA	Enf	Amended by Disaster Management Act 16 of 2015 (www.gov.za) as noted in row 67	Disaster Management Act [No. 57 of 2002] [www.gov.za]	✓	✓	✓	✓	✓	✓	✓	✓
National Payment System Department Oversight Framework	Reg	South African Reserve Bank	South Africa	Payment Systems provide channels through which funds are transferred among financial institutions to discharge the payment obligations arising in the financial markets and across the wider economy. As such, payment systems form a vital part of the economic and financial infrastructure and their efficient functioning contributes to overall economic performance. Payment systems by their very nature and the central role they play in the economy also involve significant exposures and risks for participants and provide a channel for shocks to be transmitted across the financial system. If payment and settlement systems, which facilitate the exchange of money for goods, services and financial assets, are seen as inefficient, unreliable or unsafe, this would erode public confidence in their use. For this reason, as public institutions responsible for preserving public trust in national currencies, and in line with a mandate for financial stability.	2022	NA	Enf		https://www.resbank.co.za/en/home/what-we-do/payments-and-settlements/regulation-oversight-and-supervision	✓	✓	✓	✓	✓	✓	✓	✓
The National Payment System Framework and Strategy Vision 2025		South African Reserve Bank	South Africa	This publication maps out an overarching industry vision for the future of South African payment systems. A framework for achieving this vision is outlined. This framework captures nine goals that industry stakeholders should pursue collaboratively. Six success factors that will facilitate an environment conducive to meeting these goals are identified. This is followed by a detailed exploration of each of the nine goals, including 26 tangible strategies that industry stakeholders should implement to meet each goal. Many of these strategies apply to multiple goals, just as some goals can help to contribute to meeting other goals. After examining the goals and strategies that should be used to accomplish the industry vision, next steps are proposed.	Mar-18	NA			Payments and Settlements (resbank.co.za) https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/Vision%202025.pdf	✓							
Building the UK Financial Sector's Operational Resilience: Impact Tolerances for Important Business Services CONSULTATION PAPER		Bank of England (BOE) Prudential Regulation Authority (PRA) Financial Conduct Authority (FCA)	U.K.	This Consultation Paper is an outgrowth of a July 2018 Discussion Paper, "Building the UK Financial Sector's Operational Resilience," which set out an approach to operational resilience. In December 2019, the supervisory authorities published a suite of documents ('the proposals'), which would embed that approach into policy. Proposed policies will comprise new rules (for the FCA and PRA), principles, expectations and guidance, and will be implemented through the authorities' respective supervisory areas. Not all firms would be subject to the formal policy proposals. Readers should refer to the consultation documents for the proposed scope of the policies. Due to different legislation and regulatory frameworks under which the PRA, the FCA and the Bank operate, the approach taken by each supervisory authority is not identical but their intended outcomes are aligned. Detailed proposals from each supervisory authority are set out in separate publications referenced in this paper	Mar-21	N/A	Wat	Update 3 June 2021: This update is relevant only to firms with annual gross written premiums in excess of £10 billion determined on the basis of the average annual amount assessed across a rolling period of three years, calculated by reference to the firm's accounting reference date. It has come to the PRA's attention that there was a typographical error in paragraph 3.15 of Policy Statement (PS) 6/21 'Operational resilience: Impact tolerances for important business services'. This has resulted in PS6/21 not reflecting accurately the wording of the Operational Resilience – Solvency II Part of the PRA Rulebook, effective from Wednesday 31 March 2022. The figure of £10 billion	https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf	✓							

Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies (for Operational Resilience) POLICY STATEMENT		Bank of England (BOE) Prudential Regulation Authority (PRA) Financial Conduct Authority (FCA)	U.K.	1.1 This Prudential Regulation Authority (PRA) Policy Statement (PS) provides feedback to responses to Consultation Paper (CP) 21/21 'Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies (for Operational Resilience)'.footnote [1] It also contains the PRA's final policy, in the form of: ** amendments to the Operational Resilience Part of the PRA Rulebook, the Insurance – Operational Resilience Part of the PRA Rulebook and the Group Supervision Part of the PRA Rulebook (Appendix 1); ** updated SS1/21 'Operational resilience: Impact tolerances for important business services' (Appendix 2); and ** amendments to the Operational Continuity Part of the PRA Rulebook (Appendix 3). 1.2. This PS is relevant to different types of firms as follows: Operational Resilience: ---------- UK banks, building societies, and PRA-designated investment firms (all of which will hereafter be known as 'banks'), and CRR consolidation entities; UK Solvency II firms, and the Society of Lloyd's and its managing agents (all of which will hereafter be known as 'insurers'); and Operational Continuity in Resolution: ---------- UK banks, building societies, and PRA-designated UK investment firms currently in scope of, or likely to come in scope of, the Operational Continuity Part of the PRA Rulebook.	Mar-22	N/A	Enf	PS2 / 22 | CPM21 / 21 Implementation 1.15. The implementation dates for the changes set out in this PS are: Thursday 31 March 2022 for the Operational Resilience Parts and the Group Supervision Part; and Sunday 1 January 2023 for the Operational Continuity Part.	https://www.bankofengland.co.uk/prudential-regulation/publication/2021/november/operational-resilience-operational-continuity-in-resolution-amendments	✓							
Civil Contingencies Act 2004 (c.36)	Reg	U.K. Parliament	U.K.	The Act is divided into three parts: Part 1 defines the obligations of certain civil organisations to prepare for various types of emergencies Part 2 provides additional powers for the government to use in the event of a large scale emergency Part 3 provides supplementary legislation in support of the first two parts	May 2018	N/A	Enf	Amends or repeals older Civil Defense Acts, Emergency Powers Acts, and other related Acts	http://www.legislation.gov.uk/ukpga/2004/36/contents	✓	✓	✓	✓	✓	✓	✓	✓
UK_Civil Contingencies Act_Post Implementation Review_29-Mar-2022	Reg	U.K. Parliament	U.K.	To what extent have the policy objectives been achieved? The Act continues to achieve its stated objectives. Duties are placed upon local responders, with the principle of subsidiarity ensuring they retain the flexibility to collaborate in a way that is suitable to their specific needs. The recommendations made (including changes to the guidance) aim to strengthen the fulfilment of the Act's objectives, but there is no case at this stage for a fundamental overhaul of the legislation. Whilst the objectives and the Act's fulfilment of them are broadly fit for purpose at present, the evolving risk landscape, as well as work on the Integrated Review commitments to consider strengthening LRFs and develop a National Resilience Strategy, may create a need for further changes to the Act in future.	Mar 2022	N/A			https://www.gov.uk/government/publications/civil-contingencies-act-2004-post-implementation-review-report-2022	✓	✓	✓	✓	✓	✓	✓	✓
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.	2017	$90.00	Enf	2009 version can be downloaded for free. Most current version (2017) is $90.00 (discount available for ANSI members)	https://store.asisonline.org/security-and-resilience-in-organizations-and-their-supply-chains-standard-softcover.html							✓	
California Consumer Privacy Act (CCPA)	Reg	California Constitution 1798.100 to 1798.198	U.S.A.	The California Consumer Privacy Act (CCPA) is a data privacy act intended to enhance the privacy rights and consumer protection for residents of California. Every Company that does business in California and collects personal information must abide by the law. The regulations went into effect on August 14, 2020. Additional amendments to the regulations went into effect on March 15, 2021. In November of 2020, California voters approved Proposition 24, the CPRA, which amended the CCPA and added new additional privacy protections that began on January 1, 2023. As of January 1, 2023, consumers have new rights in addition to those above, such as: The right to correct inaccurate personal information that a business has about them; and The right to limit the use and disclosure of sensitive personal information collected about them. Businesses that are subject to the CCPA have several responsibilities, including	May-23		Enf	Key differences between CCPA and the European Union's GDPR include the scope and territorial reach, definitions of protection information and opt-out right for sales of personal information.	California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General		✓					✓	✓
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. SB 1386 went into affect on July 1, 2003.	Mar 2022		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.csub.edu/its/security/california-sb-1386 https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html		✓						
CTIA Emergency Preparedness/Disaster Recovery	Std	CTIA - 2013	U.S.A.	The CTIA represents the U.S. wireless communication industry; advocates for legislative and regulatory policies, works with members to develop test plans and certification processes and building awareness. CTIA advocates on behalf of America's wireless industry for legislative and regulatory policies that foster greater innovation, investment and economic growth.	2023 and 2019		Enf	The 2nd link (Preparedness Table of Contents) is more appropriate and last revised in 2019	https://www.ctia.org/the-wireless-industry/industry-commitments/wireless-network-resiliency-cooperative-framework https://prepared.ctia.org/#table-of-contents	✓						✓	

CTPAT: Customs Trade Partnership Against Terrorism		Dept. of Homeland Security	U.S.A.	Customs Trade Partnership Against Terrorism (CTPAT) is but one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security. CTPAT is a voluntary public-private sector partnership program which recognizes that CBP can provide the highest level of cargo security only through close cooperation with the principle stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. The Security and Accountability for Every Port Act of 2006 provided a statutory framework for the CTPAT program and imposed strict program	October 2022			Business Continuity is a requirement within the Minimum Security Criteria (MSC).	https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT		✓	✓			✓		
e-CFR Part 27: Chemical Facility Anti-Terrorism Standards (as of 08/16/2017)	Reg	Dept. of Homeland Security	U.S.A.	· U.S. Govennment Publishing Office · Continuity of operations for Critical Infrastructure · Enhance security and resiliency of chemical facilities · Title 6 was last amended July 2023	Jul 2023		Enf		https://www.ecfr.gov/current/title-6/chapter-I/part-27 https://ecfr.federalregister.gov/	✓	✓	✓	✓	✓	✓	✓	✓
e-CFR Part 29: Protected Critical Infrastructure Information (as of 08/16/2015)	Reg	Dept. of Homeland Security	U.S.A.	· U.S. Govennment Publishing Office · Continuity of operations for Critical Infrastructure · Disclosure of critical information to the government · Title 6 was last amended July 2023	Jul 2023		IAI		https://www.ecfr.gov/current/title-6/chapter-I/part-29 https://ecfr.federalregister.gov/	✓	✓	✓	✓	✓	✓	✓	✓
Electronic Fund Transfer Act (EFTA)	Reg	FDIC (Federal Deposit Insurance Corporation)	U.S.A.	Passed in 1978, establishes the rights and liabilities of consumers as well as the responsibilities of all participants in electronic fund transfer activities. Last Update: November 2022	Nov 2022		Wat	Referred to as "Regulation E"	https://www.fdic.gov/regulations/laws/rules/6000-1350.html	✓						✓	✓
Fair Credit Reporting Act	Reg	FTC (Federal Trade Commission)	U.S.A.	· Ensures credit information is accurate and up-to-date · Designed to promote accuracy and ensure the privacy of the information used in consumer reports	May 2023		Wat		https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act	✓						✓	✓
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.	Mar 2021	N/A	Wat		https://fraser.stlouisfed.org/title/federal-deposit-insurance-corporation-improvement-act-1991-415	✓						✓	✓
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	Jun 2023	N/A	Wat		https://www.acquisition.gov/far/subpart-32.11	✓						✓	✓
Federal Information Security Modernization Act of 2014 (FISMA)	Reg	Department of Homeland Security (DHS)	U.S.A.	The Federal Information Security Modernization Act of 2014 (FISMA 2014) updates the Federal Government's cybersecurity practices by: Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting."	Dec 2014		Enf		www.cisa.gov/federal-information-security-modernization-act								✓
FEMA 141: Emergency Management Guide for Business & Industry	Std	FEMA	U.S.A.	National Incident Management System, is designed to integrate best practices into a comprehensive framework for use by emergency management and response personnel in an all-hazards context nationwide.	Sep 2011	N/A	Wat		https://www.fema.gov/sites/default/files/2020-04/nims_training_program_sep2011.pdf	✓							
FFIEC - Outsourcing Technology Booklet	GP	FFIEC	U.S.A.	The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) "Outsourcing Technology Services Booklet" (booklet) provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.	2021		Enf	New rev. date 07/20/2021	ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx	✓							
FFIEC BCP Handbook: Business Continuity Planning (Nov 2019) "IT Examination Handbook"	Reg	FFIEC	U.S.A.	The BCM booklet describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. The BCM booklet also outlines BCM principles to help examiners evaluate how management addresses risk related to the availability of critical financial products and services. This booklet discusses BCM governance and its related components, including resilience strategies and plan development; training and awareness; exercises and tests; maintenance and improvement; and reporting for all levels of management, including the board of directors.	Nov 2019		Wat	New link	https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/appendix-a-examination-procedures/	✓							
Financial Institutions Reform, Recovery, and Enforcement Act- (FIRREA) of 1989; (P.L. 101-73 1989 HR 1278)	Reg		U.S.A.	Policy allows regulators/examiners to impose civil penalties for violations or non-compliance with regulations, laws, temporary agency orders or any breach of a written agreement between an agency and the institution. (pronounced "fie-ree-ah") Federal legislation passed in 1989 in response to the banking and savings and loan crisis, the FDIC bailout, and the bankruptcy of the Federal Savings and Loan Insurance Corporation (FSLIC). It reorganized much of the oversight and regulatory framework for financial institutions and created the Resolution Trust Corporation (now defunct) to receive and liquidate assets from failed financial institutions.	Aug 1989		Wat		H.R.1278 - 101st Congress (1989-1990): Financial Institutions Reform, Recovery, and Enforcement Act of 1989	✓	✓	✓	✓	✓	✓	✓	✓

FINRA Rule 4380 Mandatory Participation in FINRA BC/DR Testing Under Regulation SCI	Reg	Financial Industry Regulatory Authority (FINRA)	U.S.A.	In accordance with Rule 1004 of SEC Regulation SCI, FINRA will designate members that will be required to participate in FINRA's periodic, scheduled testing of its business continuity and disaster recovery (BC/DR) plan. FINRA will do so according to established criteria that are designed to ensure participation by those members that FINRA reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of its BC/DR plan.	Mar 2015		Enf		www.finra.org/rules-guidance/rulebooks/finra-rules/4380	✓							
FRB (Federal Reserve Banks) SR 13-1 / CA 13-1 (extends SR 03-5)	Reg	Board of Governors of the Federal Reserve System	U.S.A.	SR 13-1 guidance explains changes over the past several years in banking regulations related to auditor independence and limitations placed on the external auditor. This supplemental policy statement builds upon the 2003 Policy Statement SR 03-5, which remains in effect, and follows the same organizational structure, with a new section entitled "Enhanced Internal Audit Practices" and updates to Parts I-IV of the 2003 Policy Statement. (Extends: Amended Interagency Guidance on the Internal Audit Function and its Outsourcing SR 03-5) (Supersede: Outsourcing of Information and Transaction Processing Cross Reference: SR letter 97-35)	Jan-13		Enf		www.federalreserve.gov/supervisionreg/srletters/sr1301.htm	✓							
Gramm-Leach-Bliley Act of 1999, section 501 (b): (P.L. 106-102 1999 S 900)	Reg	Public Law	U.S.A.	Gramm-Leach-Bliley Bill - Section 501(b) FINANCIAL INSTITUTIONS SAFEGUARDS. In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.	Nov 1999		Enf		www.congress.gov/bill/106th-congress/senate-bill/900 www.congress.gov/106/plaws/publ102/PLAW-106publ102.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		http://www.bki.my/standards/ms-1970-business-continuity-management-framework	✓	✓	✓	✓	✓	✓	✓	✓
NASD Rulemaking: re: Business Continuity Plans and Emergency Contact Information	Reg	U.S. Securities and Exchange Commisions	U.S.A.	The NASD is proposing certain amendments to the proposed rule change, which requires member firms to create and maintain business continuity plans and provide the NASD with certain information to be used in the event of future significant business disruptions.10 Among other things, Amendment No. 4 clarifies that the proposed rule change would not mandate that members stay in business in the event of a significant	2013		Enf		http://www.sec.gov/rules/sro/34-48503.htm	✓							
HITECH Act Enforcement Interim Final Rule	Reg	U.S. Department of Health & Human Services	U.S.A.	The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. It mandates audits of health care providers to investigate and determine if they are in compliance with the HIPAA privacy and security rules. These two laws reinforce each other, and HITECH established data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI" (patient health information).	Jun 2017		Wat		https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html	✓	✓	✓	✓	✓	✓	✓	✓
Interagency Paper for Strengthening the Resilience of US Financial System (May 2003; Implementation in 2007)	Reg	FRB (Federal Reserve Bank) OCC (Office of the Comptroller of the Currency) SEC (Securities and Exchange Commission)	U.S.A.	During discussions about the lessons learned from September 11, industry participants and others agreed that three business continuity objectives have special importance for all financial firms and the U.S. financial system as a whole: Rapid recovery and timely resumption of critical operations following a wide-scale disruption; Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location; and A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible. Firms that Play Significant Roles in Critical Financial Markets (As a guideline, the agencies consider a firm significant in a particular critical market if it consistently clears or settles at least five percent of the value of transactions in that critical market.)	Apr 2003		Enf		www.sec.gov/news/studies/34-47638.htm	✓							
IRS Revenue Procedure 98-25; 1998-1 C.B. 689 (Supersedes Rev. Proc. 91-59, 1991-2 C.B. 841)	Reg	IRS (Internal Revenue Service)	U.S.A.	The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP)	Nov 2022		Enf		www.irs.gov/businesses/automated-records	✓							
ITIL - IT Infrastructure Library	Std	ITIL (IT Infrastructure Library)	U.S.A.	Global standard in the area of service management. ITIL® (IT Infrastructure Library®) is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. Contains comprehensive publicly accessible specialist documentation on the planning, provision and support of IT services	Feb 2018		Wat		www.itlibrary.org/	✓	✓	✓	✓	✓	✓	✓	✓
The Joint Commission	Std.	The Joint Commission	U.S.A.	The mission of The Joint Commission is to continuously improve health care for the public, in collaboration with other stakeholders, by evaluating health care organizations and inspiring them to excel in providing safe and effective care of the highest quality and value. They do this by setting quality standards, evaluating an organization's performance, and providing an interactive educative experience that provides innovative solutions and	Nov 2022	Yes (varies per Certification or Accreditation)	Wat		www.jointcommission.org/accreditation-and-certification/health-care-settings/hospital/learn/our-standards/		✓						

The Joint Commission Quick Safety 41: Emergency Management; Need for continuity of operations planning	Std.	The Joint Commission	U.S.A.	Describes the critical need for continuity of operations planning along with best practices in continuity of operations planning.	Nov 2022		Wat		www.jointcommission.org/resources/news-and-multimedia/newsletters/newsletters/quick-safety/quick-safety-41-emergency-management-need-for-continuity-of-operations-planning/		✓							
Office of National Continuity Programs	Std	FEMA	U.S.A.	On behalf of the President, the Secretary of Homeland Security, and the FEMA Administrator, the Office of National Continuity Programs (ONCP) guides the planning, implementation and assessment of continuity programs that enable federal, state, local, tribal and territorial governments to continue performing essential functions and delivering critical services when typical operations are disrupted by an emergency. ONCP also ensures that at all times, the President, federal agencies and governments at all levels are able to provide timely and effective alerts and warnings regarding natural disaster, acts of terrorism and other manmade disasters or threats to public safety. The development, integration and maintenance of continuity considerations and capabilities is a shared responsibility of the whole community and helps build a more resilient nation equipped to sustain essential functions, deliver critical services and stabilize community lifelines under all conditions.	May 2023	N/A	Enf	Updated Title, and Last Revision Date	https://www.fema.gov/about/offices/continuity	✓	✓	✓	✓	✓	✓	✓	✓
NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan	Reg	CFTC (Commodity Futures Trading Commission)	U.S.A.	Requires each member to: a) establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant disruption. b) provide NFA with, and keep current, the name and contact information for all key management employees. c) provide NFA with the name of and contact information for an individual who NFA can contact in the event of an emergency.	2019	N/A	Enf		https://www.nfa.futures.org/rulebook/rules.aspx?RuleID=RULE%202-38&Section=4	✓							✓	
NFPA 111: Standard on Stored Electrical Energy Emergency and Standby Power Systems	Std	NFPA (National Fire Protection Association	U.S.A.	This standard covers preformance requirements for stored electrical energy systems providing an alternate source of electrical power in buildings and facilities in the event that the normal electrical power woruce fails. Systems include power sources, transfer equipment, controls, supervisory equipment, and accessory equipment needed to supply electrical power to the selected circuits.	2022	Print- $70; digital access starts at $11.99 per month; there is a Free Access as well	Enf	Updated Summary/Description and Associated Cost	https://catalog.nfpa.org/NFPA-111-Standard-on-Stored-Electrical-Energy-Emergency-and-Standby-Power-Systems-P1225.aspx?order_src=D750&gclid=EAIaIQobChMIx42SmrfbSwIVDZyzCh2rAQJdEAAYASAAEgJKqPD_BwE	✓						✓	
NFPA 232: Standard on Protection of Records	Std	NFPA (National Fire Protection Association	U.S.A.	This 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.	2022	Print- $70; digital access starts at $11.99 per month; there is a Free Access as well		Updated Summary/Description and Associated Cost	https://catalog.nfpa.org/NFPA-232-Standard-for-the-Protection-of-Records-P1243.aspx	✓						✓	
NFPA 1600: Standard on Continuity, Emergency, and Crisis Management	Std	NFPA (National Fire Protection Association	U.S.A.	Has been adopted by the US Department of Homeland Security as a voluntary consensus standard for emergency preparedness. The National Commission on Terrorist Attacks Upon the Unites States recognized NFPA 1600 as our National Preparedness Standard. Widely used by public, not-for-profit, nongovernmental, and private entities on a local, regional, national, international and global basis. The current edition is the last published edition as a stand-alone standard. The standard has been consolodated into NFPA 1660. NFPA 1660 - Standard for Emergency, Continuity, and Cirsis Management: Preparedness, response, and Recovery Scope- this standard estabilses a common set of criteria for emergency managment and business continuity programs; mass evacuation, sheltering, and re-entry programs; and the development of pre-incident plans for personnel responding to emergencies. (2024)	2019; 2024	PDF- $84; print $78 (both offered in Spanish); digitial access $11.99 per month, Free Access as well. NFPA 1660- 2024 Print- $91	Enf		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.	The publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines.	Nov 2010	N/A	Enf		https://csrc.nist.gov/CSRC/media/Events/HIPAA-2010-Safeguarding-Health-Information-Buil/documents/2-2b-contingency-planning-swanson-nist.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 components 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	Dec 2020	N/A	IAI		https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	✓	✓	✓	✓	✓	✓	✓	
NIST Special Publication 800-34 Rev. 1 Contingency Plannig Guide for Federal Inforamtion Systems	Reg	National Institute of Standards and Technology (NIST)	U.S.A.	The purpose of this publiciation is to provide instructions, recommendateions and considerations for federal information system contingency planning. This guide defines the seven-step contingency planning process that organizations may apply to develop and maintain a viable contingency planning program for their informaiton systems.	May-10	N/A	Enf		nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf	✓	✓	✓	✓	✓	✓	✓	✓
OCC 2000-14: Infrastructure Threats -- Intrusion Risks: Message to Bankers and Examiners	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.	May 2000		Wat		www.occ.gov/news-issuances/bulletins/2000/bulletin-2000-14.html	✓							
OCC Bulletin 2008-16 - Information Security: Application Security	Reg	OCC	U.S.A.	This bulletin reminds national banks and their technology service providers that application security1 is an important component of their information security program. All applications, whether internally developed, vendor-acquired,2 or contracted for,3 should be subject to appropriate security risk assessment and mitigation processes. Vulnerabilities in applications (see Appendix A) increase operational and reputation risk as unplanned or unknown weaknesses may compromise the confidentiality, availability, and integrity of data. Although this guidance is focused on the risks and risk management techniques associated with Web-based applications, the principles are applicable to all types of software.	5/8/2008		Enf		www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-16.html	✓							

~~OCC Bulletin 2013-29 – Third-Party Relationships: Risk Management Guidance~~ OCC Bulletin 2023-17 - Third-Party Relationships: Interagency Guidance on Risk Management	Reg	OCC	U.S.A.	The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws. This bulletin rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk." This bulletin supplements and should be used in conjunction with other OCC and interagency issuances on third-party relationships and risk management listed in appendix B. In connection with the issuance of this bulletin, the OCC is applying to federal savings associations (FSA) certain guidance applicable to national banks, as indicated in appendix B.	6/6/2023		Enf	Rescinds OCC Bulletin 2013-29, New title, number, summary, and link.	www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html or https://www.occ.gov/news-issuances/federal-register/2023/88fr37920.pdf	✓	✓	✓	✓	✓	✓	✓	✓
OSHA - Occupational Safety and Health Administration	Reg	OSHA (Occupational Safety and Health Administration)	U.S.A.	Some businesses may be required by regulation to establish Emergency Action Plans meeting certain requirements (see 29 CFR 1910.38 and OSHA's compliance policy). Effective plans should take into account what personal protective equipment workers may require, as well as other resilience resources for emergency responses. Employers should also be aware that some states have OSHA-approved occupational safety and health plans that may have more stringent requirements than what Federal OSHA requires.	Nov 2002		Enf		https://www.osha.gov/emergency-preparedness	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risk Management Handbook Volume III, Standard 4.4 Contingency Planning	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. Replaces RMH Vol II Procedure 4.4.	Feb 2014		Enf		https://www.cms.gov/files/document/rmhviii4-4contingencyplanningstandardpdf		✓						✓
SEC Adviser Business Continuity and Transition Planning PROPOSED Rule	Reg	Securities and Exchange Commission (SEC)	U.S.A.	PROPOSED new rule and rule amendments under the Investment Advisers Act of 1940 ("Advisers Act") that would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations.	2016		Wat	The SEC has invited feedback on the proposed rule. Below is an excerpt from the rule: "Proper planning and preparation for possible distress and other significant disruptions in an adviser's operations is essential so that, if an entity has to exit the market, it can do so in an orderly manner, with minimal or no impact on its clients. As discussed above, an adviser's fiduciary duty obligates it to take steps to protect client interests from being placed at risk as a result of the adviser's inability to provide advisory services and, thus, it SEC-registered advisers should be required to adopt and implement a written business continuity and transition plan that is tailored to the risks associated with the adviser's operations and includes certain components, reflecting its critical role as an agent for its clients."	www.sec.gov/rules/proposed/2016/ia-4439.pdf	✓							
SEC Regulation SCI	Reg	Securities and Exchange Commission (SEC)	U.S.A.	The U.S. Securities and Exchange Commission adopted Regulation Systems Compliance and Integrity and Form SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. Specifically, the rules are designed to: Reduce the occurrence of systems issues; Improve resiliency when systems problems do occur; Enhance the Commission's oversight and enforcement of securities market technology infrastructure. Regulation SCI applies to "SCI entities," a term which includes self-regulatory organizations ("SROs"), including stock and options exchanges, registered clearing agencies, FINRA and the MSRB, alternative trading systems ("ATSs"), that trade NMS and non-NMS stocks exceeding specified volume thresholds, disseminators of consolidated market data ("plan processors"), and certain exempt clearing agencies. Regulation SCI applies primarily to the systems of SCI entities that directly support any one of six key securities market functions - trading, clearance and settlement, order routing, market data, market regulation, and market surveillance ("SCI systems"). Subject to certain exceptions, the compliance date of Regulation SCI was nine months after the effective date of the regulation, or November 3, 2015.	Nov 2014		Enf	The SEC designed Regulation SCI in response to securities markets being increasingly dependent on technology and automated systems. Regulation SCI strives to reduce the number of market disturbances stemming from this reliance on technology, as well as speed up recovery when disturbances do occur.	This is the location of the published final rule: Securities and Exchange Commission -- SEC Final Rules 2014 https://www.sec.gov/rules/final/finalarchive/finalarchive2014.shtml Select Release 34-73639 (Nov 19, 2014) for a pdf of the rule This is the location of the rule correction: Securities and Exchange Commission -- SEC Final Rules 2015 https://www.sec.gov/rules/final/finalarchive/finalarchive2015.shtml Select Release 34-73639A (Dec 22, 2015) for a pdf of the rule correction	✓							
FINRA 4370. Business Continuity Plans and Emergency Contact Information	Reg	FINRA is authorized by Congress to protect America's investors	U.S.A.	Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to FINRA staff.	Feb 2015			No changes since 2015.	https://www.finra.org/rules-guidance/rulebooks/finra-rules/4370	✓							
FINRA BCP Guide	Reg	FINRA is authorized by Congress to protect America's investors	U.S.A.	FINRA requires firms to create and maintain written business continuity plans (BCPs) relating to an emergency or significant business disruption. Rule 4370—FINRA's emergency preparedness rule — spells out the required BCP procedures. A firm's BCP must be appropriate to the scale and scope of its business.	Dec 2020			Regulatory notice 21-44 published in 2021 Business Continuity Planning Lessons from the COVID-19 Pandemic.	https://www.finra.org/rules-guidance/key-topics/business-continuity-planning	✓							

H.R.3844 - Federal Information Security Management Act of 2002 S.2521, Public Law No. 113-283 updates FISMA 2002: Federal Information Security Modernization Act of 2014.	Reg	US Congress	U.S.A.	Federal Information Security Management Act of 2002 - Requires the Director of the Office of Management and Budget to oversee Federal agency information security policies and practices, including by requiring each Federal agency to identify and provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of information or information systems. Requires each agency's senior officials to provide security for the information and systems that support their operations and assets and to develop plans and procedures to ensure the continuity of such information and systems. **Updates in 2014 Act.** Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; Amending and clarifying the Office of Management and Budget's (OMB) oversight	Dec 2014		Enf		H.R.3844 - 107th Congress (2001-2002): Federal Information Security Management Act of 2002	Congress.gov	Library of Congress https://www.congress.gov/bill/113th-congress/senate-bill/2521/text	✓	✓	✓	✓	✓	✓	✓	✓

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: Sept. 9, 2023

Categories (column B):