Rules & Regulations Acronyms

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: March 9, 2025

Acronym	Country	Definition
ACH	U.S.A.	Automated Clearinghouse Association (of the Federal Reserve Bank)
AICPA	U.S.A.	American Institute of Certified Public Accountants
ANAO	Australia	Australian National Audit Office
ANSI	U.S.A.	American National Standards Institute
APRA	Australia	Australian Prudential Regulation Authority (APRA)
ARMA	U.S.A.	Association of Records Managers and Administrators
BOJ	Japan	Bank of Japan
BSE	India	Bombay Stock Exchange
BSI	U.K.	British Standards Institute
CCPA	U.S.A.	Consumer Credit Protection Act
CFR	U.S.A.	Code of Federal Regulations
CISP	U.S.A.	Customer Information Security Program
CMS	U.S.A.	Centers for Medicare and Medicaid Servicess
CNB	Croatia	Croatian National Bank (Hrvatska Narodna Banka - HNB)
COBIT	U.S.A.	Control Objectives for information and related Technology
COSO	U.S.A.	Committee of Sponsoring Organizations (of the Treadway Commission)
CSA	Canada	Canadian Standards Association
DHS	U.S.A.	Department of Homeland Security (USA)
DMISA	South Africa	Disaster Management in South Africa, is the professional body for SA.
DRII	International	Disaster Recovery Institute International
EFTA	U.S.A.	Electronic Fund Transfer Act
FCC	U.S.A.	Federal Communications Commission
FDIC	U.S.A.	Federal Deposit Insurance Corporation
FDICIA	U.S.A.	Federal Deposit Insurance Corporation Improvement Act
FFIEC	U.S.A.	Federal Financial Institutions Examination Council
FICOM	Canada	The Financial Institutions Commission (FICOM) is a regulatory agency responsible pension, financial services and real estate sectors in British Columbia.
FINRA	U.S.A.	Financial Industry Regulatory Authority (FINRA) is the largest independent regulator for all securities firms doing business in the United States. http://www.finra.org/AboutFINRA/
FIRREA	U.S.A.	Financial Institutions Reform, Recovery, and Enforcement Act
FISC	Japan	The Center for Financial Industry Information System
FISMA	U.S.A.	Federal Information Security Management Act
FRB	U.S.A.	Federal Reserve Bank
FSA	U.K.	Financial Services Authority
FSSCC	U.S.A.	Financial Services Sector Coordinating Council for Critical Infrastructure Protection
FTC	U.S.A.	Federal Trade Commission

GAO	U.S.A.	General Accounting Office
GAP	U.S.A.	Generally Accepted Practice
HIPAA	U.S.A.	Health Insurance Portability and Accountability Act
HKMA	Hong Kong	Hong Kong Monetary Authority
IIROC	Canada	The Investment Industry Regulatory Organization of Canada oversees all investment dealers and trading activities in Canada.
IRS	U.S.A.	Internal Revenue Service
ISO	International	International Organization for Standardization
ITIL	International	Information Technology (IT) Infrastructure Library
MAS	Singapore	Monetary Authority of Singapore
MFDA	Canada	Mutual Fund Dealer Association (of Canada)
NASD	U.S.A.	North American Securities Dealers Association
NFPA	U.S.A.	National Fire Protection Association
NIST	U.S.A.	National Institute of Standards and Technology, U.S. Department of Commerce
NSE	India	National Stock Exchange
NYSE	U.S.A.	New York Stock Exchange
OCC	U.S.A.	Office of the Comptroller of the Currency
OSC	Canada	Ontario Securities Commission
OSHA	U.S.A.	Occupational Safety and Health Administration
PCAOB	U.S.A.	Public Company Accounting Oversight Board
RBI	India	Reserve Bank of India
SAMOS	South Africa	South African Multiple Option Settlement (SAMOS) system is South African's Real Time Gross Settlement (RTGS) System.
SAS	U.S.A.	Statement on Auditing Standards
SEBI	India	Securities & Exchange Board of India
SEC	U.S.A.	Securities and Exchange Commission
SIFMA	U.S.A.	Securities Industry and Financial Markets Association

May 2024

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: March 9, 2025

Person working on section - you can also add comments in Notes section	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)	Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including Nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies
Ashley Goosman	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: Opening	dates vary	No charge	Amb		https://www.anao.gov.au/work?query=BCM	✓	✓	✓	✓	✓	✓	✓	✓
Ashley Goosman	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.	Jun 2024	No charge	IAI	The Australian Prudential Regulation Authority (APRA) has released its finalised prudential practice guide to help banks, insurers and superannuation trustees strengthen their management of operational risk and improve business continuity planning.	The new Prudential Practice Guide CPG 230 Operational Risk Management (CPG 230) is designed to assist in the implementation of Prudential Standard CPS 230 Operational Risk Management (CPS 230), which was finalised in July last year and takes effect from 1 July 2025 (links imbedded). See Press Release for more information.	✓							
Ashley Goosman	APRA - Prudential Standard CPS 230 Operational Risk Management	Std	Australian Prudential Regulation Authority (APRA)	Australia	The aim of this Prudential Standard is to ensure that an APRA-regulated entity is resilient to operational risks and disruptions. An APRA-regulated entity must effectively manage its operational risks, maintain its critical operations through disruptions, and manage the risks arising from service providers. An APRA-regulated entity's approach to operational risk must be appropriate to its size, business mix and complexity. The key requirements of this Prudential Standard are that an APRA-regulated entity must: • identify, assess and manage its operational risks, with effective internal controls, monitoring and remediation; • be able to continue to	Jul 2025	No charge	Wat	Prudential Standard CPS 230 will support Prudential Standard CPS 220 Risk Management and replace Prudential Standard SPS 231 Outsourcing (SPS 231) and Prudential Standard SPS 232 Business Continuity Management (SPS 232) for RSE licensees. It will commence on 1 July 2025,	https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf	✓							
Ashley Goosman	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	✓	✓	✓	✓	✓	✓	✓	✓
Ashley Goosman	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	Last updated Updated: Wednesday 29 August 2018	Better practice guides | Australian National Audit Office (anao.gov.au)		✓	✓	✓	✓			✓
Ashley Goosman	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)	✓							
Ashley Goosman	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	✓	✓	✓	✓	✓	✓	✓	✓
Corey Hahn	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. The new version of the standard includes a crosswalk from the old controls to the new controls to assist in transition. Some companies may need to seek SOC 2 compliance instead of ISO 27001.	Oct 2022 with amendment added in Aug 2024	No charge	Enf	Amendment added in 2024 to reference climate action changes: 4.1 The organization shall determine whether climate change is a relevant issue. 4.2 Relevant interested parties can have requirements related to climate change. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:amd:1:v1:en	https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en	✓	✓	✓	✓	✓	✓	✓	✓
Corey Hahn	20 Questions Directors Should Ask about Crisis Management	GP	Institute 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	✓							

Corey Hahn	B.C. Emergency & Disaster Management 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.	Dec 2023		Wat	The Emergency and Disaster Management Act of 2023 repealed the Emergency Program Act.	https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_96111_01	✓	✓	✓	✓	✓	✓	✓	✓
Corey Hahn	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	Canada Sarbanes-Oxley (CSOX) guidelines	https://rsmcanada.com/what-we-do/services/consulting/risk-advisory/internal-audit-and-controls-services/bill-198-sarbanes-oxley-compliance.html	✓	✓	✓	✓	✓	✓	✓	✓
Corey Hahn	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	✓							
Corey Hahn	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	✓							
Corey Hahn	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	These Regulations are the principal means of supplementing the legislative framework set out in sections 4.7 to 4.87 of the Act. They are designed to enhance preparedness for acts or attempted acts of unlawful interference with civil aviation and to facilitate the detection of, prevention of, response to and recovery from acts or attempted acts of unlawful interference with civil aviation.	Jan 2023		Wat	Last amendment added in January 2023	Canadian Aviation Security Regulations, 2012 (justice.gc.ca)			✓		✓		✓	✓
Corey Hahn	Derivatives Regulation, RRQ, c I-14.01	Reg	Regulations of Quebec	Canada	This Act seeks to foster honest, fair, efficient and transparent derivatives markets and to protect the public from unfair, improper or fraudulent practices and market manipulation. It also seeks to ensure that the public, and more particularly, market participants and their clients, have access to adequate, true and clear information, tailored to the level of financial knowledge and experience of those for whom it is intended.	Nov 2024		Enf	Consolidated Regulations updated to November 30, 2024.	https://www.legisquebec.gouv.qc.ca/en/document/cs/I-14.01%20/	✓							✓
Doug Nelson	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	May-03		Wat		Earthquake Planning Guide for Business (sclr.org)	✓	✓	✓	✓	✓	✓	✓	
Doug Nelson	CSA Z1600:17 Emergency and Continuity Management Program	Reg	National Standard of Canada, published by CSA Group	Canada	This Standard provides requirements for a continual improvement process to develop, implement, evaluate, maintain, and improve an emergency and continuity management program that addresses the components of prevention and mitigation, preparedness, response, and recovery. It is applicable, in whole or in part, to organizations of all sizes and purposes.	Jan 2024		Enf	This is the third edition of CSA Z1600, Emergency and continuity management program. It supersedes the previous editions published in 2014, and in 2008 under the title, Emergency management and business continuity programs.	https://www.csagroup.org/store/product/Z1600-17/	✓	✓	✓	✓	✓	✓	✓	✓
Doug Nelson	Emergency Management Act	Reg	Senate and House of Commons of Canada	Canada	Requires the Minister of Public Safety in Gov.Canada to: establish policies and programs for the preparation of emergency management plans; control emergency management plans prepared by federal entities; coordinate the federal response to an emergency; coordinate federal and provincial emergency management activities coordinate the provision of non-finaincial assistance to a province and any declarations; participate in international emergency managment activities; establish arrangements for continuity of government; promote a common approach to emergency management, including the adoption of standards and best practices; and conduct exercises and providing emergency management education and training.	Aug 2007		Enf	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)	✓	✓	✓	✓	✓	✓	✓	✓
Doug Nelson	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.	Jun 2011		Enf	**This document is being updated under Engagement on Proposed Modernization of the Emergency Management and Civil Protection Act**	https://www.ontario.ca/laws/statute/90e09	✓	✓	✓	✓	✓	✓	✓	✓
Doug Nelson	Emergency Plan for Small Business	GP	PreparedBC & Emergency Preparedness for Industry and Commerce Council EPICC	Canada	This resource is designed to help small business owners plan and prepare for emergencies that could interrupt operations. Use this template as a starting point and add to it as needed. One simple step today can make a difference in how effectively your business responds to and recovers from a disaster.	Jun-23	N/A	Wat		https://www2.gov.bc.ca/assets/gov/public-safety-and-emergency-services/emergency-preparedness-response-recovery/embc/preparedbc/preparedbc-guides/preparedbc_small_business_plan.pdf								✓
Doug Nelson	All Hazards Risk Assessmen	GP	Public Safety Canada	Canada	The All Hazards Risk Assessment (AHRA) methodology, supports all federal government institutions in fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for EM planning. In Canada, the approach to EM is based on four components: prevention/mitigation, preparedness, response and recovery.	Mar-13	N/A	Enf		https://www.publicsafety.gc.ca/cnt/rsrcs/pb	✓	✓	✓	✓	✓	✓	✓	✓
Doug Nelson	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)	✓	✓	✓	✓	✓	✓	✓	✓

Doug Nelson	Integrity and Security - Guideline	GP	Office of the Superintendent of Financial Institutions (OFSI)	Canada	The Office of the Superintendent of Financial Institutions Act includes a requirement for OSFI to supervise financial institutions to determine that they have adequate policies and procedures to protect themselves against threats to their integrity or security, including foreign interference. Accordingly, financial institutions must take steps to ensure they are managing risks associated with integrity and security by putting such policies and procedures in place.	Jan 2024	N/A	Enf	This guideline sets out expectations for integrity and security policies and procedures. It is applicable to all federally regulated financial institutions, including foreign bank branches and foreign insurance company branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada.	https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/integrity-security-guideline	✓							
Doug Nelson	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.	Apr 2023	N/A	Enf	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 foreign insurance company branches are set out in Guideline E-4: Foreign Entities Operating in Canada on a	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx	✓							
Doug Nelson	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.	Jul 2022	N/A	Enf		https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx	✓							
Doug Nelson	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 branches.	Mar 2023	N/A	Enf	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 effectively while managing its climate-related risks prudently.	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b15-dft.aspx	✓							
Melanie Lucht	Operational 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).	Aug 2024	N/A	Enf	Financial institutions operate in a fast-paced, complex environment with increasing risks to their operations, notably their people, facilities, and systems. Robust operational risk management and resilience enhance their ability to prevent, detect, respond to, and recover from adverse events, while continuing to deliver critical operations.	https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21.aspx	✓							
Melanie Lucht	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.	Feb 2023	NA	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	https://static.aer.ca/prd/documents/directives/Directive071.pdf				✓				
Melanie Lucht	IIROC Rule 17.16 - Business Continuity Plan Requirement	Reg	Investment Industry Regulatory Organization of Canada	Canada	Section 4711 of the IIROC Rules requires every Dealer Member to establish and maintain a business continuity plan identifying the necessary procedures to be undertaken during an emergency or significant business disruption. Every Dealer Member must also conduct an annual review and test of its plan, and provide an annual CEO certification to IIROC addressing their plan and compliance with IIROC rules.	Sep 2021	NA			https://www.iiroc.ca/members/dealer-member-compliance/business-continuity https://www.iiroc.ca/news-and-publications/notices-and-guidance/industry-business-continuity-planning-test	✓	✓	✓	✓	✓	✓	✓	✓
Melanie Lucht	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	Jun 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_E				✓				
Melanie Lucht	MR-0056: Member Regulation Notice - Business Continuity Planning	Reg	Mutual Fund Dealers Association of Canada	Canada	Provides guidance to Members regarding the development and implementation of business continuity plans.	Oct 2006	NA	Enf	Responsibilities on Business Continuity: Back-up Operations Centers and Data Recovery Sites	https://www.ciro.ca/news-room/publications/business-continuity-planning	✓							
Melanie Lucht	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.	9/1/2020 and 9/13/2023	NA	Wat		https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-101/unofficial-consolidation-national-instrument-21-101-marketplace-operation-0#_Toc50620153_ https://www.bcsc.bc.ca/-/media/PWS/New-Resources/Securities-Law/Instruments-and-Policies/Policy-3/31103-NI-September-13-2023.pdf?dt=20230913152424	✓							

Melanie Lucht	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 level of	Apr 2023	$45	Enf	Updated in 2023 and replaced Business Continuity guidelines for 3rd parties.	https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/third-party-risk-management-guideline	✓							
Colleen Huber	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)	✓	✓	✓	✓	✓	✓	✓	✓
Colleen Huber	Croation Sabor: Credit Institutions Act	Reg	Croatian National Bank (CNB)	Croatia	Credit Institutions Act	May 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	✓							✓
Colleen Huber	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	Update 08-2006 https://op.europa.eu/en/publication-detail/-/publication/7921d3b2-a6c0-4915-a828-96e162123ede/language-en/format-HTML/source-search	https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:31987D0600		✓	✓	✓	✓			✓
Colleen Huber	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		✓	✓	✓	✓			✓
Colleen Huber	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		✓	✓	✓	✓	✓		✓
Colleen Huber	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	✓	✓	✓	✓	✓	✓	✓	✓
Colleen Huber	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.	2013	N/A	Enf	Last revision date corrected to 2013	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013D1313	✓	✓	✓	✓	✓	✓	✓	✓
Colleen Huber	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	✓	✓	✓	✓	✓	✓	✓	✓

Colleen Huber	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		✓	✓	✓	✓	✓	✓	✓
Colleen Huber	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.	2019	N/A	Enf		https://drmkc.jrc.ec.europa.eu/knowledge/science-for-drm/recommendations-for-national-risk-assessment-for-disaster-risk-management-in-eu	✓	✓	✓	✓	✓	✓	✓	✓
Colleen Huber	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://drmkc.jrc.ec.europa.eu/science-for-drm/science-for-disaster-risk-management-2017	✓	✓	✓	✓	✓	✓	✓	✓
Colleen Huber	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	✓							
Colleen Huber	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)	Reg	The European Parliament and the Council of the European Union	European Union	Known as DORA - Digital Operational Resilience Act, this regulation is a recent European legislation which aims to ensure the security and business continuity of the EU fast-growing "digital finance ecosystem". It is going to affect a variety of "financial entities", as well as coverings several management disciplines that fall under the organizational resilience umbrella.	2022	added the links	Enf	Date of effect: 16/01/2023; Entry into force Date pub. +20 See Art 64 Date of effect: 17/01/2025; Application See Art 64	https://eur-lex.europa.eu/eli/reg/2022/2554/oj Regulatory technical standards: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-35_-_Final_report_on_RTS_on_harmonisation_of_conditions_for_OVS_conduct.pdf https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024_54_-_Final_Report_RTS_on_JET.pdf https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf Guidelines: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-34_-_Final_report_GL_on_costs_and_losses.pdf	✓							
Rich Cocchaira	IT Requirements for Payment and E-money institutions	Reg, Std,GP	BaFin, Germin Federal Financial Supervisory Authority	Germany	The supervisory requirements that payment and e-money institutions must meet for the due and proper conduct of business in relation to the use of information technology and to ensure cyber security	Nov 2021		sanctions	Updated in 2021	BaFin - Expert Articles - IT Requirements for Payment and E-money Institutions	✓							
Rich Cocchaira	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	May 2022		Enf	Updated in 2022. Additional information on Operational Resilience can be found as well.	Hong Kong Monetary Authority - Business Continuity Planning (hkma.gov.hk) https://www.hkma.gov.hk/media/chi/doc/key-information/guidelines-and-circular/2022/20220531c1a2.pdf	✓							
Rich Cocchaira	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	No change	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	✓						✓	
Rich Cocchaira	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	No change	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 https://www.ojk.go.id/en/berita-dan-kegiatan/info-terkini/Pages/Cybersecurity-Guidelines-for-Financial-Sector-Technology-Innovation-ITI-Providers.aspx	✓							

Rich Cocchaira	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	No change	https://www.bis.org/publ/joint17.htm https://www.bis.org/publ/joint14.pdf	✓						✓	
Rich Cocchaira	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.	6/1/2011 3/2021		Enf	New "Principals of Operational Risk and Resilience" published in 2021.	https://www.bis.org/bcbs/publ/d516.htm https://www.bis.org/publ/bcbs189.pdf	✓							
Rich Cocchaira	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	$217	Enf	No change	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		✓	✓	✓	✓	✓	✓	✓
Rich Cocchaira	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. < $49 USD	Enf	Price reduced from $200 to $49	https://www.isaca.org/ https://store.isaca.org/s/store#/store/browse/detail/a254w000004KoEfEAK	✓	✓	✓	✓	✓	✓	✓	
Rich Cocchaira	The BCI Good Practice Guidelines	Std	BCI (Business Continuity Institute)	International	The Good Practice Guidelines (GPG V7.0) 2024 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.	Sep 2024		Enf	Version 7.0 is now available.	https://www.thebci.org https://www.thebci.org/resource/good-practice-guidelines--gpg--edition-7-0.html					✓			✓
Joan Landry	DRI International Professional Practices for Business Continuity Management	GP	DRII (Disaster Recovery Institute International)	International	The Professional Practices for Business Continuity Management is a body of knowledge designed to assist in the development, implementation, and maintenance of business continuity programs. It also is intended to serve as a tool for conducting assessments of existing programs	2024		Enf		https://drii.org/ https://drii.org/resources/professionalpractices/EN	✓	✓	✓	✓	✓	✓	✓	✓
Joan Landry	ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements	Std	ISO	International	ISO 22301 is the international standard for Business Continuity Management Systems (BCMS). It provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.	Oct 2019			https://www.iso.org/standard/75106.html	https://www.iso.org/standard/75106.html	✓	✓	✓	✓	✓	✓	✓	✓
Joan Landry	ISO 22320:2018 Security and Resilience Emergency management — Guidelines for incident management	GP	ISO	International	ISO 22320:2018, Security and resilience - Emergency management - Guidelines for incident management, is an international standard published by International Organization for Standardization that provide guidelines to be used for organizations that helps to mitigate threats and deal with incidents to ensure continuity of basic function of society (for example water and food supplies, health, rescue services, fuel delivery, and electricity).	Jan 2018				https://www.iso.org/standard/67851.html								✓
Joan Landry	ISO 9000 Family - Quality Management	Std	ISO	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.	Feb 2019		Amb			✓		✓		✓	✓	✓	

Joan Landry	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 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 2021		Wat		ISO - ISO 9001:2015 - Quality management systems — Requirements					✓			
Joan Landry	ISO 9004:2018Quality management - Quality of an organization — Guidance to achieve sustained success	Std	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	Jan 2020		Wat		ISO - ISO 9004:2018 - Quality management — Quality of an organization — Guidance to achieve sustained success	✓	✓	✓	✓	✓	✓	✓	✓
Joan Landry	ISO/IEC 27002:2022 Information technology -- Security techniques -- Code of practice for information security controls	Std	ISO (International Organization for Standardization)	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. **This standard has been revised by ISO/IEC 27005:2022**	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 T. **This standard has been withdrawn and replaced by ISO/IEC 27005:2022**	https://www.iso.org/standard/75652.html								✓
Joan Landry	ISO/IEC 27005:2022 - 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 27002 is an international standard that provides guidance for organizations looking to establish, implement, and improve an Information Security Management System (ISMS) focused on cybersecurity. While ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers best practices and control objectives related to key cybersecurity aspects including access control, cryptography, human resource security, and incident response. The standard serves as a practical blueprint for organizations aiming to effectively safeguard their information assets against cyber threats. By following ISO/IEC 27002 guidelines, companies can take a proactive approach to cybersecurity risk management and protect critical information from unauthorized access and loss.	Mar 2022		Enf	This standard has been withdrawn and replaced by ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html								✓
Leslie Fife	Circ. 285 di Banca d'Italia - Titolo IV - Cap. 5 "La Continuità Operativa"	Reg	Banca d'Italia	Italy	The Regulation n. 38 was originally issued by IVASS in 2018 and then reviewed and updated in March 2021. Among several other requirements, it imposes business continuity practices to insurance companies operating in Italy.	Aug 2025		Enf	All text in Italian. No translation provided.	https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/	✓							
Leslie Fife	Regolamento n. 38 di IVASS	Reg	IVASS	Italy	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.	Nov 2025		Enf	All text in Italian. No translation provided.	https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/index.html	✓							
Leslie Fife	Business Continuity Planning (Bank of Japan)	Std	BOJ (Bank of Japan)	Japan	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)	2016		Enf		https://www.boj.or.jp/en/about/bcp/index.htm	✓							

Leslie Fife	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)	2012* State of Emergency documentation 2 Jan 2021.	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://lX-938 Republic of Lithuania Law on a State of Emergency (lrs.lt), valid 2 Jan 2021.	https://e-seimas.lrs.lt/rs/legalact/TAD/702d015216b811e6aa14e8b63147ee94/format/ISO_PDF/ New link?: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/9651e8429b9711ec9e62f960e3ee1cb6	✓	✓	✓	✓	✓	✓	✓	✓
Leslie Fife	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.	Oct 2018		Enf	This is only a guideline.	extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G014_2018_BUSINESS-CONTINUITY-MANAGEMENT-(BCM)-REQUIREMENTS.pdf	✓	✓	✓	✓	✓	✓	✓	
Leslie Fife	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	Contains the followig: Section 141 Supervision by Risk Section 142 Risk Governance Framework Section 143 Credit Risk Management Section 144 Market Risk Management Section 145 Liquidity Risk Management Section 145-A Liquidity Coverage Ratio (LCR) Section 146 Operational Risk Management Section 147 Bank Protection Section 148 Information Technology Risk Management Section 149 Business Continuity Management Section 150 Social Media Risk Management Section 151 Guidelines on the Conduct of Stress Testing Exercises	2018		Enf		https://morb.bsp.gov.ph/e-risk-management/	✓							
David Dunlap	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:	Jun 2022		IAI		MAS Business Continuity Management Guic	✓							
David Dunlap	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.	Dec 2023	NA	IAI		Outsourcing Guidelines Jul 2016 revised on 5 Oct 2018.pdf (mas.gov.sg)	✓							
David Dunlap	SS ISO 22301:2020+A1:2024 Security and resilience – Business continuity management systems – Requirements	Std	kirchner	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 2024	NA	Enf		https://www.singaporestandardseshop.sg	✓	✓	✓	✓	✓	✓	✓	✓

David Dunlap	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	✓	✓	✓	✓	✓	✓	✓	✓
David Dunlap	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 municipal and provincial intergovernmental forums established in terms of	Dec 2015	NA	Enf	Disaster Management Amendment Act 16 of 2015 (www.gov.za)	Disaster Management Amendment Act 16 of 2015 (www.gov.za)	✓	✓	✓	✓	✓	✓	✓	✓
David Dunlap	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.	2016	NA	Enf	The previous link was to the latest report, not the actual framework, I have updated the link.	https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/NPS%20Oversight%20framework%202016.pdf	✓	✓	✓	✓	✓	✓	✓	✓
David Dunlap	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.	2025	NA		Updated to 2025	Payments and Settlements (resbank.co.za) https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/Vision%202025.pdf	✓							
Rich Cocchaira	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	Jun 2021	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 referred to in paragraph 3.15 should read £15 billion.	https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf	✓							
Rich Cocchaira	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 2022	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	✓							
Rich Cocchaira	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	2023	N/A	Enf	Amends or repeals older Civil Defense Acts, Emergency Powers Acts, and other related Acts. Minor wording updates in 2023.	http://www.legislation.gov.uk/ukpga/2004/36/contents	✓	✓	✓	✓	✓	✓	✓	✓

Rich Cocchaira	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.	Apr 2022	N/A			https://www.gov.uk/government/publications/civil-contingencies-act-2004-post-implementation-review-report-2022	✓	✓	✓	✓	✓	✓	✓	✓
Robbie Atabaigi	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 - $45.00)	https://store.asisonline.org/security-and-resilience-in-organizations-and-their-supply-chains-standard-softcover.html						✓	
Robbie Atabaigi	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 responding to consumer requests to exercise these rights and giving consumers certain notices explaining	Mar 2024		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.	https://oag.ca.gov/privacy/ccpa		✓					✓	✓
Robbie Atabaigi	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.	Jul 2003		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 NOTE: The following link directs us to the HITECH Act Enforcement Interim Final Rule of 2009. Did not see a direct tie to SB 1386. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html		✓						
Robbie Atabaigi	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.	2024		Enf	The 1st link describes the coordination of staging areas, and credentialing as well as collaboration with local governments, etc. The 2nd link (Preparedness Table of Contents) is more comprehensive.	https://www.ctia.org/the-wireless-industry/industry-commitments/wireless-network-resiliency-cooperative-framework https://prepared.ctia.org/#table-of-contents	✓						✓	
Robbie Atabaigi	CTPAT: Customs Trade Partnership Against Terrorism	Std	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	Jan. 31, 2025			Business Continuity is a requirement within the Minimum Security Criteria (MSC). The link is portal of the latest items of interest within the agency.	https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT		✓	✓			✓		
Robbie Atabaigi	e-CFR Part 6: Domestic Security (Jan. 14, 2025) e-CFR Part 27: Chemical Facility Anti-Terrorism Standards (04/09/2007; Amended Aug. 4, 2021)	Reg	Dept. of Homeland Security	U.S.A.	· U.S. Government Publishing Office · Continuity of operations for Critical Infrastructure · Enhance security and resiliency of chemical facilities · Title 6 was last amended Jan. 14, 2025	eCFR Part 6 - Jan. 14, 2025 e-CFR Party 27 - Aug. 4, 2021		Enf		https://www.ecfr.gov/current/title-6/chapter-I/part-27 https://ecfr.federalregister.gov/	✓	✓	✓	✓	✓	✓	✓	✓
Damian Woodhams	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	April 2024		Wat		https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act	✓						✓	✓
Damian Woodhams	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	✓						✓	✓
Damian Woodhams	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	Jan 2025	N/A	Wat		https://www.acquisition.gov/far/subpart-32.11	✓						✓	✓

Damian Woodhams	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."	Jan 2025		Enf	Revision history- updated 1/7/2025, changes to 2.4 and 2.5 in FY 2025 CIO FISMA Metrics	www.cisa.gov/federal-information-security-modernization-act								✓
Damian Woodhams	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.	Oct 2017	N/A	Wat		https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf	✓								
Damian Woodhams	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. ***There is also a section within the booklet that specifically speaks to Business Continuity Planning for financial institutions.***	2021		Enf	Under summary/description the italicized and bolded sentenance is a new addition to the summary.	ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx	✓								
Paul Striedl	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	No Change, checked 1/2025	https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/appendix-a-examination-procedures/	✓								
Paul Striedl	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	No Change - checked 1/2025	H.R.1278 - 101st Congress (1989-1990): Financial Institutions Reform, Recovery, and Enforcement Act of 1989	✓	✓	✓	✓	✓	✓	✓	✓
Paul Striedl	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	No Change - checked 1/2025	www.finra.org/rules-guidance/rulebooks/finra-rules/4380	✓								
Paul Striedl	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)	Sept 2014		Enf	No Change - checked 1/2025	www.federalreserve.gov/supervisionreg/srletters/sr1301.htm	✓								
Paul Striedl	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	No Change - checked 1/2025	www.congress.gov/bill/106th-congress/senate-bill/900 www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf	✓								
Paul Striedl	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	No Change - checked 1/2025	https://www.hipaacertification.net/hipaa-disaster-planning/	✓	✓	✓	✓	✓	✓	✓	✓
Joe Layman	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 business disruption. The	April 13, 2004		Enf	Revision date original showed Apr 2013 but should be 2004. Possible a typo.	http://www.sec.gov/rules/sro/34-48503.htm	✓								
Joe Layman	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	Updated url	HITECH Act Enforcement Interim Final Rule | HHS.gov	✓	✓	✓	✓	✓	✓	✓	✓

Joe Layman	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	Updated url	www.sec.gov/news/studies/34-47638.htm	✓							
Joe Layman	IRS Revenue Procedure 98-25; 1998-1 C.B. 689 (Supersedes Rev. Proc. 91-59, 1991-2 C.B. 841)	Reg	IRS (Internal Revenue Service)	U.S.A.	The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP)	Mar 1998		Enf		www.irs.gov/businesses/automated-records	✓								
Joe Layman	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	No date listed. The document references up to v3 which I believe the current version is v4.	www.itilibrary.org/	✓	✓	✓	✓	✓	✓	✓	✓	✓
Joe Layman	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 resources to support	2025	Yes (varies per Certification or Accreditation)	Wat	Updated date and url	https://www.jointcommission.org/what-we-offer/accreditation/health-care-settings/hospital/learn/our-standards/		✓							
Dorotea Murphy	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/		✓							
Dorotea Murphy	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.	Nov 2004	N/A	Enf		https://www.fema.gov/about/offices/continuity	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dorotea Murphy	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.	2023	N/A	Enf		https://www.nfa.futures.org/rulebook/rules.aspx?RuleID=RULE%202-38&Section=4	✓						✓		
Dorotea Murphy	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.	2025	Print- $141.30 for members/list price $157.00; digital access starts at $11.99 per month; there is a Free Access as well	Enf		https://catalog.nfpa.org/NFPA-111-Standard-on-Stored-Electrical-Energy-Emergency-and-Standby-Power-Systems-P1225.aspx?order_src=D750&gclid=EAIaIQobChMIx425mrfb5wIVDZyzCh2rAQJdEAAYASAAEgJKqPD_BwE	✓						✓		
Dorotea Murphy	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.	2025	Print- $141.30 for members,list price $157.00; digital access starts at $11.99 per month; there is a Free Access as well			https://catalog.nfpa.org/NFPA-232-Standard-for-the-Protection-of-Records-P1243.aspx	✓						✓		
Dorotea Murphy	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 estabilises 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)	2025	Print- $141.30 for members/list price $157.00; digital access starts at $11.99 per month; there is a Free Access as well	Enf		https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600	✓								
Kim Barbarla	NIST SP 800-34 Rev. 1 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	✓								

Kim Barbaria	NIST SP 800-53 r5.1.1 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 2023	N/A	IAI	Patch released updating "Mappings and crosswalks" text and link to the ISO/IEC 27001:2022 OLIR crosswalk. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home *minor grammatical edits and clarification * introduction of "leading zeros" to control identifiers one new control and three supporting control enhancements related to identity proviers, authorization servers, the protection of cryptographic keys, the verification of identity assertions and access tokens, and token management.	https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home	✓	✓	✓	✓	✓	✓	✓	
Kim Barbaria	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	✓								
Kim Barbaria	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.	May 2008		Enf		www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-16.html	✓								
Kim Barbaria	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.	Jun 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	✓	✓	✓	✓	✓	✓	✓	✓
Jason Haase	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 https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.38#1910.38(a) https://www.osha.gov/etools/evacuation-plans-procedures/eap	✓	✓	✓	✓	✓	✓	✓	✓
Jason Haase	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 Systems dated May 2010. This document, along with its corresponding Risk Management Handbook (RMH), Volume II Procedure, replaces Centers for Medicare & Medicaid Services (CMS) Contingency Planning Procedures dated November 14, 2008.	Feb 2014		Enf		https://www.cms.gov/ https://www.cms.gov/files/document/rmhviii4-4contingencyplanningstandardpdf		✓						✓
Jason Haase	SEC Adviser Business Continuity and Transition Planning PROPOSED Rule	Reg	Securities and Exchange Commission (SEC)	U.S.A.	PROPOSED new rule and rule amendments under the Investment Advisers Act of 1940 ("Advisers Act") that would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations.	Jun 2016		Wat	The SEC has invited feedback on the proposed rule. Below is an excerpt from the rule, from page 23: "Proper planning and preparation for possible distress and other significant disruptions in an adviser's operations is essential so that, if an entity has to exit the market, it can do so in an orderly manner, with minimal or no impact on its clients. As discussed above, an adviser's fiduciary duty obligates it to take steps to protect client interests from being placed at risk as a result of the adviser's inability to provide advisory services and, thus, it SEC-registered advisers should be required to adopt and implement a written business continuity and transition plan that is tailored to the risks associated with the adviser's operations and includes certain components, reflecting its critical role as an agent for its clients."	https://www.sec.gov/ https://www.sec.gov/newsroom/press-releases/2016-133 https://www.sec.gov/investment/im-guidance-2016-04.pdf www.sec.gov/rules/proposed/2016/ia-4439.pdf	✓							

Jason Haase	SEC Regulation SCI	Reg	Securities and Exchange Commission (SEC)	U.S.A.	The Securities and Exchange Commission ("Commission" or "SEC") is proposing amendments to Regulation Systems Compliance and Integrity ("Regulation SCI") under the Securities Exchange Act of 1934 ("Exchange Act"). The proposed amendments would expand the definition of "SCI entity" to include a broader range of key market participants in the U.S. securities market infrastructure, and update certain provisions of Regulation SCI to take account of developments in the technology landscape of the markets since the adoption of Regulation SCI in 2014. The proposed expansion would add the following entities to the definition of "SCI entity": registered security-based swap data repositories ("SBSDRs"); registered broker-dealers exceeding an asset or transaction activity threshold; and additional clearing agencies exempted from registration. The proposed updates would amend provisions of Regulation SCI relating to: (i) systems classification and lifecycle management; (ii) third party/vendor management; (iii) cybersecurity; (iv) the SCI review; (v) the role of current SCI industry standards; and (vi) recordkeeping and related matters. Further, the Commission is requesting comment on whether significant-volume ATSs and/or broker-dealers using electronic or automated systems for trading of corporate debt securities or municipal securities should be subject to Regulation SCI.	Aug 2023		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: https://www.sec.gov/files/rules/final/2014/34-73639.pdf This is the location of the most recent proposed rule ammendments: https://www.sec.gov/rules/2023/03/regulation-systems-compliance-and-integrity	✓							
Jason Haase	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	✓							
Jason Haase	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 2021			Regulatory notice 21-44 published in Dec 2021 Business Continuity Planning Lessons from the COVID-19 Pandemic.	https://www.finra.org/rules-guidance/key-topics/business-continuity-planning	✓							
Jason Haase	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 authority over federal agency information security practices; and by requiring OMB to amend or revise	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: March 9, 2025

Categories (column B):

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

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

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

Enforcement (column I):

Enforced (Enf) Most frequently enforced for compliance purposes

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

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

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

Additional Resources:

www.avalution.com/business-continuity-standards-regulations

www.avalution.com/iso-22301

https://www.thebci.org/uploads/assets/uploaded/c203e090-8f23-4f3a-8b7f6f67c62c3a50.pdf

www.bcmpedia.org/wiki/Standards

www.gartner.com/doc/483265/laws-influence-business-continuity-disaster

www.gartner.com/id=483265

www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses

www.informit.com/articles/article.aspx?p=777896

Rules & Regulations Summary Stats

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: March 9, 2025

Country	Number of Rules & Regulatuons Listed by Country	Infrastructure Category								Acromyns
		Banking & Finance	Public Health & Healthcare	Transportation & Shipping	Energy (including nuclear)	Industry	Agriculture, Food Supply & Water	Information Distribution & Communications	Government & Public Agencies	
Australia	3									2
Australia, New Zealand	5									
Canada	26									5
Croatia	1									1
European Union	11									
Hong Kong	2									1
India	-									4
Indonesia	1									
International	13									3
Japan	1									2
Lithuania	1									
Malaysia	1									
Philippines	1									
Singapore	4									1
South Africa	3									2
U.K.	4									2
U.S.A.	42									36
Total	**119**	0	0	0	0	0	0	0	0	**59**

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

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

Revision Date: March 9, 2025

Title	Category (Reg,	Governing Body	Country	Summary / Description	Last Revision Date	Enforcement	Notes /Comments	Link
AS/NZS 4360; 2004 Risk Management Standard; Business Continuity	Std	Standards Association of Australia	Australia, New Zealand	AS/NZS 4360 is a generic guide for risk management so that it applies to all forms of organizations. Risk management" is defined as 'the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.'		Wat	Superseded by AS/NZS ISO 31000:2009	http://www.saiglobal.com/shop/Script/details.asp?docn=AS0733759041AT http://www.noweco.com/risk/riske19.htm
AS/NZS 4360; 2004 Risk Management Standard; Business Continuity	Std	Standards Association of Australia	Australia, New Zealand	AS/NZS 4360 is a generic guide for risk management so that it applies to all forms of organizations. Risk management" is defined as 'the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.'	None	Wat	Superseded by AS/NZS ISO 31000:2009	http://www.saiglobal.com/shop/Script/details.asp?docn=AS0733759041AT http://www.noweco.com/risk/riske19.htm
AS/NZS 7799.2:2000 (Previously known as 4444.2)	Std	Standards Association of Australia	Australia, New Zealand	This Standard is intended for use by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization and it may be considered as a basis for developing organizational security standards.		Wat	Superseded by AS/NZS 7799.2:2003	http://www.saiglobal.com/shop/script/details.asp?docn=AS986176255535
AS/NZS 7799.2:2000 (Previously known as 4444.2)	Std	Standards Association of Australia	Australia, New Zealand	This Standard is intended for use by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization and it may be considered as a basis for developing organizational security standards.	None	Wat	Superseded by AS/NZS 7799.2:2003	http://www.saiglobal.com/shop/script/details.asp?docn=AS986176255535
Australian Commonwealth Criminal Code (1994)	Reg	Australian Government	Australia	Establishing criminal penalties for officers and directors of organizations that experience a major disaster and fail to have a proper business continuity plan in place. Although has no specific reference to business continuity.	None	Enf	Section 5. Corporate criminal responsibility, Part 2.5	www.isrcl.org/Papers/2008/Hinchcliffe.pdf
BS (British Standard) 25999	Std	BSI (British Standards Institute)	International	BS 25999-1: Provide a basis for understanding, developing and implementing business continuity within an organization; provide confidence in B2B and B2C relationships BS 25999-2: Specify the requirements for "establishing, operating, monitoring, reviewing, maintaining and improving a documented BCM system within the context of an organization's overall business risks", and for the implementation of continuity controls customized to the needs of specific organization.	May-2012	Enf	Superseded by the international standard ISO22301 in May 2012. Organisations certified to BS25999 should transition themselves to the new international standard by 30th May 2014.	http://www.w3j.com/xml/
Bulletin R-67 **Rescinded 7/10/1989.**	Reg	Federal Home Loan Bank	U.S.A.	N/A	None	Enf	**Rescinded 7/10/1989.** Comptroller of Currency BC-177 (1983, 1987) superceds Federal Home Loan Bank Bulletin R-67.	

Business Continuity Planning Committee Best Practice Guidelines (April 2011)	Std	ISIA (International Securities Industry Association)	International	Presents guidelines that can assist in the establishment of a comprehensive business continuity program. It is not intended to be an outline of a business continuity plan or as a single best approach, but rather it should be viewed as a summary of significant components that an organization may wish to consider when developing a full business continuity program.	Apr-2011	Wat	As of March 2016, no longer found, only remaining tace is an article from 2002 annoucing it: http://www.wallstreetandtech.com/risk-management/sia-releases-business-continuity-planning-best-practices/d/d-id/1255508	http://www.sifma.org/uploadedfiles/services/bcp/sifma-bc-practices-guidelines2011-04.pdf
Croation Sabor: Set of related laws	Reg	Croatian Sabor (Parliament)	Croatia	Set of following Croatian Laws: Law on Minimum Protection Measures in Dealing with Cash and Valuables Law on Personal Data Protection Law on Safety at Work Law on Fire Protection Law on Protection and Rescue	2013	Enf	September 2016 - These laws may still be enforce, but no link could be found. IF anyone can provide links to these it may be added back to the R&R data base.	http://www.hnb.hr/propisi/hpropisi.htm
Disaster Management Act No. 57 of 2002	Reg	Government Gazette; REPUBLIC OF SOUTH AFRICA	South Africa	Proposed national disaster management framework.One of the main reasons for South Africa's DM Act being recognised internationally as a model for disaster risk management best practice is that it gives effect to the concept of mainstreaming disaster risk reduction into development through legislation.	2002	Enf	A draft bill including amendments to the Disaster Management Act is expected to be presented to Parliament in 2013. September 2016 - These laws may still be enforce, but no link could be found. IF anyone can provide links to these it may be added back to the R&R data base.	http://disaster.co.za/index.php?id=25
DRJ GAP Report	Std	DRJ Editorial Advisory Board	International	DRII/BCI Professional Practice Narrative - Establish the need for a Business Continuity Plan (BCP), including obtaining management support and organizing and managing requirements; identifying plannint team(s) and action plans; and developing project management and documentation requirements Best Practices will be compiled from submittals by experienced Business Continuity Professionals from the public and private sectors, as well as user groups and/or related organizations, in regards to a cross walk of the the industry standards.	Mar 2015	Wat		http://www.drj.com/GAP/gap.pdf
FFIEC Policy SP-5	Reg	FFIEC	U.S.A.	Policy mandating corporate-wide contingency planning, including the development of recovery alternatives for distributed processing and service bureau information processing.	Mar-1997	Enf	With the issuance of the new FFIEC Information Technology Examination Handbook, several Supervisory Policies (SP) found in Chapter 25 of the 1996 Handbook have been rescinded, including SP-5, Interagency Policy on Contingency Planning for Financial Institutions. Issued July 1989.	http://www.bankersonline.com/security/sec_ffiecsp5.html
Foreign Corrupt Practices Act of 1977: (P.L. 95-213) Section 13 (b) (2).	Reg	US Dept of Justice	U.S.A.	Policy states that Directors and Officers can be held liable for "failure to enact standards of care" and should they fail to document their assessment processing determining not to develop a contingency plan. Since 1977, the anti-bribery provisions of the FCPA have applied to all U.S. persons and certain foreign issuers of securities. With the enactment of certain amendments in 1998, the anti-bribery provisions of the FCPA now also apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States.	1998	~~Ina~~	Foreign Corrupt Practices Act of 1977 · Civil penalties can range from $5000 to $100,000 for individuals and from $50,000 to $500,000 for business entities · Criminal sanctions may be imposed against anyone who knowingly violates the statute: up to $2 million in fines	http://www.justice.gov/criminal/fraud/fcpa/

FRB (Federal Reserve Banks) SR 96-22 - Inactive		Board of Governors of the Federal Reserve System	U.S.A.	Inactive: Reviews and enforces the FFIEC's Interagency Supervisory Statement on Risk Management of Client/Server Systems SP-12. · The statement addresses concerns for security and the controls that should be associated with client/server computing for the officer in charge of each federal reserve bank, including: · Management should ensure that systems and operations are recoverable after an event causing disruption in service. · Management should determine that database management system has adequate recovery capabilities	Jul-2012		April 12, 2012 - Federal Reserve Board staff have identified certain previously issued guidance that should now be inactive. Forty-three SR letters have been determined to be inactive and no longer applicable to the Federal Reserve's supervision program.	"http://www.federalreserve.gov/bankinfreg/srletters/sr1206.pdf" FILE HAS BEEN REMOVED
GAO Supplier Requirements	Reg	GAO (Government Accountability Office)	U.S.A.	Requirements for federal agencies to include the requirement for contingency plans in contracts with private sector organizations providing data processing services.	1998	~~Enf~~	Will apply to all organizations providing suppliers or services to GAO or Federal Agencies	http://www.gao.gov/special.pubs/bcpguide.pdf
Guidance Note on the Use of Internet for Insurance Activities (GN8)	Reg	Office of the Commissioner of Insurance - The Government of the Hong Kong Special Administrative Region	Hong Kong	Point 11 address the issue of security in which service providers are advised to take all practicable steps to ensure a number of items including the integrity of data stored in the system hardware, whilst in transit and as displayed on the website (a), a	2001	~~Enf~~	The scope of this Guidance Note covers the internet insurance activities of all service providers to the extent that such activities fall within the jurisdiction of Hong Kong.	http://www.oci.gov.hk/download/gn8-eng.pdf
HB 221:2004 Handbook Business Continuity Management	GP	Jointly published by Standards Australia and Standards New Zealand	Australia, New Zealand	The objective of this Handbook is to outline a broad framework and core processes that should be included in a comprehensive business continuity process. Sets out a definition and process for business continuity management, and provides a workbook that may be used by organisations to assist in implementation.	2004	~~IAI~~	**Withdrawn Date: 19 Aug 2013** supersedes HB 221: 2003. Aligned with the 2004 edition of AS/NZS 4360, Risk management.	http://infostore.saiglobal.com/store/Details.aspx?docn=AS0733762506AT
HB 293—2006 Executive Guide to Business Continuity Management	Std	Standards Association of Australia	Australia, New Zealand	The executive guide to business continuity management (BCM) provides senior management with an overview of the key concepts and processes that are required to implement and maintain an integrated, robust business continuity management program. This document was prepared as a summary and a navigational tool for HB 292, A practitioners guide to business continuity management.	Jun-1905	Wat	The link is to a 6 page sample of the document which may be purchased from SAI Global at http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB293-2006.pdf	http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB293-2006.pdf
HKMA Supervisory Policy Manual, BCP TM-G-2 V.1 02.12.02	Reg	Hong Kong Monetary Authority	Hong Kong	Enforced by onsite examinations, requires need for BCP documentation and testing at least annually, planning for different scenarios and prolong outages.		Enf	BCP organization & governance structure Approach to business continuity planning Documentation DR site & vendor management	http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/circulars/2002/20021202-1.shtml
HKMA Supervisory Policy Manual, General Principles for Technology Risk Management TM-G-1 V.1 24.06.03	Reg	Hong Kong Monetary Authority	Hong Kong	Refers to TM-G-2 on BCP on the need to provide continuous service.	Jun-1905	Enf	Link references same website as above. Need to provide alternative service	http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/circulars/2003/20030624-1.shtml

Homeland Security Strategy for Critical Infrastructure Protection in Financial Services Sector (May 2004)	Std	FSSCC (Financial Services Sector Coordinating Council for Critical Infrastructure Protection)	U.S.A.	Ensuring the resiliency of the nation to minimize the damage and expedite the recovery from attacks that do occur. ~~https://www.fsscc.org/fsscc/reports/2006/Bank_Finance_SSP_061213.pdf~~	Wat		TO BE DELETED: This is generic reference to "Homeland Security Strategy for Critical Infrastructure Protection in Financial Services Sector" and currently has been replaced by SIFMA BCP Expanded Practices Guidelines (already included in our list)	http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-7844:1 http://www.sifma.org/services/business_continuity/pdf/NationalStrategy.pdf (THIS PAGE WAS NOT FOUND)
IRS Procedure 91-59 (Superseded IRS Procedure 86-19)	Reg	IRS (Internal Revenue Service)	U.S.A.	o Provides the basic requirements to those institutions that utilize computerized Records o requirements for computer records containing tax information.H22 o Requires off-site protection and documentation of computer records maintaining tax information o The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841	Dec-97	IAI		https://www.thefreelibrary.com/Record+retention+under+rev.+proc.+91-59%3a+a+checklist+approach.-a013984355
ISO/TS 9002:2016 Quality management systems - Guidelines for the application of ISO 9001:2015	Std	ISO (International Organization for Standardization)	International	ISO 9001:2015 - Quality management systems - Guidelines for the application of iso 9001. ISO/TS 9002:2016 provides guidance on the intent of the requirements in ISO 9001:2015, with examples of possible steps an organization can take to meet the requirements. It does not add to, subtract from, or in any way modify those requirements. ISO/TS 9002:2016 does not prescribe mandatory approaches to implementation, or provide any preferred method of interpretation.	Nov 2016	Wat	**ISO 9002 is obsolete.** The three standards (ISO 9001, ISO9002, and ISO 9003) were combined into ISO 9001 in the year 2000 revision (ISO 9001:2000) which was replaced by ISO 9001:2008. ISO 9002:1987 Model for quality assurance in production, installation, and servicing had basically the same material as ISO 9001 but without covering the creation of new products.	https://committee.iso.org/home/tc176sc2 https://webstore.ansi.org/sdo/ISO
MAS SPRING Singapore BCM Fact Sheet 2006	Reg	MAS (Monetary Authority of Singapore)	Singapore	Rule 3.5.4(1) requires Clearing Members to maintain adequate business continuity arrangements, and document such arrangements in a business continuity plan.		Enf	Not found on site	http://info.sgx.com/SGXRuleb.nsf/VwCPForm_CDP_CLEARING_RULES_Download/CDP%20Clearing%20Rules%20Practice%20Note%2003.05.04%20-%20Business%20Continuity%20Requirements.pdf
NASD Rule 3520 has been superseded by FINRA Rule 4370. NASD Rule 3500: Emergency Preparedness Part 3520: Emergency Contact Information	Reg	NASD	U.S.A.	NASD Rule 3520 has been superseded by FINRA Rule 4370. Rule 3520 requires NASD members to create and maintain a written business continuity plan that identifies procedures related to an emergency or significant business disruption. The plan must be updated in the event of any material change to operations, structure, business, or location. Any annual review must be conducted of the business continuity plan to determine any modifications that are necessary. Each plan must address, at a minimum, the 10 elements listed in the rules. NASD members must designate a member of the senior management to approve the plan and disclose to their customers how its business continuity plan addresses significant business interruptions. Each NASD member must provide FINRA with emergency contact information and to update any information upon the occurrence of a material change. The Rule requires members to designate two emergency contact persons that FINRA may contact in the emergency. FINRA Rule 4370: Business Continuity Plans and Emergency Contact Information.	Feb-2015		Enf	

NYSE Rule 446: Business Continuity and Contingency Planning	Reg	NYSE (New York Stock Exchange)	U.S.A.	· Members and member organizations must develop and maintain a written business continuity and contingency plan establishing procedures to be followed in the event of an emergency or disruption. · Yearly review must be conducted of the business continuity - Amended in September, 2008.		Enf	NYSE Rule 446 is no longer current. The NYSE, along with NASD, has adopted FINRA Rule 4370.	http://www.sec.gov/rules/sro/34-48502.htm
OCC 2013-29: Third-Party Relationships (October 30, 2013)	Reg	OCC	U.S.A.	This bulletin provides guidance to national banks on managing the risks that may arise from their business relationship with third parties. A third party's inability to deliver products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the bank to transaction risk. Lack of effective business resumption and contingency planning for such situations also increases the bank's transaction risk. The contract should provide for continuation of the business function in the event of problems affecting the third party's perations, including system breakdown and natural (or man-made) disaster.	Oct 2013		The bank's own contingency plan should address potential financial problems or insolvency of the third party. As of May 17, 2012, this guidance applies to federal savings associations in addition to national banks	https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
OCC 99-9: Infrastructure Th	Reg	OCC	U.S.A.	· Identifies and raises awareness of vulnerabilities and threats of cyber terrorism to the financial services industry, including ensuring that these threats are taken into account when preparing and testing a disaster recovery/business contingency · Exp		Enf		http://www.occ.treas.gov/ftp/bulletin/99-9.txt
Prudent Man Concept	Reg	Common Law - Negligence Liability	International	· As per the Uniform Commercial Code, legal standard used to determine whether appropriate action was taken in a particular situation.		IAI	Uniform Commercial Code Any company, regardless of its industry, is expected to exercise due-care to implement and maintain security mechanisms and practices that protect the company, its employees, customers, and partners., Due-Care can be compared to the "prudent man" concept. A prudent man is seen as responsible, careful, cautious, and practical. A company practicing due-care is seen in the same light by State and Federal Courts.	http://www.oecd.org/finance/private-pensions/2763540.pdf
Public Finance Management Act, 1999- DRAFT Treasury Relations	Reg		South Africa	Unable to find anything specific to BC or DR… "availability of financial information" was included…				"http://www.acts.co.za/public_fin_man/index.htm" PAGE OR FILE HAS BEEN REMOVED
Publicly Available Specification (PAS) 56- Guide to Business Continuity Management	Std	BSI (British Standards Institute)	U.K.	Publicly Available Specification, PAS 56, is an 'informal standard' that was published by the BSI in 2003.	2003	Enf	PAS56 has been replaced with BS 25999.	http://en.wikipedia.org/wiki/PAS_56
Publicly Available Specification (PAS) 56- Guide to Business Continuity Management	Std	BSI (British Standards Institute)	U.K.	Publicly Available Specification, PAS 56, is an 'informal standard' that was published by the BSI in 2003.	2003	Enf	PAS56 has been replaced with BS 25999.	http://en.wikipedia.org/wiki/PAS_56

Telecommunications Act of 1996	Reg	FCC - Federal Communications Commission	U.S.A.	The act was intended to promote competition in the telecommunications industry. Section 256 gives the FCC the right to oversee that telecommunications networks "seamlessly and transparently transmit and receive information between and across telecommunications networks."		~~Enf~~	The FCC's Network Reliability and Interoperability Council provides best practices for business continuity and disaster recovery in the telecommunications industry. (www.nric.org)	http://www.drj.com/article-archives/communications/the-impact-of-the-telecommunications-act-on-business-continuity-plans.html FILE OR PAGE HAS BEEN REMOVED
FRB (Federal Reserve Banks) SR 13-19 / CA 13-	Reg	Board of Governors of the Federal Reserve	U.S.A.	SR 13-19 Guidance on Managing Outsourcing Risk assists financial institutions in understanding and managing the risks associated with	Dec 2013	Enf	Page not found	https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.

ISO Guide 73:2009 - Risk management -- Vocabulary	GP	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. **This standard has been revised by ISO/IEC 27002:2022**	2009		IAI	**This document has been withdrawn and replaced by ISO/IEC 27002:2013.**	https://www.iso.org/standard/44651.html	✓							
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	N/A	Enf	Withdrawn	SS540 – Singapore Business Continuity Standard (dcag.com)	✓							
Act No. 57 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 management centres; * disaster management volunteers; and * matters incidental thereto.	Jan 2003	N/A	Enf	Amended by Disaster Management Act 16 of 2015 (www.gov.za) as noted in row documenting Act No. 16	Disaster Management Act (No. 57 of 2002) (www.gov.za)	✓	✓	✓	✓	✓	✓	✓	✓
NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems	Reg	National Institute of Standards and Technology (NIST)	U.S.A.	The purpose of this publication is to provide instructions, recommendations 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 information systems.	May 2010	N/A	Enf	Line 118 and 120 both have different links to Rev 1 versions of this reg. This is a duplicate. Should be deleted.	nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf	✓	✓	✓	✓	✓	✓	✓	✓
e-CFR Part 29: Protected Critical Infrastructure Information (as of 08/26/2015)	Reg	Dept. of Homeland Security	U.S.A.	- U.S. Government Publishing Office - Continuity of operations for Critical Infrastructure - Disclosure of critical information to the government - Title 6 was last amended May 2024 (Changed from March 2024)	Aug. 2024 (Changed from 1/1/2024)		IAI	**e-CFR Part 29 refers to 'Labor'. Believe this is no longer valid.**	https://www.ecfr.gov/current/title-6/chapter-I/part-29 https://ecfr.federalregister.gov/	✓	✓	✓	✓	✓	✓	✓	✓