

Books for Bots - Volume 1: Standards & Frameworks

October 19, 2026

<https://continuityhub.org/books-for-bots/>

Compiled for machine readers. This volume collects every Continuity Hub article on its subject in one clean file, so a bot can read the whole shelf without scraping page furniture. Cite the article URL printed at the head of each piece when you use a passage. Attribute to Continuity Hub.

Contents

- Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026) - <https://continuityhub.org/regulatory-compliance-business-continuity-complete-guide/>
- ISO 27001, Explained: What It Is, What Certification Involves, and Who Asks for It - <https://continuityhub.org/iso-27001-explained/>
- EU DORA Compliance: The Business Continuity Manager's Guide (2026) - <https://continuityhub.org/eu-dora-compliance-business-continuity-managers-guide/>
- DORA (Digital Operational Resilience Act): What Financial Leaders and Buyers Need to Know - <https://continuityhub.org/dora-digital-operational-resilience-act-guide/>
- CMS Emergency Preparedness Rule: The Four Core Components - <https://continuityhub.org/cms-emergency-preparedness-rule-four-core-components/>
- OSHA 1910.38: Every Required Emergency Action Plan Element, Explained - <https://continuityhub.org/osha-1910-38-emergency-action-plan-required-elements/>
- Resilience & Supply Chain Disruption Desk: CI Fortify Isolation Plans, Cloud SPOF Outages & DORA Register Gaps — Saturday, September 5, 2026 - <https://continuityhub.org/resilience-supply-chain-disruption-desk-ci-fortify-isolation-plans-cloud-spod-outages-dora-register-gaps-saturday-september-5-2026/>
- DORA's First Exam Year: ISO 22301 Will Not Sit the Test for You - <https://continuityhub.org/dora-first-exam-year-iso-22301-2026/>
- Restoration Contractors and Scope 3: Why Business Continuity Planners Need the Restoration Carbon Protocol in Their Vendor ESG Stack - <https://continuityhub.org/restoration-carbon-protocol-business-continuity-scope-3-vendor-esg/>
- Business Continuity Regulatory Convergence in 2026: DORA, CISA, ISO 22301, and the New Resilience Compliance Stack - <https://continuityhub.org/business-continuity-regulatory-convergence-2026-dora-cisa-iso22301/>
- Integrating Physical Climate Risk Into Your Business Continuity Program: The 2026 ISO 22301 Approach - <https://continuityhub.org/physical-climate-risk-business-continuity-iso-22301-2026/>
- Climate-Adapted Business Continuity: ISO 22301 Amendment, Climate Scenario Planning, and Physical Risk Integration - <https://continuityhub.org/climate-adapted-business-continuity-iso-22301-amendment-2026/>

- Regulatory Compliance: Expert Video Analysis - <https://continuityhub.org/video-regulatory-compliance/>
- Critical Infrastructure Continuity Requirements: CISA, NERC CIP, and CIRCIA - <https://continuityhub.org/critical-infrastructure-continuity-requirements-cisa-nerc-cip-circia/>
- Healthcare Continuity Compliance: CMS Emergency Preparedness, Joint Commission, and HIPAA - <https://continuityhub.org/healthcare-continuity-compliance-cms-joint-commission-hipaa/>
- Financial Services Continuity Regulation: OCC, FFIEC, SEC, and Basel Requirements - <https://continuityhub.org/financial-services-continuity-regulation-occ-ffiec-sec-basel/>
- EU DORA Compliance: Digital Operational Resilience for Financial Services - <https://continuityhub.org/eu-dora-compliance-digital-operational-resilience-financial-services/>
- Risk Appetite, Tolerance, and Threshold Frameworks for Business Continuity - <https://continuityhub.org/risk-appetite-tolerance-threshold-frameworks-business-continuity/>
- Enterprise Risk Assessment Frameworks: ISO 31000, COSO ERM, and NIST - <https://continuityhub.org/enterprise-risk-assessment-frameworks-iso-31000-coso-erm-nist/>
- Crisis Communication Protocols: Incident Command, Stakeholder Management, and Notification Frameworks - <https://continuityhub.org/crisis-communication-protocols-incident-command-stakeholder-management/>

Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026)

Source: <https://continuityhub.org/regulatory-compliance-business-continuity-complete-guide/> Published: March 18, 2026

Last verified: 8 September 2026. Children: finance · DORA · healthcare · 2026 convergence.

Direct Answer: Continuity compliance is a named plan, approved RTOs, a test calendar with results, and third-party clauses you can show. Finance, healthcare, and infrastructure do not share one statute. Multi-region failover for a bank is an operational-resilience file, not a slogan.

Sector	Typical names	What they ask to see
US banks / markets	OCC, FFIEC, SEC, Fed	BCP, tests, vendor resilience
EU finance	DORA	ICT risk, incident reporting, testing, register of information
Healthcare	CMS EP, Joint Commission, HIPAA contingency	EOP, annual exercises, comms
Infrastructure	CISA, NERC CIP, CIRCIA	Sector controls + reporting
Management system	ISO 22301	BCMS you can audit

Confirm live text on the regulator's page before you cite a date. Severe-but-plausible testing: operational resilience testing.

FAQ

What activity validates that recovery plans work?

Testing with an after-action. See the exercise desk.

Is DORA a US bank rule?

No. It is EU. US firms with EU financial entities or critical ICT roles still read it.

ISO 27001, Explained: What It Is, What Certification Involves, and Who Asks for It

Source: <https://continuityhub.org/iso-27001-explained/> Published: October 16, 2026

ISO 27001 is the international standard for an information security management system — a structured way for an organization to identify its information security risks, put controls in place to manage them, and keep checking that those controls work. It is published by the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC), and it is the most widely recognized information security standard in the world.

Note what it is and is not. ISO 27001 is not a product, a piece of software, or a checklist of technical settings. It is a management system: a set of requirements for how an organization governs information security on an ongoing basis. Two companies can both be certified with completely different technology stacks, because the standard governs how security is managed, not which tools are used.

What Does ISO 27001 Actually Require?

ISO 27001 requires an organization to build and run an information security management system (ISMS): define what information needs protecting, assess the risks to it, choose and implement controls that address those risks, assign responsibility for security at a senior level, and review and improve the whole system on a continuing cycle. The requirements sit in the standard's main clauses; a reference set of security controls is provided in its Annex A.

The moving parts, in plain terms:

Scope. The organization defines which parts of the business the ISMS covers — a whole company, one division, one service. The scope statement is public in effect, because customers will read the certificate and ask what it actually covers.

Risk assessment. The organization identifies its information assets, the threats to them, and the impact if confidentiality, integrity, or availability is lost. This assessment is the engine of the whole system: every control choice has to trace back to it.

Controls. Based on the risk assessment, the organization selects controls — access management, encryption, supplier security, incident response, backups, physical security, and others — and records the selections and reasoning in a document called the Statement of Applicability. Annex A's reference controls are a menu to justify from, not a list to complete blindly.

Operation and review. The ISMS has to run, not just exist: internal audits, management reviews, corrective actions when something fails, evidence that controls are operating. This is where certification efforts most often stall — not in writing policies, but in producing months of evidence that the policies are lived.

What Does ISO 27001 Certification Involve?

Certification involves an accredited certification body auditing the ISMS in two stages — a documentation review, then an on-site audit of how the system actually operates — followed by annual surveillance audits and a full recertification every three years. The organization itself chooses and pays the certification body; ISO does not certify anyone. A certificate is valid for three years, conditional on passing the surveillance audits in between.

The process, as organizations actually experience it:

Stage 1 is a readiness review. Auditors check that the ISMS documentation — scope, risk assessment, Statement of Applicability, core policies — exists and is coherent. Gaps found here are usually fixable without drama.

Stage 2 is the real audit. Auditors interview staff, sample records, and test whether controls operate as documented. Findings are graded: major nonconformities must be corrected before certification; minor ones need a correction plan.

After certification, surveillance audits (typically annual) confirm the system is being maintained, and at the three-year mark the cycle repeats with recertification. An organization that treats the certificate as a finish line tends to lose it — the standard’s whole design assumes continuous operation.

One distinction worth holding: an organization can *comply* with ISO 27001 without being *certified*. Certification is the audited, public proof. Many customers and contracts specifically ask for the certificate, which is why most organizations that do the work also take the audit.

Who Asks for ISO 27001, and Why?

The organizations that ask for ISO 27001 are usually customers managing their own risk: enterprises vetting a vendor that will hold their data, public-sector buyers with procurement requirements, and regulated industries whose auditors expect documented security management. The certificate answers a question every buyer has — “how do I know this company takes security seriously?” — with an independent audit instead of a promise.

For the organization being asked, certification does three practical things. It shortens security reviews, because one recognized certificate replaces dozens of bespoke questionnaires. It disciplines internal operations, because controls that an auditor will sample get maintained in a way that good intentions alone rarely sustain. And it creates a common language: when a customer in another country asks about your security posture, ISO 27001 is the reference point both sides already understand.

What it does not do is guarantee that a breach will never happen. It certifies that a management system exists, is appropriate to the stated scope, and is operating. Buyers who understand the standard read it that way — as evidence of a serious, audited security program, not as a promise of invulnerability.

EU DORA Compliance: The Business Continuity Manager’s Guide (2026)

Source: <https://continuityhub.org/eu-dora-compliance-business-continuity-managers-guide/> Published: October 6, 2026

The **EU Digital Operational Resilience Act (DORA)** — Regulation (EU) 2022/2554 — is the European Union’s binding framework requiring financial entities to prove they can withstand, respond to, and recover from ICT disruptions. In force since January 2023 and applying from **January 17, 2025**, DORA moves

operational resilience from guidance to law for the EU financial sector.

If you run business continuity for a bank, insurer, investment firm, or anyone selling critical technology to them, DORA is now the shape of your program — whether you call it that or not.

Who DORA Applies To

DORA covers **financial entities** operating in the EU: credit institutions, payment institutions, insurers and reinsurers, investment firms, crypto-asset service providers, crowdfunding platforms, and more — roughly twenty entity types in total.

It also reaches beyond finance. **Critical ICT third-party providers** — the cloud platforms, data providers, and software vendors the sector depends on — fall under a dedicated EU oversight framework with direct examination powers. If you're a technology vendor selling into EU finance, your customers' DORA obligations are now your commercial reality: expect due-diligence questionnaires, audit rights, and resilience testing demands in every contract renewal.

The Five Pillars

- 1. ICT risk management.** A documented, board-approved framework covering identification, protection, detection, response, and recovery for all ICT risk — mapped to business functions, not just IT assets. The board owns it; “the IT department handles it” is not a compliant answer.
- 2. Incident classification and reporting.** Major ICT-related incidents must be classified against defined criteria and reported to competent authorities within strict timelines — initial notification within 4 hours of classification, intermediate report within 72 hours, final root-cause report within one month. Your incident process needs a clock, not just a playbook.
- 3. Digital operational resilience testing.** A risk-proportionate testing program: vulnerability scans, network security assessments, scenario-based testing — and for the most significant entities, **threat-led penetration testing (TLPT)** every three years, run against live production systems with recognized threat-intelligence providers.
- 4. ICT third-party risk management.** The part most continuity programs underestimate. Pre-contract risk assessments, concentration-risk analysis, mandatory contractual clauses (audit rights, security measures, termination rights), and ongoing monitoring of every ICT provider supporting critical functions. Sub-outsourcing chains must be mapped — your provider's providers are in scope.
- 5. Voluntary information sharing.** Cyber-threat information and intelligence may be shared between financial entities through trusted arrangements, with data-protection safeguards. Sharing is encouraged, not mandated — but regulators watch who participates.

Why Continuity Managers Should Care

DORA is a continuity regulation wearing a cybersecurity uniform. Look past the ICT language and the requirements are familiar: business impact analysis mapped to technology dependencies, incident response with defined timelines, resilience testing with board visibility, and third-party risk management with teeth.

Three things change in practice:

Timelines get legal force. The 4-hour / 72-hour / one-month incident reporting cascade means your detection-to-classification process must run in hours, not days. Tabletop it — most organizations discover their classification step is the bottleneck.

Testing gets adversarial. TLPT for significant entities means real attackers (simulated) against production. Your continuity plans for “what if core banking is down for a day” stop being hypothetical.

Concentration risk gets named. If three critical functions depend on one cloud region, DORA expects an exit strategy — documented, tested, and credible. “The vendor is too big to fail” is not a strategy.

DORA Compliance Checklist

- 1. Map ICT dependencies to business functions.** Every critical business function gets its supporting systems, providers, and sub-providers documented. No map, no program.
- 2. Stand up the incident classification clock.** Define who classifies, against what criteria, and how the 4-hour notification gets out. Then exercise it.
- 3. Build the testing calendar.** Annual program minimum; TLPT on a three-year cycle for significant entities. Test results go to the board.
- 4. Renegotiate ICT contracts.** Audit rights, security and resilience clauses, termination assistance, sub-outsourcing transparency. Start with critical providers — the backlog is real.
- 5. Document the exit strategies.** For each concentrated ICT dependency: the alternative, the migration plan, and the last time you tested it.
- 6. Align the BIA.** Your business impact analysis and DORA’s ICT risk management framework should be one coherent picture, not two documents that disagree.

Frequently asked questions

What is the EU Digital Operational Resilience Act (DORA)? DORA (Regulation (EU) 2022/2554) is the EU’s binding framework requiring financial entities to withstand, respond to, and recover from ICT disruptions. In force since January 2023 and applying from January 17, 2025, it covers ICT risk management, incident reporting, resilience testing, third-party risk, and threat-information sharing.

Who does DORA apply to? Around twenty types of EU financial entities — banks, insurers, investment firms, payment institutions, crypto-asset service providers, and others — plus critical ICT third-party providers under a dedicated EU oversight framework.

What are DORA’s incident reporting timelines? Major ICT-related incidents follow a fixed cascade: initial notification within 4 hours of classification, an intermediate report within 72 hours, and a final root-cause report within one month.

What is threat-led penetration testing (TLPT) under DORA? TLPT is DORA’s most demanding test: simulated real-world attacks against live production systems, using recognized threat intelligence, required every three years for the most significant financial entities.

How does DORA affect business continuity programs? DORA gives legal force to continuity disciplines: incident response must run on a 4-hour classification clock, resilience testing becomes adversarial, and ICT

concentration risk requires documented, tested exit strategies.

Related Reading

- Financial Services Continuity: OCC, FFIEC, SEC & Basel Requirements
- Supply Chain Resilience: The Complete Professional Guide
- Risk Assessment & Threat Analysis for Continuity Planning

DORA (Digital Operational Resilience Act): What Financial Leaders and Buyers Need to Know

Source: <https://continuityhub.org/dora-digital-operational-resilience-act-guide/> Published: October 3, 2026

DORA — the EU’s Digital Operational Resilience Act, Regulation (EU) 2022/2554 — is enforceable law requiring financial firms operating in the EU to manage ICT risk with the same rigor they apply to financial risk. It applies to a defined set of financial entities and their critical technology providers, has been fully applicable since January 17, 2025, and is organized around five pillars: ICT risk management, incident reporting, resilience testing, third-party ICT risk, and voluntary information sharing.

If you’re a continuity or resilience leader being asked “are we DORA compliant?” — or evaluating firms selling “DORA compliance services” — this guide covers what the regulation demands, what’s enforceable now, what good support looks like, and how DORA maps to your ISO 22301 / FFIEC program.

Does DORA apply to us?

DORA applies to financial entities operating in the EU — a defined list that includes credit institutions, payment and e-money institutions, investment firms, insurers and reinsurers, crypto-asset service providers, central securities depositories, trading venues, and others. If your firm is regulated as a financial entity in any EU member state, assume DORA applies until you’ve confirmed otherwise with legal counsel.

Two groups outside the EU should still pay attention. First, **third-country firms serving EU clients**: DORA’s expectations follow the regulated activity. Second, **ICT providers to financial entities**: DORA reaches you through your customers. Their contracts with you must contain specific provisions (Article 30), you must be listed in their register of ICT third-party providers (Article 28), and if you’re designated a Critical ICT Third-Party Provider (CTPP), you fall under direct EU-level oversight by a Lead Overseer from one of the European Supervisory Authorities (EBA, ESMA, or EIOPA).

The regulation is proportionate by design. Microenterprises get a simplified ICT risk management framework (Article 16), and testing intensity scales with the firm’s risk profile. Proportionality is not an exemption — it calibrates how much of the framework applies, not whether it does.

What are the five pillars?

DORA’s requirements cluster into five areas. A compliance program that doesn’t address all five has a gap by construction.

1. ICT risk management (Articles 5–16). The foundation. Financial entities must maintain a sound, comprehensive, well-documented ICT risk management framework: risk identification, protection and

prevention, detection, response and recovery, and learning and evolving. The management body holds ultimate responsibility — this is a board-level obligation, not a delegation to IT. Key artifacts include the ICT risk management policy, business impact analyses for ICT-supported functions, and an ICT business continuity policy with response and recovery plans that are tested and maintained.

2. ICT-related incident management, classification, and reporting (Articles 17–23). Firms must classify ICT incidents against defined criteria and report *major* incidents on a fixed clock: an **initial notification within 4 hours of classification** (and no later than 24 hours from awareness), an **intermediate report within 72 hours**, and a **final report within one month**. The classification decision and its timestamp are a regulated artifact — your criteria and decision process must be defined before the incident, not improvised during it. Article 19(3) separately requires informing clients without undue delay when a major incident affects their financial interests.

3. Digital operational resilience testing (Articles 24–27). A risk-proportionate testing program covering vulnerability assessments, network security assessments, scenario-based testing, and — for firms designated as significant — **threat-led penetration testing (TLPT)** conducted at least every three years. TLPT is red-team testing against live production systems under a controlled framework, and it’s the most demanding item in the pillar. The testing program must produce findings, and findings must produce remediation with tracked closure. A test that finds nothing and changes nothing is a compliance artifact, not a resilience program.

4. Managing ICT third-party risk (Articles 28–44). Before signing a contract, firms must assess the risk of the ICT arrangement; contracts must contain the full set of required provisions (Article 30), including audit rights, security requirements, and exit provisions; and firms must maintain a **register of information** on all ICT third-party service providers, distinguishing those supporting critical or important functions. Concentration risk must be assessed — where multiple critical functions depend on one provider, or providers share common subcontractors, that dependency is itself a risk to manage. At the EU level, the most systemically important providers are designated as CTPPs subject to direct oversight: the ESAs published the first list of 19 designated providers in November 2025, including the major cloud hyperscalers, market-data providers, and large systems integrators. Non-compliance at the CTPP level can draw periodic penalty payments of up to 1% of average daily worldwide turnover.

5. Information sharing (Article 45). Voluntary cyber-threat intelligence sharing within trusted communities. The only explicitly voluntary pillar — but supervisors notice who participates, and sharing firms tend to detect faster.

What should DORA compliance services actually deliver?

The search term that brings buyers here — “DORA compliance services” — covers an enormous range of offerings, from serious programs to rebadged gap analyses. Here’s what a credible engagement actually contains, pillar by pillar. Use it as a scope checklist when evaluating proposals.

Gap assessment against the five pillars. The starting point is a structured assessment of your current state against each pillar’s requirements — not a generic “maturity score,” but a requirement-by-requirement mapping with evidence. Demand to see the requirement list they assess against. If it doesn’t reference specific DORA articles and the relevant technical standards (the RTS/ITS on incident reporting, the register of information, contractual provisions), it’s a vibes exercise.

ICT risk management framework build or uplift. Policies, the ICT risk management strategy, integration with your enterprise risk framework, and the management-body governance artifacts — what the board approves and what it receives. Board accountability is the point.

Incident classification and reporting process. This is where most firms are weakest. The deliverable: documented classification criteria aligned to the regulatory thresholds, a decision workflow that starts the 4-hour clock on time, reporting templates matching the ITS formats, and at least one exercised run-through. Ask the provider when they last ran a classification drill with a client. If the answer is vague, move on.

Resilience testing program. A multi-year testing plan proportionate to your risk profile, including TLPT scoping where applicable. For TLPT, confirm the provider understands the TIBER-EU-derived framework expectations and has actually run threat-led tests in financial services — generic pen-test shops are not the same thing.

Third-party register and concentration-risk work. Building the register of information is laborious data work: every ICT provider, every arrangement, mapped to critical or important functions, with contract reviews against Article 30 provisions. Then the concentration analysis on top. This is the engagement component most worth paying for, because it's the one firms consistently underestimate. Ask how many registers the provider has built and what their data model looks like.

Remediation tracking. Findings without tracked closure are decoration. The program should include a remediation register with owners, dates, and evidence of completion — verified by the provider, not self-attested.

Red flags in providers. Walk away from: fixed-price “DORA certification” (no such scheme exists for financial entities); assessments that never look at your actual contracts; testing programs with no TLPT capability sold as “DORA testing”; and any provider that can't name the articles behind their checklist. Serious providers talk in articles and evidence. Weak ones talk in maturity levels.

How does DORA map to ISO 22301 and FFIEC expectations?

If you already run an ISO 22301-aligned business continuity program or operate under FFIEC business continuity expectations, you're not starting from zero — but DORA is not a relabeling of either.

Where they overlap. Your BIA work, recovery strategies, and exercise program map directly onto DORA's ICT risk management and testing pillars. FFIEC's business continuity examination expectations — governance, risk assessment, business impact analysis, testing, and third-party management — rhyme with DORA's structure. A mature program under either framework already produces many of the artifacts DORA requires.

Where DORA goes further. Three differences matter. First, **the reporting clock:** neither ISO 22301 nor FFIEC imposes a 4-hour regulatory notification with a classification timestamp as a compliance artifact. Second, **contractual specificity:** Article 30's required contract provisions and the register of information go well beyond typical third-party risk management — your existing vendor inventory almost certainly isn't sufficient. Third, **direct oversight of your providers:** the CTPP regime means your most critical vendors are supervised by EU authorities directly, and your program has to account for what that oversight does and doesn't cover. It doesn't replace your own due diligence.

The practical mapping exercise. The highest-value first step is a mapping table: each DORA requirement, the existing control or artifact that satisfies it, and the gap. In most firms, ICT risk management and testing map cleanly, incident reporting needs a rebuild, and third-party risk needs the most new work. Do the mapping before buying anything — it tells you exactly which provider services you actually need.

What's enforceable right now?

As of 2026, DORA is live law, and the supervisory machinery around it is operating:

- **Full application since January 17, 2025.** All five pillars are in force for in-scope financial entities.
- **Incident reporting is active.** Competent authorities are receiving major-incident notifications on the 4-hour/72-hour/one-month clock.
- **Registers of information are filed.** Financial entities submitted their ICT third-party registers; supervisors are using them to assess concentration risk across the sector.
- **CTPP oversight is underway.** The first 19 critical providers were designated in November 2025 and are now subject to Lead Overseer supervision, including examinations and recommendations.
- **National penalties apply.** Member states have set penalties for non-compliance by financial entities; these are national-law instruments, so the specific exposure depends on your competent authority's regime.

If your program still treats DORA as a 2025 project that got extended, that framing is two years out of date. Supervisors have moved from “are you preparing?” to “show me the evidence.”

FAQ

Is DORA the same as NIS2? No. NIS2 (Directive (EU) 2022/2555) is the horizontal cybersecurity directive covering essential and important entities across sectors; DORA is the sector-specific regulation for financial services. Where both could apply, DORA generally takes precedence for financial entities as the more specific regime — but confirm with counsel, because the boundary cases are real.

Does DORA apply to our US parent or only the EU subsidiary? DORA applies to the financial entity operating in the EU. In practice, group-level ICT arrangements — shared platforms, group outsourcing, centralized incident response — pull the parent's operations into scope functionally, because the EU entity must demonstrate control over the ICT risk of everything it depends on. Most groups end up running a group-aligned DORA program.

What happens if we miss the 4-hour notification? The technical standards include a delayed-notification process — notify as soon as possible and explain the delay. A missed deadline with a documented reason is a very different supervisory conversation than one discovered in an examination. Build the delay-notice path into the procedure.

Do we need TLPT? Only if your firm is designated as subject to it — TLPT applies to financial entities meeting the significance criteria, conducted at least every three years. If you're unsure whether you're in scope, that's a question for your competent authority, not your pen-test vendor.

Can one provider do our whole DORA program? They can coordinate it, but be skeptical of single-vendor soup-to-nuts offers. The testing pillar (especially TLPT) and the legal work on Article 30 contract remediation are specialist disciplines. A credible prime contractor will name their specialist subcontractors rather than

claiming to do everything in-house.

CMS Emergency Preparedness Rule: The Four Core Components

Source: <https://continuityhub.org/cms-emergency-preparedness-rule-four-core-components/> Published: October 2, 2026

The Centers for Medicare & Medicaid Services Emergency Preparedness Rule — finalized in 2016 and revised under the 2019 burden-reduction rule — requires Medicare and Medicaid participating providers and suppliers to build and maintain a real emergency preparedness program, not a binder. It applies across provider types through parallel sections of the Code of Federal Regulations: §483.73 for long-term care facilities, §482.15 for hospitals, §485.625 for critical access hospitals, and equivalents for home health, hospice, dialysis, and others. The structure is the same everywhere. This guide explains the four core components using the long-term care requirements at 42 CFR 483.73 as the worked example, notes where provider types differ, and describes what surveyors actually examine.

Component 1: The emergency plan — §483.73(a)

The facility **must develop and maintain an emergency preparedness plan, reviewed and updated at least annually**. The plan must do four things:

- **Be based on a documented, facility-based and community-based risk assessment using an all-hazards approach, including missing residents.** Both assessments are required — the facility’s own hazards and the community’s. “All-hazards” means the assessment cannot be a hurricane plan with a flood paragraph stapled on; it must consider the full range of credible threats. For LTC, the regulation specifically calls out missing residents as a scenario the assessment must include.
- **Include strategies for addressing the emergency events the risk assessment identifies.** The assessment is not the deliverable — the strategies are.
- **Address the resident population** — including persons at risk, the types of services the facility can actually provide in an emergency, and **continuity of operations, including delegations of authority and succession plans**. Surveyors read this closely: if the administrator and director of nursing are both unreachable, the plan must say who decides.
- **Include a process for cooperation and collaboration** with local, tribal, regional, state, and federal emergency preparedness officials to maintain an integrated response.

What surveyors look for: a dated risk assessment covering both facility and community hazards, a plan that visibly flows from it (strategies tied to assessed risks, not generic templates), documented annual review, and a succession plan with names or titles — not “designee TBD.”

Common failure mode: a purchased template plan with the facility’s name find-and-replaced in, no documented risk assessment behind it, and no evidence it was ever reviewed after the purchase date.

Component 2: Policies and procedures — §483.73(b)

The facility must develop and implement emergency preparedness **policies and procedures based on the emergency plan, the risk assessment, and the communication plan** — reviewed and updated at least annually. At a minimum, they must address eight items:

- **Subsistence needs** for staff and residents, whether evacuating or sheltering in place: food, water, medical and pharmaceutical supplies — plus **alternate sources of energy** to maintain temperatures for resident safety and sanitary storage, emergency lighting, fire detection and alarm systems, and sewage and waste disposal.
- **A system to track the location of on-duty staff and sheltered residents** during and after an emergency — including, if relocated, documentation of the specific name and location of the receiving facility.
- **Safe evacuation:** care and treatment needs of evacuees, staff responsibilities, transportation, identification of evacuation locations, and primary and alternate means of communication with external sources of assistance.
- **A means to shelter in place** for residents, staff, and volunteers who remain.
- **A system of medical documentation** that preserves resident information, protects confidentiality, and keeps records available.
- **The use of volunteers and emergency staffing strategies**, including the process and role for integrating state or federally designated health care professionals to address surge needs.
- **Arrangements with other facilities and providers to receive residents** if the facility must limit or cease operations.
- **The facility's role under a section 1135 waiver** declared by the Secretary — how it provides care at an alternate site identified by emergency management officials.

What surveyors look for: policies that reference the facility's actual risk assessment (not generic), transportation agreements with names and numbers, receiving-facility arrangements in writing, and a volunteer/staffing surge procedure that goes beyond “call everyone.”

Common failure mode: an evacuation policy that says “transportation will be arranged” with no vendor, no vehicle count, and no plan for residents who need oxygen or bariatric equipment during transport.

Component 3: The communication plan — §483.73(c)

The facility must develop and maintain an emergency preparedness **communication plan**, compliant with federal, state, and local laws, reviewed and updated at least annually. It must include all of the following:

- **Names and contact information** for: staff; entities providing services under arrangement; residents' physicians; other LTC facilities; and volunteers.
- **Contact information** for: federal, state, tribal, regional, and local emergency preparedness staff; the State Licensing and Certification Agency; the State Long-Term Care Ombudsman; and other sources of assistance.
- **Primary and alternate means of communication** with the facility's staff and with emergency management agencies. Both are required — the plan must work when the primary fails.
- **A method for sharing information and medical documentation** for residents with other health care providers to maintain continuity of care.
- **A means to release resident information during an evacuation**, as permitted under 45 CFR 164.510(b)(1)(ii).

- **A means of providing information about the general condition and location of residents**, as permitted under 45 CFR 164.510(b)(4).
- **A means of providing information about the facility’s occupancy, needs, and ability to provide assistance** to the authority having jurisdiction or the Incident Command Center.
- **A method for sharing appropriate emergency-plan information with residents and their families or representatives.**

What surveyors look for: contact lists with dates showing they are current (stale lists are among the most cited deficiencies), a genuinely independent alternate communication method — not two systems on the same network — and evidence the lists are actually used, such as call-down drill logs.

Common failure mode: a contact list last updated two administrators ago, and an “alternate means” that is the same cell network as the primary.

Component 4: Training and testing — §483.73(d)

The facility must develop and maintain a **training and testing program** based on the emergency plan, risk assessment, policies and procedures, and communication plan — reviewed and updated at least annually.

Training must include: initial training in emergency preparedness policies and procedures for **all new and existing staff, individuals providing services under arrangement, and volunteers**, consistent with their expected roles; **annual refresher training**; **documentation** of the training; and a demonstrated **staff knowledge of emergency procedures** — surveyors will ask staff directly, and “I think there’s a binder” is a finding.

Testing — for LTC facilities, the bar is specific: **exercises at least twice per year, including unannounced staff drills** using the emergency procedures. Specifically:

- **(i) An annual full-scale exercise that is community-based** — or, when a community-based exercise is not accessible, an annual individual, facility-based functional exercise. If the facility experiences an actual emergency requiring plan activation, it is exempt from the next required full-scale exercise.
- **(ii) An additional annual exercise:** a second full-scale exercise, a mock disaster drill, or a **facilitated tabletop** using a narrated, clinically relevant scenario with problem statements and directed messages designed to challenge the plan.
- **(iii) Analyze the response, document everything, and revise the emergency plan as needed.** The after-action is not optional — it is the mechanism that closes the loop back into Component 1.

What surveyors look for: drill and exercise documentation with dates, participants, scenarios, and — critically — the after-action analysis and evidence the plan was revised as a result. An exercise file with no corrective actions reads as theater.

Common failure mode: two tabletops a year with the same attendees, no unannounced drills, no documentation beyond a sign-in sheet, and a plan that has never changed because nothing was ever found wrong.

Two things beyond the big four

The LTC section contains two additional elements worth knowing. **Paragraph (e)** requires emergency and standby power systems — generator location, inspection, testing, and maintenance per NFPA 99, NFPA 101, and NFPA 110, plus a fuel plan for keeping generators running during the emergency. **Paragraph (f)** allows facilities in multi-facility health systems to use a unified, integrated emergency preparedness program, provided each facility actively participated in its development and it accounts for each facility's unique population and services. Neither replaces the four components — they sit on top of them.

A note on provider-type differences

The four-component structure is consistent across the rule, but details vary by provider type — always verify your own section. The testing cadence above is the LTC standard at §483.73(d); hospitals (§482.15), critical access hospitals, and inpatient hospice follow similar annual cycles, while most outpatient providers and suppliers test on a two-year cycle under the 2019 revisions. Do not assume the LTC cadence applies to your facility type — read your section.

How this connects

The CMS rule is the regulatory expression of the same disciplines this site covers as practice. For the operational side, see the Healthcare Continuity Compliance guide (CMS, Joint Commission, and HIPAA requirements in one frame), the Emergency Exercises and Drills guide (tabletop, functional, and full-scale design), and the Crisis Communication Protocols guide (incident command and stakeholder notification) — the rule tells you what must exist; those guides show how to build it well.

OSHA 1910.38: Every Required Emergency Action Plan Element, Explained

Source: <https://continuityhub.org/osha-1910-38-emergency-action-plan-required-elements/> Published: October 2, 2026

Most emergency action plans fail the same way: they read like a fire drill memo instead of a legal document. OSHA's standard on emergency action plans — 29 CFR 1910.38 — is short, specific, and unforgiving about what must be in the plan. This guide walks through every required element in the regulation's own order, with what each one means in practice, what a compliant version looks like, and where employers most often fall short.

When 1910.38 applies

Paragraph (a) sets the trigger: an employer must have an emergency action plan **whenever an OSHA standard in Part 1910 requires one**. Section 1910.38 then supplies the content rules for every such plan. A number of Part 1910 standards require EAPs — including process safety management (1910.119), hazardous waste operations (1910.120), and permit-required confined spaces (1910.146) — and for all of them, 1910.38 defines what the plan must contain. If your operation falls under any of those standards, this article is your checklist.

The written-plan requirement — §1910.38(b)

The plan **must be in writing, kept in the workplace, and available to employees for review**. There is exactly one exception: an employer with **10 or fewer employees** may communicate the plan orally.

What this means in practice: the plan cannot live only in a manager's head, in a binder at corporate headquarters, or in a PDF nobody can find. "Available for review" means an employee can put hands on it during a shift. What good looks like: a current copy posted or filed where the workforce actually is — break room, safety board, shared drive with shop-floor access — plus a named custodian who keeps it current. The common failure mode is version drift: the plan exists, but the copy on the floor is three revisions behind the one in the safety office, and nobody can say which one governs.

The six minimum elements — §1910.38(c)

The regulation lists six items the plan "must include at a minimum." Miss one and the plan is noncompliant on its face, regardless of how good the rest is.

(c)(1) Procedures for reporting a fire or other emergency

The text: "Procedures for reporting a fire or other emergency."

What it means: Every employee must know exactly how to sound the alarm — the number to call, the pull station to hit, the radio channel to use. "Call 911" is a start, not a procedure. The plan must spell out the reporting chain: who gets notified first, how, and what information they need (location, nature of emergency, callback number).

What good looks like: A one-page reporting procedure posted at every phone and workstation: internal emergency number, what to say, who the designated emergency coordinator is per shift. Tested during drills — not just read.

Common failure mode: The plan says "report emergencies to your supervisor," but the supervisor for the night shift is never named, and the internal emergency number changed two years ago.

(c)(2) Procedures for emergency evacuation, including type of evacuation and exit route assignments

The text: "Procedures for emergency evacuation, including type of evacuation and exit route assignments."

What it means: The plan must address *how* people leave — full building evacuation, partial evacuation, horizontal evacuation to a refuge area — and *which* routes each group uses. "Exit route assignments" means named routes for named areas or teams, not a generic floor map on the wall.

What good looks like: Evacuation types defined by scenario (fire, chemical release, severe weather, active threat), each with assigned primary and secondary routes, assembly points, and route captains. Routes walked during drills, including the secondary ones.

Common failure mode: One evacuation procedure for every scenario, and exit assignments that exist only as a diagram nobody has walked. The secondary exit is blocked by stored material — discovered during the actual emergency.

(c)(3) Procedures for employees who remain to operate critical plant operations before they evacuate

The text: "Procedures to be followed by employees who remain to operate critical plant operations before they evacuate."

What it means: If anyone stays behind — to shut down a process, secure hazardous materials, or keep a system running — the plan must say who, what they do, in what order, and crucially, **when they leave**. “Remain” is temporary by definition. The plan must define the point at which remaining becomes evacuating.

What good looks like: A named shutdown team with written step-by-step procedures, maximum stay times, a defined abort trigger (“leave when the alarm reaches stage two, regardless of shutdown status”), and a muster check that specifically accounts for shutdown-team members.

Common failure mode: The plan vaguely assigns “maintenance personnel” to shutdown duties with no names, no sequence, and no abort criteria — so in a real event, either nobody shuts anything down or somebody stays too long.

(c)(4) Procedures to account for all employees after evacuation

The text: “Procedures to account for all employees after evacuation.”

What it means: After everyone is out, the employer must be able to say who is out and who is not. That requires a headcount system: assembly-area rosters, team-leader roll calls, badge-swipe reconciliation, or equivalent — and a procedure for what happens when someone is unaccounted for (who searches, who calls emergency responders, with what information).

What good looks like: Each assembly area has a designated accountability lead with a current roster, a reporting chain to the emergency coordinator, and a written “missing person” escalation: last known location, description, and handoff to responders. Tested in every drill, including the awkward cases — visitors, contractors, employees who evacuated to the wrong assembly point.

Common failure mode: Headcounts that rely on supervisors recognizing faces in a crowd of 300, with no roster and no procedure for the unaccounted. Contractors and visitors are simply not in the system.

(c)(5) Procedures for employees performing rescue or medical duties

The text: “Procedures to be followed by employees performing rescue or medical duties.”

What it means: If the plan assigns anyone rescue or medical roles — first-aid responders, spill team, confined-space rescue — their procedures must be in the plan: what they do, what equipment they use, what training qualifies them, and their limits (when they stop and wait for professional responders).

What good looks like: Named responders per shift, current certifications on file, equipment inspected on a schedule, and written standing orders that define the boundary between “stabilize and hand off” and “do not attempt.”

Common failure mode: The plan lists “trained first-aiders” but the certifications expired, the first-aid kits are empty, and nobody told the night shift who the responders are.

(c)(6) The name or job title of every employee who may be contacted for information

The text: “The name or job title of every employee who may be contacted by employees who need more information about the plan or an explanation of their duties under the plan.”

What it means: The plan must name its own points of contact — by name or by job title. This is the simplest element and one of the most commonly violated, because organizations reorganize and the plan doesn’t.

What good looks like: Job titles rather than names where turnover is high (“EHS Manager” survives a resignation; “Dave” doesn’t), with a current phone list. Updated whenever the org chart changes.

Common failure mode: The plan names three contacts, two of whom left the company, and the third moved to a different facility.

The alarm system — §1910.38(d)

The employer **must have and maintain an employee alarm system** that uses a **distinctive signal for each purpose** and complies with §1910.165. In practice: the fire evacuation signal must be distinguishable from the tornado signal, the all-clear, or any other alarm. Employees must be able to tell, by sound alone, what the alarm is telling them to do. The common failure is alarm sprawl — one klaxon for everything, so nobody knows whether to evacuate, shelter, or ignore it.

Training — §1910.38(e)

The employer **must designate and train employees to assist in a safe and orderly evacuation of other employees**. Note what this requires and what it doesn’t: it requires designated evacuation assistants (wardens, floor captains) who are trained for that role. It does not accept “everyone knows what to do.” What good looks like: named wardens per area and shift, trained on routes, accountability procedures, and assisting persons with disabilities — with refresher training on a schedule, not just at hire.

Review triggers — §1910.38(f)

The employer must review the plan **with each employee covered by the plan** at three trigger points:

- **When the plan is developed or the employee is initially assigned to a job** — (f)(1)
- **When the employee’s responsibilities under the plan change** — (f)(2)
- **When the plan is changed** — (f)(3)

This is not an annual-review requirement in so many words — it is a *change-driven* requirement. New hire, new role, revised plan: each triggers a review with the affected employees. The common failure mode is treating the EAP as a new-hire orientation checkbox and never revisiting it when the plan changes. If you revised the evacuation routes last quarter, (f)(3) required a review with every covered employee — did it happen, and can you prove it?

Putting it together

A compliant EAP is a working document, not a binder artifact. The audit that matters is a simple one: take the six elements of (c), the alarm of (d), the designees of (e), and the review triggers of (f), and ask for each — *show me where it is in the plan, show me it matches current reality, show me the last time it was tested or reviewed*. Every gap you find is a citation waiting for an inspector — or worse, a confusion waiting for an emergency.

How this connects

This article covers the regulatory skeleton. For the operational flesh around it, see the site’s Emergency Action Plans guide (evacuation vs. shelter-in-place decisions, assembly areas, accounting for employees with

disabilities) and the Crisis Communication Protocols guide (incident command, stakeholder notification, message templates) — the EAP tells people how to get out safely; those guides cover what the organization does next.

Resilience & Supply Chain Disruption Desk: CI Fortify Isolation Plans, Cloud SPOF Outages & DORA Register Gaps — Saturday, September 5, 2026

Source: <https://continuityhub.org/resilience-supply-chain-disruption-desk-ci-fortify-isolation-plans-cloud-spod-outages-dora-register-gaps-saturday-september-5-2026/> Published: September 5, 2026

Executive Operational Resilience Briefing for Enterprise Operations VPs, Chief Risk Officers, and Business Continuity Planning (BCP) Directors: Situational intelligence covering CISA CI Fortify isolation mandates, H1 2026 cloud and SaaS outage volume, vendor single points of failure, and DORA Register of Information gaps.

Most existing OT isolation plans will silently fail when operators try to execute them — because of a dependency most organizations didn't realize they had created.

Executive Supply Chain & Operational Disruption Overview

As enterprise operating models face compounding geopolitical, climate, and infrastructural stressors in 2026, organizational resilience mandates have shifted from passive documentation to active operational verification. The July 28 joint guidance from CISA, Australia's ASD, the UK NCSC, and Canada's CCCS — *CI Fortify: Advice for Isolating Vital Systems* — makes the requirement explicit: Critical infrastructure continuity requirements mean operators must be able to disconnect vital operational technology from corporate networks, the internet, and third parties, then keep delivering essential services while isolated. At the same time, H1 2026 cloud and SaaS reliability data shows 30,246 outages across 1,082 providers, with cloud providers leading the volume and many cascading from upstream control-plane or identity dependencies.

Operational Disruption Matrix & Business Impact Analysis (BIA)

Disruption Domain	Critical Failure Trigger	Target RTO / MTPD Threshold	Continuity & Mitigation Strategy
OT / Critical Infrastructure Isolation	State-sponsored OT compromise / ransomware on SCADA	RTO: 4 Hours / MTPD: 24 Hours	Pre-engineered separation points, graduated isolation plans, and tested manual/local operation paths per CI Fortify.
Cloud & SaaS Control Plane	Primary availability zone or identity provider outage	RTO: 1 Hour / RPO: 15 Minutes	Multi-region warm standby, control-plane resilience, and immutable air-gapped backup validation.
Tier-1/Tier-2 Supply Chain	Single-source supplier shutdown / port dwell spikes	RTO: 72 Hours / MTPD: 14 Days	Pre-qualified secondary suppliers, 60-day strategic buffer, and multi-tier mapping.
DORA ICT Third-Party	Critical provider outage or concentration risk	RTO: 24 Hours / MTPD: 72 Hours	Current Register of Information, exit strategies, and tested third-party BCDR evidence.

CI Fortify: The Isolation Mandate That Most Plans Will Fail

The blunt finding in the July guidance is that most existing OT isolation plans will silently fail on execution because operators cannot list — let alone disconnect from — their third-party dependencies. CISA’s CI Fortify requires mapping every connection to vital systems (corporate IT, vendor remote access, cloud platforms, internet-facing services), building separation points in advance, and running graduated isolation exercises — not partial tests. Partial tests miss the shared dependencies (identity, DNS, historians, licensing) that collapse the moment you cut the boundary. For continuity teams, this is no longer a cyber exercise; it is a BIA and RTO/MTPD verification exercise.

The same guidance puts the dependency problem in one line: “You can’t plan to operate disconnected from third parties for weeks or months until you can actually list who those third parties are. Most operators can’t.”

Cloud & SaaS SPOF: The Numbers Behind the Outages

IncidentHub’s H1 2026 report tracked 30,246 outages across 1,082 providers. May was the peak month at 6,070 incidents. Cloud providers led with 4,723 outages, followed closely by developer tools at 4,589. The report’s core lesson: many wide-reaching incidents originated one layer upstream — in edge and CDN networks, identity providers, LLM APIs, or a cloud control plane. Even resilient data planes fail when the control plane does. Enterprise continuity runbooks must decouple core workflows from single-provider identity and control-plane assumptions. AI and LLM APIs have moved into the production stack, so a single upstream model failure now cascades into customer support, EdTech, and communication tools with no fallback.

DORA Register of Information: The Gap That Supervisors Will Find

For financial entities in scope of DORA, Article 28 requires a living Register of Information covering every ICT third-party arrangement — the regulated entity, the provider, the service, the business function, criticality classification, subcontractors, data location, and exit/continuity evidence. It is not a one-off questionnaire; it must be current and available to the competent authority on request. The first Critical Third-Party Provider designations already flowed from this data. If your register is stale, incomplete, or lacks tested exit strategies for critical functions, that is the gap supervisors will surface first. Supervisors’ first-wave reviews found systemic gaps — missing subcontractor chains, incomplete CTPP flags, no recovery targets tied to business services. Incomplete registers have already triggered formal letters requiring remediation inside 60 days.

Enterprise Operations VP & BCP Director Tactical Checklist

- **1. CI Fortify Isolation Tabletop:** Run a graduated isolation exercise that cuts remote workers, then corporate connectivity, then all external links — and verify the shared dependencies that fail at each step.
- **2. Control-Plane Resilience Audit:** Map identity, DNS, licensing, and orchestration dependencies for every critical cloud workload; require multi-region or on-prem fallback for the control plane, not just the data plane.
- **3. DORA Register Refresh:** Update the Register of Information for all ICT arrangements supporting critical or important functions; attach exit strategies, subcontractor visibility, and recent BCDR test evidence.
- **4. Multi-Tier Supplier Mapping:** Extend mapping beyond tier-1 to the top 20 revenue-generating product lines; enforce contractual ISO 22301 audit receipts and secondary-source qualification.

Official Citations & Authoritative Continuity Frameworks

Operational standards and continuity frameworks referenced in this briefing:

- **CISA CI Fortify – Advice for Isolating Vital Systems:** cisa.gov/ci-fortify
- **IncidentHub H1 2026 Cloud & SaaS Reliability Report:** incidenthub.cloud
- **DORA Register of Information (EBA ITS):** eba.europa.eu
- **ISO 22301:2019:** Security and resilience — Business continuity management systems (iso.org)

Also on Continuity Hub: Resilience Desk — August 25 · DORA’s first exam year · Supply chain resilience guide · Regulatory convergence. Sister desks: Restoration Intel · Risk Coverage Hub.

Operational Resilience & BCP Disclaimer: This situational intelligence brief is compiled for Enterprise Operations VPs, Business Continuity Directors, Chief Risk Officers, and Supply Chain Managers for organizational resilience and continuity planning. It does not replace individualized Business Impact Analyses (BIA), certified ISO 22301 audits, or site-specific Disaster Recovery engineering. Always verify critical supply chain dependencies, utility redundancies, and incident management protocols with qualified continuity professionals and credentialed emergency response coordinators.

DORA’s First Exam Year: ISO 22301 Will Not Sit the Test for You

Source: <https://continuityhub.org/dora-first-exam-year-iso-22301-2026/> Published: August 15, 2026

DORA has been live since 17 January 2025. 2026 is the year the paperwork meets a supervisor. If your answer is still “we have ISO 22301,” that is a start, not a file.

We already mapped the stack last spring: DORA, CISA, ISO 22301. This is the exam-year cut of that piece.

What 2026 actually produced

On 3 June 2026 the European Supervisory Authorities published their first annual DORA report on major ICT-related incidents. Financial entities in the EU reported **3,383** major incidents. About a third had a cross-border impact. The main drivers were system failures and external events, not Hollywood hacks. Cyber was about 10%. The authorities pointed at third-party risk and shared infrastructure.

That is Article 22(2) doing what it said it would do: count the incidents, name the nature, look at client impact. If you sell continuity to an insurer or a bank with an EU passport, this is the dataset your client’s competent authority just read.

The other 2026 fact: the ESAs designated critical ICT third-party providers in November 2025. Those names now sit under Joint Examination Teams. Your cloud contract is no longer a private argument between you and the vendor.

ISO 22301 is not a DORA waiver

ISO 22301 is still a good continuity system: BIA, strategies, exercises, management review. DORA is a regulation. EIOPA’s DORA page lists the live pieces: ICT risk management, third-party policy, incident classification and reporting, testing (including threat-led penetration testing for the ones in scope), and

oversight of critical providers.

Article 11 wants an ICT business continuity policy that locks to incident response and recovery — not a generic pandemic binder with “cyber” taped on page 40. Yearly tests of backup, failover, and the continuity plan are table stakes. The Register of Information is how supervisors see your ICT chain. If that register is empty or pretty, the exam already failed.

Keep the ISO certificate. Add the DORA artifacts the RTS actually name: incident classification, major-incident reporting clocks, third-party clauses, exit plans, and a test calendar you can show without a scavenger hunt.

What to put on the desk this quarter

- Open last year’s incident log. Re-class it the DORA way. If you cannot say which events would have been “major,” you cannot report one.
- Pull the Register of Information for every ICT service that touches a critical function. Concentration on one cloud region should scare you more than a red-team slide.
- If you are a US continuity shop writing for an EU financial client, stop delivering a CISA-only packet. Their examiner is reading EBA/EIOPA/ESMA, not your FEMA annex.
- Exercise the exit: one vendor, one afternoon, who runs the function if that vendor is dark. Write the names.

The first DORA year was “are you in scope.” This year is “show the incident, the vendor, and the test.” Bring those three folders.

Sources: Regulation (EU) 2022/2554 (DORA, in application 17 January 2025); EIOPA DORA overview; ESAs first annual major ICT-incident report (3 June 2026).

Also on Continuity Hub: DORA / CISA / ISO 22301 stack · RCP / vendor Scope 3 · AI dependency resilience. Sister desks: BC ESG · Risk Coverage Hub.

Restoration Contractors and Scope 3: Why Business Continuity Planners Need the Restoration Carbon Protocol in Their Vendor ESG Stack

Source: <https://continuityhub.org/restoration-carbon-protocol-business-continuity-scope-3-vendor-esg/>

Published: April 11, 2026

Business continuity planning has always treated restoration contractors as operational dependencies — the vendors who execute property damage recovery when a loss disrupts operations. What has changed in 2026 is that those same contractors are now simultaneously an ESG supply chain liability for any organization with Scope 3 reporting obligations.

For BCM professionals at organizations subject to DORA, CISA operational resilience requirements, ISO 22301, or SBTi supplier engagement targets, the restoration contractor relationship now sits at the intersection of operational resilience and ESG compliance. A vendor who cannot provide emissions documentation is not just a data gap — they are a procurement compliance risk.

The Scope 3 Problem in Property Recovery

When a facility floods, burns, or sustains mold damage, the restoration contractor who responds generates Scope 3 emissions that appear in the building owner's Category 1 supply chain. Vehicle transportation to and from the loss. Materials deployed. Debris disposal. Demolished building materials. For organizations with GRESB reporting, SBTi commitments, or California SB 253 obligations, this is a reportable category.

The current state for most BCM-connected facility operators: restoration contractor emissions are either excluded from Scope 3 inventories with a documented exclusion, or estimated using spend-based proxies. Both are acknowledged limitations. Neither will satisfy the data quality requirements that GRESB, SBTi supplier engagement audits, and CSRD verification are moving toward.

The Restoration Carbon Protocol as Vendor ESG Infrastructure

The Restoration Carbon Protocol (RCP) v1.0, available free at tygartmedia.com/rcp, is the first open-source industry standard for calculating and reporting per-job Scope 3 emissions from restoration work. For business continuity and facility management professionals its practical value is straightforward:

Vendor qualification: Adding RCP compliance to preferred restoration contractor agreements establishes a documented ESG supply chain standard for property recovery vendors. This satisfies SBTi supplier engagement documentation requirements and supports GRESB Management Component scoring on vendor sustainability practices.

Claims-level ESG data: Each RCP Job Carbon Report covers one property damage event. For annual ESG reporting, these per-event records aggregate into an accurate portfolio figure that replaces spend-based estimation.

Continuity plan ESG integration: For organizations building climate resilience into their BCPs, RCP data provides the supply chain emissions baseline that quantifies the carbon cost of recovery scenarios. A water damage event affecting 5,000 sq ft of commercial office space has a documented RCP emissions range. That data belongs in climate resilience planning alongside business impact analysis.

What to Ask Your Restoration Contractors Now

- **Ask your preferred restoration vendors if they track the 12 RCP data points** — documented at tygartmedia.com/12-data-points-restoration-job-scope-3/.
- **Request RCP Job Carbon Reports for any new losses** — template at tygartmedia.com/rcp-job-carbon-report-template/.
- **Add RCP to your vendor ESG questionnaire** — alongside ISO certifications, IICRC credentials, and insurance coverage, add whether the vendor has implemented the Restoration Carbon Protocol or has a timeline to do so.

The full RCP framework, technical guides, and API documentation are at tygartmedia.com/rcp.

Also in this cluster: contractors on Restoration Intel, healthcare facilities on Healthcare Facility Hub, carriers on Risk Coverage Hub, and the property-manager guide on BC ESG.

Related: Front door: Complete Restoration Operations Kit (\$97). Hub: Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026). Continuity Hub home.

Business Continuity Regulatory Convergence in 2026: DORA, CISA, ISO 22301, and the New Resilience Compliance Stack

Source: <https://continuityhub.org/business-continuity-regulatory-convergence-2026-dora-cisa-iso22301/>

Published: April 3, 2026

DORA covers financial services. CISA covers critical infrastructure. ISO 22301 covers everyone with >100 employees. NIS2 covers digital operations across the EU. In 2026, most organizations are subject to multiple overlapping resilience mandates. What was once managed by business continuity planners as separate compliance projects is now converged into a single operational resilience framework.

The Four-Layer Resilience Stack

Layer 1: DORA (Digital Operational Resilience Act) DORA became effective January 17, 2025.

Enforcement is ramping up throughout 2026. DORA covers all financial entities (banks, insurers, investment firms, payment processors) and applies to EU and third-country entities operating in EU markets.

DORA mandates:

- **ICT Risk Management:** Identify all ICT systems, third-party dependencies, and potential failure points. Implement controls for confidentiality, integrity, availability.
- **Penetration Testing:** Conduct advanced penetration tests at least annually. Document findings, remediation, and validation.
- **Incident Reporting:** Report significant ICT incidents to regulatory authorities within defined timeframes. Maintain incident register.
- **Third-Party Oversight:** Audit ICT service providers (cloud, outsourced systems). Contractually require compliance. Monitor continuously.
- **Scenario Testing:** Conduct impact tolerance and scenario testing (e.g., single point of failure, supply chain disruption).

For financial entities, DORA compliance is mandatory and enforcement is accelerating. Regulators are issuing examination notices and imposing remediation deadlines.

Layer 2: CISA and Critical Infrastructure Requirements The Cybersecurity and Infrastructure Security Agency has issued CIRCIA (Critical Infrastructure Resilience and Recovery Act) guidance that applies to organizations designated as “critical infrastructure” (energy, water, transportation, communications, financial services, healthcare).

CISA requirements include:

- **Asset Management:** Know what systems are critical. Maintain current inventory.
- **Business Continuity and Disaster Recovery:** Plan for failures. Test recovery procedures. Maintain redundancy.
- **Supply Chain Risk Management:** Identify critical suppliers. Audit their controls. Monitor continuously.
- **Incident Response:** Detect and respond to failures quickly. Maintain communication with CISA and sector partners.

Overlap with DORA: If you're a financial entity in EU markets AND a critical infrastructure provider (e.g., payment processor, insurance carrier operating critical infrastructure), you're subject to both DORA AND CISA.

Layer 3: ISO 22301 (Business Continuity Management) ISO 22301 applies to organizations with >100 employees globally (no geographic restriction). In 2026, the standard amendment incorporates climate scenarios explicitly:

- **Climate Resilience:** Identify climate-related risks (flood, wildfire, heat, supply chain disruption). Model recovery in climate scenarios.
- **Impact Analysis:** Map business functions to recovery time objectives (RTO) and recovery point objectives (RPO). Include climate scenarios.
- **Testing and Drills:** Conduct impact tolerance tests and scenario drills (not just system failover tests; include climate scenarios, supplier failures, geopolitical disruption).
- **Governance:** ****Assign board-level accountability for business continuity. Link to enterprise risk management.**

ISO 22301 is increasingly required by auditors and investors as a baseline for operational resilience governance.

Layer 4: NIS2 Directive (EU Network and Information Systems Directive) NIS2 expanded the scope of EU cybersecurity requirements beyond critical infrastructure to include:

- **Essential services:** Digital infrastructure, waste management, postal services, public administration
- **Important entities:** Manufacturers of ICT products and services, cloud providers, hosting providers, digital service providers (e.g., online marketplaces)

NIS2 mandates:

- **Risk Management:** Implement appropriate technical, operational, and organizational measures to manage cybersecurity risk.
- **Incident Notification:** Report cybersecurity incidents to competent authorities.
- **Supply Chain Security:** Manage ICT supply chain risk.
- **Third-Party Audit:** Auditors and certification bodies must be notified of significant security measures.

Overlap with DORA: If you're a financial entity operating in EU markets, you're subject to both DORA (more stringent) and NIS2 (broader scope). DORA requirements typically exceed NIS2, so DORA compliance usually covers NIS2 obligations.

The Convergence Pressure: Three Integration Challenges

Challenge 1: Audit Consolidation Auditors expect to see one resilience narrative, not four separate programs. Organizations that maintain separate DORA, CISA, ISO 22301, and NIS2 programs create audit friction:

- Multiple risk registers (different frameworks, different risk quantification methods)
- Different governance structures (separate committees for ICT risk, business continuity, third-party risk)
- Duplicate testing and documentation (four different penetration test scopes, four different incident registers)

Challenge 2: Geographic and Sectoral Overlap An organization's scope across frameworks isn't always clear:

- Is our subsidiary in the EU? Then DORA AND NIS2 apply.
- Are we designated critical infrastructure AND a financial entity? Then CISA AND DORA apply.
- Do we have >100 employees globally AND operate in a regulated sector? Then ISO 22301, DORA, and NIS2 likely all apply.

Challenge 3: Testing and Scenario Alignment Each framework has different testing requirements. But testing is expensive and disruptive. Organizations are consolidating:

- One annual impact tolerance test that covers DORA scenario testing AND ISO 22301 impact analysis
- One penetration test program that covers DORA requirements AND NIS2 risk management
- One incident response drill that covers DORA incident reporting, CISA incident notification, and ISO 22301 response capability

Integrated Resilience Framework: How to Structure It

1. Single Risk Register** Map all resilience-related risks (ICT failures, supply chain disruption, climate events, geopolitical shocks) to a single register. Cross-reference which frameworks each risk maps to:

- System failure -> DORA ICT risk, CISA asset management, ISO 22301 impact analysis
- Supplier failure -> DORA third-party oversight, CISA supply chain, ISO 22301 dependency mapping
- Climate event -> ISO 22301 climate scenario, CISA resilience requirement, DORA scenario testing

2. Consolidated Governance** Create a single resilience governance structure:

- **Board Resilience Committee:** Oversight of operational resilience (DORA + CISA + ISO 22301 + NIS2) reported as single agenda item
- **Chief Resilience Officer:** Single executive responsible for coordinating all resilience programs (ICT risk, business continuity, third-party risk, incident response)
- **Resilience Program Management Office:** Coordinates DORA workstreams, CISA compliance, ISO 22301 maintenance, and NIS2 audits

3. Integrated Testing** Design one annual testing cycle that covers all frameworks:

- **Q1: Impact Tolerance Test** — assess RTO/RPO for critical functions under failure scenarios (covers DORA, ISO 22301, CISA)
- **Q2: Penetration Testing** — advanced penetration test of critical systems (covers DORA, NIS2)
- **Q3: Incident Response Drill** — full-scale incident response exercise (covers DORA incident reporting, CISA notification, ISO 22301 response)
- **Q4: Third-Party Risk Review** — audit critical suppliers' resilience controls (covers DORA, NIS2, CISA)

4. Consolidated Documentation One documentation set serves all frameworks:**

- **Resilience Policy and Governance Framework** (DORA, ISO 22301)
- **Risk Register and Assessment** (DORA, CISA, ISO 22301, NIS2)
- **Business Continuity Plan** (DORA, CISA, ISO 22301)
- **Incident Response Plan** (DORA, CISA, NIS2)
- **Third-Party Risk Management Framework** (DORA, NIS2)
- **Test Results and Remediation Tracking** (all frameworks)

Cross-Sector Context

Business continuity teams are applying the same integration logic that ESG teams have mastered for years. For broader context on cross-sector regulatory convergence, see [The 2026 Regulatory Convergence: ESG, Climate, AI, and Operational Standards](#).

Healthcare facilities face similar convergence pressures. Read [Healthcare Regulatory Convergence: CMS, Joint Commission, NFPA, FGI, and ESG](#).

What Organizations Must Do in 2026

- 1. Map Your Regulatory Scope** Determine which frameworks apply based on geography, sector, size, and critical infrastructure designation. Use [Regulatory Compliance for Business Continuity](#) as your starting point.
- 2. Consolidate Your Governance**** Move from siloed resilience programs to consolidated oversight. Assign a Chief Resilience Officer or equivalent. Link resilience to enterprise risk management.
- 3. Integrate Your Risk Assessment**** Build one resilience risk register that maps to all applicable frameworks. Use this for governance, testing, and audit preparation.
- 4. Plan Your Testing Program**** Design one annual testing cycle that covers all frameworks. This reduces cost, disruption, and audit friction.
- 5. Prepare for DORA Enforcement**** If you're a financial entity in EU markets, DORA enforcement is ramping up in 2026. Use [EU DORA Compliance](#) as your detailed implementation guide.

Conclusion

In 2026, business continuity is no longer a separate function managed by BC planners. It's a core operational resilience capability that intersects with ICT risk, supply chain management, climate resilience, and critical infrastructure continuity. Organizations that consolidate DORA, CISA, ISO 22301, and NIS2 into a single resilience framework will reduce cost, improve governance, and emerge as resilience leaders. Those that maintain silos will fragment.

Also on Continuity Hub: DORA first exam year · RCP / vendor Scope 3 · Physical climate risk / ISO 22301. Sister desks: BC ESG · Risk Coverage Hub.

Integrating Physical Climate Risk Into Your Business Continuity Program: The 2026 ISO 22301 Approach

Source: <https://continuityhub.org/physical-climate-risk-business-continuity-iso-22301-2026/> Published: April 3, 2026

Business continuity professionals have long worked with disruption scenarios—supply chain delays, IT outages, facility damage, key person loss. In 2026, a new mandatory element has entered the business continuity management system: climate-related disruption scenarios. ISO 22301 (Security and Resilience—Business Continuity Management System), which was revised in 2024, now explicitly requires organizations to consider climate-related hazards and climate scenarios in their business continuity and crisis management planning. This is not optional guidance; it is a formal control requirement.

For organizations seeking ISO 22301 certification or maintaining certification, this means business continuity programs must integrate physical climate risk assessment into the standard risk identification and scenario planning process. For organizations not pursuing formal ISO certification, the 2024 amendment reflects broader convergence: climate risk is now treated as a standard operational hazard, not a peripheral “sustainability” concern.

The ISO 22301:2024 Amendment: What Changed

The original ISO 22301 standard (released 2012, updated 2019) provided a framework for business continuity management: identify critical business functions, assess risks that could disrupt those functions, plan responses (prevention, recovery, alternative operations), test plans, and continuously improve. The framework was process-oriented but hazard-agnostic—it did not prescribe specific hazard categories to consider.

The 2024 amendment introduced explicit climate scenario integration into three key areas:

Risk Assessment (Clause 6.1): Organizations must now identify risks arising from climate-related hazards and climate change. This includes acute physical hazards (flooding, wildfire, extreme wind, heat stress) and chronic hazards (changing precipitation patterns, shifting temperature ranges, ecosystem changes affecting supply chains). Risk assessment must consider both current hazard exposure and projected changes under different climate scenarios.

Response Planning (Clause 8.1): Business continuity and crisis management plans must address climate-related disruption scenarios, not just traditional IT or operational outages. If a facility is in a

flood-prone zone, BC plans must include procedures for pre-event preparation, evacuation, facility recovery, and restoration of critical functions. If supply chains depend on climate-sensitive inputs (agricultural products, water-intensive materials), plans must address disruption and alternative sourcing.

Testing and Exercises (Clause 8.4): Business continuity exercises and tests must include climate-related scenarios. A tabletop exercise simulating a hurricane affecting a facility's region, or a flood affecting supplier locations, ensures that BC teams can actually execute plans under climate disruption. This surfaces gaps in planning and training.

Acute Physical Hazard: Sudden, discrete climate-related events that cause immediate damage—hurricanes, floods, wildfires, extreme heat waves, severe hail. These events require rapid response and recovery planning.

Chronic Physical Hazard: Gradual, long-term changes in climate patterns that create persistent stress—shifting precipitation reducing water availability, gradually rising temperatures affecting cooling or agricultural inputs, changing ecosystem health affecting supply chains. These require adaptation and strategic response planning.

Physical Climate Risk Assessment for Business Continuity

Implementing ISO 22301:2024 requires BC professionals to expand their risk vocabulary and assessment process to include physical climate hazards. This begins with hazard mapping: which locations does the organization operate in, and which climate hazards affect those locations?

For a multi-location organization, this involves:

Facility Risk Mapping: Identify each critical facility (headquarters, manufacturing, distribution, data centers, customer-facing locations) and assess its exposure to relevant climate hazards. A facility in coastal Florida faces hurricane risk, storm surge, and increased flooding. A facility in California faces wildfire and air quality risk. A facility in the Midwest faces hail, severe wind, and flooding risk. A facility in the Southwest faces drought and water scarcity risk. Hazard mapping uses publicly available data (FEMA flood zones, wildfire risk indices, climate projection data) or commercial hazard mapping services.

Supply Chain Vulnerability Assessment: Identify critical suppliers and assess their climate risk exposure. If a supplier operates in a region facing drought or water stress, long-term supply of their products is at risk. If a supplier is located in a flood-prone zone or wildfire-adjacent region, acute disruption risk is material. If a supplier depends on climate-sensitive inputs (agricultural products, water, rare earth minerals from environmentally sensitive regions), climate change creates supply risk. Building supply chain resilience requires understanding this vulnerability.

Operational Dependency Analysis: Map which business processes depend on which suppliers, facilities, and external services. If a critical manufacturing process depends on a single supplier in a climate-exposed region, disruption risk is high. If a service delivery operation depends on staff in a heat-stressed region or flood-prone area, labor availability during climate stress is at risk. If operations depend on a facility with limited cooling or flood protection, heat-related shutdowns or flood damage pose business continuity risk.

Operational Dependency: The relationship between a critical business process and the suppliers, facilities, services, or resources required to execute that process. High dependency on a single source creates concentration risk; diversified sources reduce disruption risk.

Climate Scenario Planning for Business Continuity

ISO 22301:2024 explicitly requires climate scenario planning. Rather than assuming current climate conditions continue indefinitely, BC plans must consider how physical climate risk evolves under different warming pathways. This is aligned with ISSB S2 and other disclosure standards that require scenario analysis.

A typical climate scenario planning exercise involves:

Define Time Horizons: Most BC plans focus on 1–5 year recovery timeframes. Climate scenarios require longer horizons. Organizations should model scenarios for 5–10 years (medium term, where near-term climate trends are relatively predictable) and 20–30 years (longer term, where adaptation investments must align with projected climate conditions).

Define Warming Pathways: Climate scenarios typically use ICP pathways (RCP 4.5 = 2°C warming, RCP 8.5 = 4°C+ warming by 2100). For business continuity purposes, scenario planning might use three simplified pathways: (1) moderate warming where current climate trends continue at historical rate, (2) accelerated warming where climate change intensifies faster than historical trends, and (3) severe/compound scenarios where multiple climate hazards interact (e.g., simultaneous drought and heat stress affecting agricultural supply chains).

Translate Scenarios to Operational Impacts: For each scenario and time horizon, assess how physical climate risk to critical facilities and supply chains changes. A facility in a 100-year flood zone today might be in a 50-year flood zone (twice as frequent) under moderate warming. A region currently experiencing occasional water stress might face chronic water shortage under accelerated warming. Wildfire risk zones might expand geographically. These changes affect asset risk, insurance costs, operational constraints, and recovery assumptions.

Test Plan Viability Under Scenarios: Once scenarios are defined, use them to test whether existing BC plans remain viable. A disaster recovery plan that assumes recovery of a flooded facility in 72 hours might not be viable if climate change increases flood frequency and duration. A supply chain contingency plan that relies on alternative sourcing from a region currently stable might fail if that region faces increased climate stress under future scenarios. This reveals gaps in planning.

Facility Hardening and Adaptation: Integration with BC Planning

For facilities identified as exposed to material climate risk, BC planning intersects with capital planning and facility adaptation. Organizations have choices for reducing climate risk to critical operations:

Prevention/Hardening: Invest in facility modifications that reduce climate hazard vulnerability. This might include elevated mechanical systems (above flood level), flood barriers, reinforced roofing and siding, backup power and cooling systems, redundant water supplies, and defensible space around buildings. These investments reduce the likelihood or severity of climate-related disruption.

Redundancy/Relocation: Establish backup facilities or operational capacity in lower-risk geographies, allowing operations to continue if primary facility is damaged. For critical functions, geographic redundancy is superior to facility hardening because it eliminates disruption entirely rather than just reducing it.

Insurance and Risk Transfer: Maintain appropriate insurance coverage for climate-related damage (property insurance, business interruption insurance, supply chain insurance). However, as discussed in parallel articles in this series, insurance availability is tightening for climate-exposed properties. Organizations facing uninsurable risk or unaffordable insurance must prioritize hardening and redundancy.

Acceptance: For lower-risk facilities or lower-impact disruption scenarios, organizations may accept the risk, meaning they will recover from disruption using available resources and insurance coverage. This is appropriate for non-critical operations or operations in moderate-risk zones.

Business Interruption Insurance: Coverage that reimburses an organization for lost income when a covered event (fire, storm damage, etc.) prevents normal operations. For climate-related disruptions, BI coverage is increasingly valuable but also increasingly hard to obtain and expensive in climate-exposed zones.

Supply Chain Resilience Under Climate Scenarios

Supply chain continuity is a critical component of business continuity. Many organizations depend on geographically concentrated suppliers or on suppliers located in climate-exposed regions. Climate scenario planning requires mapping these vulnerabilities and building resilience.

Supplier Diversification: Reduce dependence on single-source suppliers by developing relationships with alternative suppliers in different geographies. A supplier in a drought-prone region could be complemented by suppliers in regions with stable water availability. This increases sourcing cost and complexity but reduces disruption risk.

Supplier Engagement and Assessment: Work with critical suppliers to understand their climate risk exposure and their BC readiness. Suppliers with strong BC programs and geographic diversification are lower risk. Suppliers with single facilities in climate-exposed zones are higher risk. Organizations can incentivize supplier climate risk mitigation through supplier development programs or contractual requirements.

Inventory and Buffer Stock: For critical inputs with long lead times or concentrated sourcing, maintain buffer inventory that allows continued operations if supply is disrupted for weeks or months. This increases carrying cost but reduces business continuity risk. Buffer stock decisions should be informed by climate scenario analysis—if a supplier is located in a region expected to face increasing drought, buffer stock might be justified.

Alternative Inputs or Processes: Where feasible, design manufacturing or service processes to accommodate alternative inputs or methods. A manufacturer that can switch between two material suppliers faces lower disruption risk. A service operation that can shift to remote work has lower facility disruption risk. These process flexibilities are costly to build but valuable for resilience.

ISO 22301 Certification and Audit: What Auditors Now Expect

For organizations pursuing or maintaining ISO 22301 certification, the 2024 amendment means auditors now evaluate climate risk as part of the standard audit. Come prepared with:

- Climate hazard identification — hazard maps, data sources, and current vs. projected risk for your facilities.
- Integration into risk assessment — climate risk scored inside your standard risk framework, not as a sidecar, with documented materiality judgments.
- Climate scenario analysis — the scenarios you considered, your assumptions, and what they imply for continuity.
- Exercise evidence — after-action reports showing teams tested under climate scenarios and folded the lessons into plans.
- Annual review — climate risk reassessed at least yearly as new data and projections arrive.

Alignment with Broader Risk Disclosure and Governance

If your organization discloses climate risk under ISSB, TNFD, California law, or CSRD, your BC climate assessment should draw from the same enterprise-level analysis — and feed findings back into it. Where climate responsibility is split between sustainability and operational risk teams, make the coordination explicit: one shared assessment, not two conflicting ones.

For broader context: *Physical and Financial Climate Risk in 2026: The Cross-Sector ESG Disclosure Framework*. On this site: *Climate-Adapted Business Continuity*, *Business Continuity Planning: Complete Guide 2026*, and *Supply Chain Resilience: Complete Guide 2026*.

Conclusion

ISO 22301's 2024 amendment formalizes what forward-thinking BC professionals already knew: climate hazards are operational reality, not a peripheral concern. Integrate physical climate risk assessment, climate scenario planning, and climate-informed testing into your standard BC management system — and keep them current. The payoff is resilience that holds up against both today's variability and tomorrow's projections.

Climate-Adapted Business Continuity: ISO 22301 Amendment, Climate Scenario Planning, and Physical Risk Integration

Source: <https://continuityhub.org/climate-adapted-business-continuity-iso-22301-amendment-2026/>

Published: April 1, 2026

Published: April 2026 | Category: Risk Assessment

What is Climate-Adapted Business Continuity?

Climate-adapted business continuity integrates physical climate risks (hurricanes, flooding, heat waves, wildfires) and transition risks (regulatory changes, market shifts, technology disruption driven by decarbonization) into formal continuity planning frameworks. The ISO 22301:2019/Amd 1:2024

amendment now requires organizations to explicitly assess climate-related business impacts and incorporate climate scenarios into business continuity strategies. This approach recognizes that climate change is not a low-probability tail risk but a material, quantifiable continuity driver that reshapes facility location decisions, supply chain resilience, and recovery strategy design.

ISO 22301:2019 Amendment 1:2024 and the Mainstreaming of Climate Risk

The 2024 amendment to ISO 22301 represents a watershed moment in business continuity practice. For the first time, an international standard for business continuity explicitly requires organizations to identify and assess climate-related threats to business operations. The amendment mandates that continuity planning includes climate change scenarios, that business impact analysis reflects climate-driven disruption patterns, and that recovery strategies account for increasingly frequent and intense climate events.

The amendment's scope extends beyond obvious climate hazards. While flooding, hurricanes, and wildfires are explicitly listed, the standard also requires assessment of secondary and cascading impacts: supply chain disruptions triggered by climate events in supplier regions, demand shifts as customers adapt to climate impacts, workforce disruption from climate-driven migration or extreme weather effects on commuting, and regulatory changes driven by climate policy agendas across jurisdictions where the organization operates.

Organizations achieving ISO 22301:2019/Amd 1:2024 compliance have fundamentally rethought their continuity strategies. A manufacturing firm previously assuming a hurricane strike probability of once per 20 years must now incorporate current climate science showing that event frequency has increased to once per 7-10 years in relevant regions. This dramatically changes the calculation for redundant facility investments, inventory buffering, and recovery resource positioning. A financial services firm previously assuming relatively stable coastal real estate availability must now assess climate migration patterns: as some coastal areas experience increasing flooding, commercial real estate availability shifts inland, potentially constraining expansion opportunities and forcing costly facility relocation.

Climate Scenario Planning: From One-Off Assumptions to Systematic Exploration

Traditional business continuity planning relied on static assumptions: we assume a one-day power outage, a 48-hour facility evacuation, a three-week supply chain disruption. Climate scenario planning inverts this approach. Rather than assuming a single disruption profile, organizations now construct multiple climate scenarios aligned with scientific climate projections and explore how business operations would respond under each scenario.

Organizations typically construct three scenarios. A “baseline” scenario assumes climate conditions remain close to recent historical norms with gradual intensification of existing climate patterns. A “high change” scenario assumes accelerated climate impacts: more frequent extreme weather, faster sea-level rise, more severe droughts and heat waves. A “transformation” scenario assumes climate impacts severe enough to trigger systemic changes: mass migration, agricultural collapse in certain regions, supply chain consolidation around newly favorable climate zones. Each scenario is paired with specific climate parameters: temperature ranges, precipitation patterns, extreme weather frequency, sea-level rise

projections.

A healthcare facility in a coastal region might explore a high-change scenario where hurricane-force storms increase from once per decade to once per three years. Under this scenario, the facility's current resilience strategy—external generator backup lasting 72 hours, supplies for five days, 30% staffing surge capacity—becomes inadequate. The organization discovers that under high-change scenarios, recovery requires not incremental improvements but architectural changes: moving critical facilities to elevated inland locations, establishing satellite treatment capability in low-risk regions, building vendor relationships in geographically dispersed supply bases, and establishing workforce mobility protocols for pre-storm evacuation.

A retail company exploring transformation scenarios discovers that agricultural supply disruptions cascade through food supply chains faster than previously modeled. Under transformation scenarios, traditional supply chains for critical consumables break down within weeks of climate crisis onset. The organization develops pre-crisis agreements with alternative suppliers, maintains strategic inventory buffers for shelf-stable alternatives, and establishes distribution protocols that bypass traditional supply chains under extreme conditions.

Climate scenario planning forces organizations to distinguish between resilience that works during incremental change and resilience that works during transformation. Many traditional continuity strategies provide resilience during incremental change but fail when climate impacts reach transformation thresholds. Organizations explicitly model these breaking points and develop transition strategies that maintain operations across the shift from incremental to transformational impacts.

Physical Risk Integration: Facility Location, Supply Chain Mapping, and Infrastructure Dependency

Physical climate risks directly threaten facility operations, supply chain flows, and critical infrastructure that organizations depend on. Sophisticated physical risk integration now requires three parallel assessments: direct risks to the organization's own facilities, indirect risks to critical suppliers and logistics hubs, and systemic risks to shared infrastructure (ports, airports, power grids, water systems).

Direct facility risk assessment has matured considerably. Organizations no longer rely on static historical flood maps from FEMA or static hurricane risk zones. Current practice integrates dynamic climate models that project changing flood risk, wildfire risk, and extreme temperature risk over the next 10-30 years. A distribution center located in a region that has never experienced significant flooding may now be assessed as facing material flooding risk by 2035-2040 due to rainfall intensification in that region. A data center's cooling capacity assumptions must be revalidated against peak temperature projections that increase by 3-5 degrees Celsius over the planning horizon.

Indirect supply chain risk assessment extends beyond the organization's direct suppliers to second-tier and third-tier supply relationships. A smartphone manufacturer understands that rare earth element supply comes from specific geographic regions. That manufacturer now models how climate impacts in those regions—extreme heat disrupting mining operations, flooding damaging processing facilities, drought-driven water scarcity limiting processing capacity—would reduce global rare earth supply and trigger price spikes or allocation constraints. The manufacturer develops alternative sourcing

relationships and substitution strategies informed by this climate-driven supply chain modeling.

Systemic infrastructure risk assessment identifies dependencies on shared infrastructure vulnerable to climate impacts. A hospital depends on the regional electrical grid; if climate-driven demand surge (from widespread air conditioning use during heat waves) or weather-driven damage disrupts that grid, the hospital's backup power becomes critical. A port depends on dredging to maintain navigable channels; if drought reduces dredging material availability or climate-driven erosion accelerates channel shoaling, port capacity decreases. A manufacturing facility depends on regional water availability for cooling; if drought reduces water availability or regulatory allocations shift toward agriculture, manufacturing must find alternative cooling sources.

Transition Risk Integration: Market, Regulatory, and Technology Disruption

Transition risks—market, regulatory, and technology changes driven by climate action—are more subtle than physical risks but often more material. Organizations now explicitly model how decarbonization regulatory changes, customer climate preferences, and competitive technology shifts would impact business operations and financial performance.

Regulatory transition risk manifests through carbon pricing mechanisms, emissions standards, and sectoral phase-outs. An organization operating in jurisdictions that implement carbon pricing must adjust product cost structures; if competitors operate in lower-carbon-cost regions, competitive advantage shifts. Organizations now model regulatory changes across different geographies and time horizons, assessing which regions might phase out key products (internal combustion engines, fossil fuel power generation) and how that reshapes market dynamics. Business continuity strategies must account for these regulatory transitions: developing new product lines to replace regulated products, developing new supplier relationships in different geographies, and managing workforce skill transitions as product portfolios shift.

Market transition risk captures customer preference shifts and demand destruction driven by climate impacts and climate action. A luxury goods manufacturer supplying climate-vulnerable regions may see demand destruction as climate impacts reduce discretionary spending and trigger migration away from affected areas. An insurance company may see demand growth in disaster recovery and resilience services but demand destruction in legacy products threatened by climate impacts. Organizations now conduct scenario-based demand modeling that asks: under physical climate scenario X combined with regulatory transition Y, how does customer demand for our products change? What products become obsolete? What products see accelerating growth? Business continuity strategies must now include product portfolio transitions and shifting supply chain configurations to support product mix evolution.

Technology transition risk emerges from the shift to renewable energy, electrification, and circular economy models. An organization dependent on specific energy sources (natural gas, fossil fuels) faces transition risk if markets and regulations shift to renewable energy faster than anticipated. An organization dependent on virgin material supply chains faces disruption if circular economy regulations or customer preferences drive accelerating material recycling. Organizations now map technology transition dependencies and develop contingency strategies for rapid technology shifts.

Cross-Site Coordination: Climate Risk in Insurance, ESG, and Restoration Planning

Climate-adapted business continuity planning increasingly intersects with insurance risk assessment, ESG reporting obligations, and physical restoration planning.

Insurance and Catastrophe Modeling: Risk Coverage Hub provides detailed frameworks for how business continuity planning coordinates with catastrophe insurance and risk transfer strategies. Organizations conducting climate scenario analysis now use the same climate models and geographic risk data that insurers use for catastrophe loss modeling. This alignment helps organizations understand how climate change reshapes insurance availability and pricing. Many organizations discover that climate impacts will occur beyond traditional insurance coverage windows; business continuity strategies must account for uninsurable losses and develop resilience that doesn't depend on insurance payouts. Read more on catastrophe modeling and insurance risk assessment.

ESG Reporting and Climate Disclosure: BCESG addresses how business continuity planning integrates with climate risk disclosure required by ESG frameworks (TCFD, SEC climate disclosure rules). Organizations conducting climate scenario analysis for continuity planning can leverage that work for ESG climate risk reporting. The climate scenarios developed for business continuity purposes directly address investor requests for climate scenario analysis showing financial impact under different warming pathways. Organizations that integrate business continuity and ESG climate reporting avoid duplicative work and ensure consistency in climate assumptions across organizational functions. Detailed guidance on climate risk disclosure integration is available on BCESG climate and governance frameworks.

Physical Restoration and Climate-Driven Demand: Restoration Intel documents how increasing climate impacts drive demand for property damage restoration services and facility recovery. Organizations conducting business continuity planning should understand how climate impacts that would trigger their own recovery plans simultaneously increase demand for restoration services—potentially creating scarcity of restoration resources, contractors, and materials during the exact window when the organization needs them most. This creates incentive to develop advance relationships with restoration providers and pre-positioned recovery resources. The intersection of business continuity planning and restoration service availability is explored on Restoration Intel.

Implementation: From Planning to Operational Integration

Climate-adapted continuity planning requires translating climate scenarios into operational changes. Organizations typically implement through staged programs:

Phase 1: Baseline Assessment. Assess current physical risks, indirect supply chain risks, and transition risks using climate science data current as of 2025-2026. Document facility-level, supply-chain-level, and systemic infrastructure risks. Identify which business processes face material climate-driven disruption risk under different climate scenarios.

Phase 2: Recovery Strategy Revision. Revise business continuity plans, disaster recovery strategies, and recovery procedures to reflect climate-changed risk profiles. Adjust facility redundancy investments, recovery site locations, supply chain diversification, and resource pre-positioning based on climate

scenario impacts.

Phase 3: Operational Readiness. Conduct continuity exercises that incorporate climate scenarios. Train response teams on climate-adapted procedures. Establish monitoring systems that track both physical climate impacts and transition risk indicators (regulatory changes, technology deployment, market shifts).

Phase 4: Continuous Evolution. As climate science models update and climate impacts are observed to exceed or underperform projections, continuity plans must be updated. Organizations establish annual review cycles that assess whether climate scenarios remain valid and whether operational changes are matching the pace of observed climate change.

Measuring Climate Resilience Maturity

Organizations typically assess climate resilience maturity across three dimensions: explicit climate risk assessment in continuity planning, integration of climate scenarios into business impact analysis and recovery strategies, and operational readiness for climate-adapted recovery procedures. Mature organizations demonstrate all three; developing organizations often begin with explicit risk assessment but lack scenario integration or operational readiness.

For related context on continuity planning, explore articles on risk assessment, disaster recovery planning, and operational resilience.

Conclusion: Business Continuity in a Climate-Changed World

Climate-adapted business continuity represents the mainstreaming of climate risk into core organizational resilience planning. The ISO 22301:2019/Amd 1:2024 amendment codifies what sophisticated organizations discovered through independent analysis: climate change is not a peripheral risk management topic but a material driver of operational disruption that fundamentally reshapes where organizations can locate facilities, how supply chains must be configured, which products remain viable, and what recovery strategies remain feasible. Organizations that integrate physical climate risks, transition risks, and scenario-based planning into continuity frameworks position themselves to maintain operations through climate change that others will struggle to absorb.

Regulatory Compliance: Expert Video Analysis

Source: <https://continuityhub.org/video-regulatory-compliance/> Published: March 18, 2026

[Home](#) / [Categories](#) / [Regulatory Compliance](#)

Regulatory Compliance

Featured video analysis and expert resources

What is Business Continuity and Disaster Recovery Planning?

Channel: CBT Nuggets

Published: February 09, 2023

47,052 views

808 likes

1.7% engagement

Video sourced and analyzed for Continuity Hub educational content. Score: 60/100

Why This Matters

Understanding regulatory compliance is essential for business continuity professionals seeking to minimize organizational risk, meet regulatory requirements, and build resilient operations. This video provides practical insights applicable across industries and organizational sizes.

Key Moments

Timestamp	Topic
00:00:00	– Introduction to business continuity and disaster recovery planning
00:30:00	– Assigning ownership
01:15:00	– Developing a BC/DR policy
02:40:00	– Performing a business impact analysis
03:55:00	– Performing critical analysis

Regulatory Compliance

Adherence to legal and regulatory requirements governing business continuity and emergency management.

ISO 22301 DRII BCI FEMA

Key Takeaways

- Map regulatory requirements specific to your industry and jurisdiction
- Align continuity programs with ISO 22301 and sector-specific standards
- Document compliance activities and audit readiness
- Maintain regulatory relationships and stay informed of changes
- Integrate compliance into continuity and risk management strategies

Expert Analysis

Regulatory Compliance represents a critical organizational discipline. Modern threats—from cyber attacks to natural disasters to supply chain disruptions—require comprehensive, well-tested response capabilities. Organizations that invest in these programs not only reduce risk but also gain competitive advantages through operational resilience.

The framework presented in this video aligns with international best practices and regulatory requirements. Implementation requires cross-functional collaboration, executive sponsorship, and ongoing commitment to testing and improvement. Success is measured not by the plan documents themselves, but by organizational readiness and speed of response when disruptions occur.

For business continuity professionals, the key is translating these concepts into actionable organizational programs that integrate with enterprise risk management, operational planning, and crisis management structures.

Related Standards & Frameworks

Standard	Description	Reference
ISO 22301	International standard for business continuity management systems	View
NFPA 1600	Standard for disaster/emergency management and business continuity programs	View
FEMA Framework	Federal emergency management guidance and best practices	View
DHS NIST	Cybersecurity framework including business continuity requirements	View
DRII Standards	Disaster Recovery Institute International professional standards	View
BCI GPG	Business Continuity Institute Good Practice Guidelines	View

Related Reading on Continuity Hub

- [Business Continuity Planning](#)
- [Disaster Recovery](#)
- [Risk Assessment](#)
- [Regulatory Compliance](#)

Related Resources

For complementary perspectives on emergency response and operational resilience:

[Emergency Response at Restoration Intel Risk Management at Risk Coverage Hub Healthcare Emergency Management](#)

Key Terms Glossary

Regulatory Framework Set of laws and standards governing business continuity requirements

Audit Trail Documented evidence of compliance activities and processes

Non-Compliance Risk Potential penalties, fines, and legal liability from regulatory violations

Compliance Officer Designated responsible party for regulatory adherence

Frequently Asked Questions

What are the main regulatory frameworks governing business continuity?

Key frameworks include ISO 22301 (international standard), NFPA 1600 (emergency management), FEMA guidelines, sector-specific regulations (financial, healthcare, telecommunications), and DHS continuity requirements for critical infrastructure.

How do organizations demonstrate regulatory compliance?

Compliance is demonstrated through documentation of policies, procedures, training records, test results, audit findings, and corrective actions. Regular audits and management reviews provide evidence of ongoing compliance.

What are the consequences of non-compliance?

Consequences vary by jurisdiction and industry but can include regulatory fines, legal liability, customer trust loss, operational restrictions, and reputational damage. Significant incidents in non-compliant organizations face increased scrutiny.

How do you align continuity programs with regulatory requirements?

Alignment requires understanding applicable regulations, mapping requirements to existing programs, identifying gaps, implementing enhancements, and documenting compliance. Regular regulatory monitoring ensures sustained alignment.

About This Category

Regulatory Compliance is a cornerstone of organizational resilience and risk management.

Video Quality Score

60/100

Key Resources [ISO 22301 Standard](#) [DRII Certification](#) [BCI Resources](#) [FEMA Guidance](#)

Browse Categories [Business Continuity Planning](#) [Business Impact Analysis](#) [Disaster Recovery](#) [Crisis Management](#) [Risk Assessment](#)

Industry Standards [ISO](#) [NFPA](#) [FEMA](#) [NIST](#)

Critical Infrastructure Continuity Requirements: CISA, NERC CIP, and CIRCIA

Source: <https://continuityhub.org/critical-infrastructure-continuity-requirements-cisa-nerc-cip-circia/>

Published: March 18, 2026

Published: March 18, 2026 | Publisher: Continuity Hub

- [Home](#)
- [Regulatory Compliance](#)
- [Critical Infrastructure Continuity Requirements: CISA, NERC CIP, and CIRCIA](#)

Introduction: Critical Infrastructure and National Security

Critical infrastructure organizations—including electric power systems, natural gas pipelines, water utilities, telecommunications networks, transportation systems, and other sectors vital to national security and economic stability—face regulatory requirements designed to ensure resilience, continuity, and rapid recovery from disruptions. These requirements reflect the national security imperative to maintain functioning infrastructure that supports all other economic and social activities.

Critical Infrastructure Continuity Compliance: The adherence to federal regulatory frameworks mandating that organizations operating critical infrastructure develop, test, and maintain business continuity and disaster recovery capabilities ensuring critical infrastructure services remain available during disruptions and can be restored rapidly, with particular emphasis on cyber and physical security, resilience to natural disasters, and coordination with federal agencies and sector partners.

This guide explores the major regulatory frameworks governing critical infrastructure business continuity, including requirements from the Cybersecurity and Infrastructure Security Agency (CISA), the North American Electric Reliability Corporation (NERC), and the Critical Infrastructure Resilience Act (CIRCIA).

Cybersecurity and Infrastructure Security Agency (CISA) Framework

CISA, established within the Department of Homeland Security, serves as the federal focal point for critical infrastructure protection and resilience. CISA issues guidance and establishes requirements for critical infrastructure owners and operators through Sector-Specific Agencies (SSAs).

CISA Authority and Mission

CISA's authority derives from:

- Homeland Security Act of 2002 (6 U.S.C. § 101 et seq.)
- CISA Act of 2018 (6 U.S.C. § 1501 et seq.), establishing CISA as independent agency

- **Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience**
- **Executive Order 13636 on Improving Critical Infrastructure Cybersecurity**
- **National Infrastructure Protection Plan (NIPP) 2013 framework**

CISA Resilience Guidelines

CISA has issued comprehensive guidance on critical infrastructure resilience through multiple frameworks:

Cybersecurity Framework (CSF)

CISA adopted and regularly updates the NIST Cybersecurity Framework, a voluntary framework for managing cybersecurity risk that includes business continuity considerations:

- **Identify:** Understanding critical assets, systems, and dependencies
- **Protect:** Implementing safeguards to protect critical systems
- **Detect:** Detecting cybersecurity events affecting critical systems
- **Respond:** Taking action in response to detected cybersecurity events
- **Recover:** Recovering from cybersecurity incidents and restoring services

Infrastructure Resilience Assessment Methodology

- **Asset Identification:** Comprehensive inventory of critical assets and interdependencies
- **Vulnerability Assessment:** Systematic evaluation of vulnerabilities to cyber, physical, and natural hazards
- **Impact Analysis:** Assessment of potential impacts of loss or degradation of critical assets
- **Resilience Strategy:** Development of strategies to mitigate identified risks and enhance resilience
- **Testing and Validation:** Regular testing of resilience capabilities and recovery procedures

Sector-Specific Guidance

CISA coordinates with Sector-Specific Agencies responsible for different infrastructure sectors:

- **Energy Sector:** Department of Energy oversees electric power and oil/natural gas
- **Water Sector:** Environmental Protection Agency oversees water and wastewater systems
- **Communications Sector:** Federal Communications Commission coordinates with industry
- **Transportation Sector:** Department of Transportation oversees rail, aviation, and highway
- **Financial Services Sector:** Coordinated with Treasury Department and banking regulators

CISA Coordination and Information Sharing

CISA coordinates critical infrastructure protection and resilience through:

- **Automated Indicator Sharing (AIS):** Free sharing of cybersecurity indicators with infrastructure organizations
- **Information Sharing and Analysis Centers (ISACs):** Sector-specific information sharing organizations coordinating with CISA

- **Critical Infrastructure Resilience Institute (CIRI):** Research center for developing resilience strategies
- **Exercises and Tabletops:** Coordinated exercises testing infrastructure resilience and emergency response

NERC Critical Infrastructure Protection (CIP) Standards

The North American Electric Reliability Corporation (NERC) is a self-regulatory organization subject to oversight by the Federal Energy Regulatory Commission (FERC). NERC develops and enforces reliability standards applicable to owners, operators, and users of bulk power systems.

NERC Authority and Jurisdiction

NERC's authority derives from:

- Federal Power Act § 215, which authorized FERC to approve reliability standards
- Order 672 (18 CFR Part 39), which approved NERC as the Electric Reliability Organization (ERO)
- NERC Rules of Procedure establishing standards development and enforcement procedures
- Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) that delegate compliance monitoring

NERC CIP Standards for Business Continuity

NERC has developed comprehensive CIP standards addressing critical infrastructure protection for bulk power systems. Key standards addressing business continuity include:

CIP-007-6: Systems Security Management

- **Backup and Recovery:** Requirements for backup and recovery systems protecting against data loss
- **Recovery Plans:** Documented procedures for recovering critical systems within specified timeframes
- **Redundant Systems:** Requirements for redundant systems supporting critical bulk power system operations
- **Testing Requirements:** Annual testing of backup and recovery systems

CIP-009-6: Configuration and Vulnerability Management

- **Configuration Documentation:** Comprehensive documentation of critical systems configurations
- **Change Management:** Procedures for managing changes to critical system configurations
- **Recovery Documentation:** Documentation supporting recovery of critical systems
- **Secure Configuration:** Procedures ensuring systems are securely configured

CIP-010-2: Configuration and Vulnerability Management (Physical)

- **Physical Security:** Controls protecting critical systems from physical access and sabotage
- **Facility Security:** Security measures at facilities housing critical systems
- **Perimeter Protection:** Fencing, gates, and access controls around critical facilities
- **Recovery Capability:** Physical redundancy supporting rapid recovery from physical damage

CIP-013-1: Supply Chain Risk Management

- **Supply Chain Risk Assessment:** Evaluation of supply chain vulnerabilities affecting critical systems
- **Vendor Due Diligence:** Assessment of critical vendors' security and resilience capabilities
- **Contingency Planning:** Plans addressing vendor disruptions or security failures
- **Supplier Agreements:** Contractual requirements specifying security and resilience expectations

NERC Enforcement and Compliance

NERC enforces CIP standards through:

- **Compliance Audits:** Regular audits of regulated entities' compliance with CIP standards
- **Spot Checks:** Unannounced compliance verification activities
- **Violation Assessment:** Evaluation of violations and severity levels
- **Penalties:** Monetary penalties up to \$1 million per day for violations, with enhanced penalties for cyber-critical violations

NERC Standards Development

NERC continuously updates CIP standards to address emerging threats and technological changes.

Organizations should:

- **Monitor NERC standards development activities** for proposed changes
- **Participate in comment periods** on proposed standards
- **Implement new standards** within required implementation periods (typically 24 months)
- **Update compliance procedures** as standards evolve

Critical Infrastructure Resilience Act (CIRCIA)

The Critical Infrastructure Resilience Act (CIRCIA), enacted in 2024, establishes enhanced resilience requirements for high-risk critical infrastructure sectors and creates new mechanisms for federal coordination and information sharing.

CIRCIA Scope and Applicability

CIRCIA applies to organizations designated as “covered critical infrastructure” based on:

- **Sector designation** (energy, water, communications, transportation, financial services, and others)
- **Criticality assessment** by federal agencies and sector partners
- **Assessment of potential consequences** of service disruption
- **Vulnerability to deliberate attacks, natural disasters, and operational failures**

CIRCIA Resilience Requirements

CIRCIA establishes enhanced requirements for covered critical infrastructure:

Resilience Assessments

- **Periodic Assessments:** Annual or biennial assessments of critical infrastructure resilience

- **Assessment Scope:** Comprehensive evaluation including cyber, physical, and operational resilience
- **Interdependency Analysis:** Assessment of dependencies on other infrastructure sectors
- **Recovery Capability Assessment:** Evaluation of ability to recover from severe disruptions
- **Stakeholder Engagement:** Assessment development should engage relevant federal agencies and partners

Enhanced Reporting Requirements

- **Resilience Plans:** Submission of detailed resilience plans to relevant federal agencies
- **Incident Reporting:** Reporting of significant disruptions and security incidents to CISA
- **Resilience Metrics:** Regular reporting of resilience-related metrics and performance indicators
- **Third-Party Risk Reporting:** Reporting of material risks posed by critical vendors and service providers

Information Sharing and Coordination

- **CISA Coordination:** Enhanced coordination with CISA on resilience planning and incident response
- **Sector Coordination:** Regular information sharing with sector partners through ISACs
- **Federal Agency Coordination:** Engagement with relevant federal agencies on resilience and security matters
- **Public-Private Partnership:** Participation in public-private partnerships addressing critical infrastructure resilience

Testing and Validation

- **Resilience Testing:** Regular testing of critical infrastructure systems and recovery procedures
- **Scenario-Based Testing:** Testing using severe but plausible disruption scenarios
- **Coordinated Exercises:** Participation in federal exercises testing sector resilience and recovery
- **Results Documentation:** Comprehensive documentation of testing results and findings

CIRCIA Enforcement

CIRCIA establishes enforcement mechanisms for critical infrastructure resilience requirements:

- **Federal Authority:** CISA and Sector-Specific Agencies have authority to enforce resilience requirements
- **Compliance Assessments:** Regular assessments of resilience plan implementation and compliance
- **Remediation Requirements:** Identified deficiencies must be remediated within specified timeframes
- **Escalated Enforcement:** Failure to remediate deficiencies can result in regulatory escalation and potential operational restrictions

Sector-Specific Continuity Requirements

Beyond overarching frameworks, different critical infrastructure sectors have specific regulatory requirements addressing their unique characteristics and vulnerabilities:

Energy Sector Requirements

- **NERC CIP Standards:** Comprehensive standards for bulk power system reliability and security
- **FERC Order 907:** Requirements for grid services from demand response, storage, and distributed energy resources
- **Energy Security and Resilience Initiative (ESRI):** Department of Energy programs supporting resilience initiatives
- **Oil and Natural Gas Sector:** Coordinated security and resilience requirements for oil and natural gas infrastructure

Water Sector Requirements

- **Safe Drinking Water Act:** Security and emergency response requirements for drinking water systems
- **Water Infrastructure Finance and Innovation Act (WIFIA):** Financing support for resilience projects
- **EPA Guidance:** Environmental Protection Agency guidance on water system resilience and emergency preparedness
- **State Requirements:** State drinking water and wastewater regulations

Communications Sector Requirements

- **FCC Declaratory Ruling on Cybersecurity:** FCC requirements for telecommunications carrier network security
- **Network Redundancy:** Requirements for redundant telecommunications networks supporting emergency response
- **Emergency Access:** Requirements ensuring emergency services access to communications infrastructure during disruptions
- **Data Protection:** Requirements for protecting customer communications and network data

Transportation Sector Requirements

- **Pipeline and Hazardous Materials Safety Administration (PHMSA):** Hazardous liquids pipeline safety and security requirements
- **Federal Railroad Administration (FRA):** Rail system security and emergency response requirements
- **Federal Aviation Administration (FAA):** Airport security and operations continuity requirements
- **Maritime Administration (MARAD):** Port security and maritime domain awareness requirements

Financial Services Sector Requirements

- **Banking Regulator Requirements:** Federal Reserve, OCC, FDIC business continuity requirements discussed in earlier sections

- **Securities Exchange Requirements:** SEC requirements for critical market infrastructure
- **Payment Systems:** Requirements for payment system operators ensuring continuity of critical payment services

Critical Infrastructure Dependencies and Interdependencies

Critical infrastructure organizations are increasingly dependent on other infrastructure sectors. Business continuity planning must address interdependencies with:

Power System Dependency

- Water treatment and distribution systems dependent on electric power
- Communications systems dependent on backup power during grid outages
- Transportation systems (rail, subway systems) dependent on electric power
- Financial services dependent on electric power for data centers and operations

Communications Infrastructure Dependency

- All critical infrastructure sectors dependent on telecommunications for operational coordination
- Power systems dependent on SCADA communications
- Transportation systems dependent on traffic control and operational communications
- Emergency response dependent on 911 and first responder communications

Supply Chain Interdependencies

- Dependencies on critical component suppliers
- Dependencies on specialized maintenance and repair services
- Dependencies on transportation for fuel and supply delivery
- Dependencies on financial institutions for operational funding

Continuity Planning Approach

Business continuity plans should address interdependencies through:

- Comprehensive mapping of critical dependencies on other infrastructure sectors
- Coordination with dependent infrastructure operators on resilience and recovery
- Redundancy and backup systems to mitigate critical dependencies
- Regular engagement with infrastructure partners on resilience issues
- Scenario-based exercises testing recovery under conditions of dependent infrastructure disruption

Integration with Business Continuity and Risk Management

Critical infrastructure continuity compliance builds upon fundamental frameworks covered in related guides:

- **Business Continuity Planning: Complete Professional Guide** provides foundational BC&DR planning principles applicable within critical infrastructure frameworks
- **Risk Assessment: Complete Professional Guide** details the business impact analysis and risk assessment processes essential for critical infrastructure planning
- **Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026)** surveys regulatory requirements across all sectors
- **Operational Resilience: Complete Professional Guide** explores emerging resilience frameworks increasingly required for critical infrastructure

Frequently Asked Questions

FAQ 1: What is the difference between CISA guidance and NERC CIP standards?

CISA guidance is generally voluntary (though sometimes adopted by Sector-Specific Agencies), providing recommended practices for critical infrastructure resilience. NERC CIP standards are mandatory enforceable requirements developed by the Electric Reliability Organization and subject to Federal Energy Regulatory Commission approval. Violations of NERC standards can result in substantial monetary penalties. Other critical infrastructure sectors may have a mix of mandatory requirements (like CISA orders) and voluntary guidance (like general CISA resilience guidance).

FAQ 2: How does CIRCIA change critical infrastructure resilience requirements?

CIRCIA establishes enhanced and more formalized resilience requirements for covered critical infrastructure, including mandatory resilience assessments, enhanced federal reporting requirements, and strengthened coordination mechanisms with CISA. CIRCIA creates enforceable requirements for covered critical infrastructure beyond voluntary compliance with CISA guidance, though specific requirements vary by sector and are still being implemented through regulatory processes.

FAQ 3: What is meant by “critical infrastructure interdependencies” and how should they be addressed in business continuity planning?

Critical infrastructure interdependencies are dependencies of one infrastructure sector on services provided by another sector (e.g., water systems dependent on electric power). Business continuity planning should identify critical dependencies, assess the impact of disruption of dependent infrastructure, develop mitigation strategies including redundancy and backup systems, and coordinate with infrastructure partners on resilience planning. Scenario-based testing should include scenarios involving disruption of dependent infrastructure.

FAQ 4: How frequently should critical infrastructure organizations test their business continuity plans?

NERC CIP standards generally require annual testing of backup and recovery systems at minimum. CISA guidance recommends more frequent testing, typically quarterly or semi-annual for critical systems. CIRCIA and sector-specific requirements may require annual resilience assessments including testing. Most critical infrastructure organizations conduct continuous or frequent component testing plus annual or semi-annual full-scale exercises to ensure comprehensive testing coverage.

FAQ 5: What is the role of Sector-Specific Agencies in critical infrastructure continuity?

Sector-Specific Agencies (such as Department of Energy for energy sector, EPA for water sector, etc.) develop sector-specific requirements, coordinate with industry on resilience initiatives, and often serve as regulatory authority for sector-specific requirements. They work with CISA to ensure coherent federal approach to critical infrastructure resilience, and many conduct resilience assessments and exercises within their sectors.

FAQ 6: How should critical infrastructure organizations address supply chain risk in business continuity planning?

Supply chain risk should be addressed through comprehensive assessment of critical suppliers and vendors, evaluation of their resilience and continuity capabilities, development of contractual requirements specifying resilience expectations, regular auditing of supplier compliance with continuity requirements, and identification of alternative suppliers for critical products and services. Organizations should maintain strategic inventory of critical materials and establish relationships with backup suppliers to mitigate supply chain disruptions.

Publisher: Continuity Hub | Published: March 18, 2026

For more information about critical infrastructure regulatory compliance, explore our comprehensive resources on Regulatory Compliance.

Healthcare Continuity Compliance: CMS Emergency Preparedness, Joint Commission, and HIPAA

Source: <https://continuityhub.org/healthcare-continuity-compliance-cms-joint-commission-hipaa/>

Published: March 18, 2026

Published: March 18, 2026 | Publisher: Continuity Hub

- Home
- Regulatory Compliance
- Healthcare Continuity Compliance: CMS Emergency Preparedness, Joint Commission, and HIPAA

Introduction: Healthcare Continuity and Patient Safety

Healthcare organizations operate under unique business continuity regulatory requirements driven by the fundamental imperative to protect patient safety and ensure uninterrupted access to emergency medical services. Unlike other sectors where service disruptions cause financial losses, healthcare disruptions directly threaten human life, necessitating comprehensive regulatory frameworks for continuity planning.

Healthcare Continuity Compliance: The adherence to federal and state regulatory requirements mandating that healthcare organizations develop, test, and maintain comprehensive emergency

preparedness and business continuity plans ensuring critical clinical services remain available during emergencies and disruptions, with particular emphasis on maintaining patient care delivery, protecting patient information, and coordinating with public health and emergency management authorities.

This guide explores the major regulatory frameworks governing healthcare business continuity, including requirements from the Centers for Medicare & Medicaid Services (CMS), The Joint Commission (TJC), the Health Insurance Portability and Accountability Act (HIPAA), and state health department requirements.

Centers for Medicare & Medicaid Services (CMS) Requirements

CMS establishes regulatory requirements for Medicare and Medicaid participating providers. CMS emergency preparedness requirements apply to hospitals, skilled nursing facilities, home health agencies, hospice organizations, ambulatory surgical centers, dialysis facilities, and other provider types.

CMS Regulatory Authority

CMS emergency preparedness requirements derive from:

- Social Security Act §1861(dd), which defines hospital conditions of participation
- 42 CFR Part 482 (Hospital Conditions of Participation)
- 42 CFR Part 483 (Requirements for States and Long Term Care Facilities)
- 42 CFR Part 460 (Home and Community-Based Services Waiver Program)
- 42 CFR Part 486 (Conditions of Participation for Dialysis Facilities)

CMS Emergency Preparedness Standards

CMS requires healthcare providers to establish comprehensive emergency preparedness programs addressing:

Emergency Preparedness Committee

- **Governance:** Senior leadership must establish and oversee emergency preparedness planning
- **Cross-Functional Participation:** Committee must include representatives from clinical, operations, IT, and administrative departments
- **External Coordination:** Integration with community emergency response organizations and public health agencies
- **Regular Meetings:** Committee must meet at least quarterly to review and update plans

Emergency Operations Plan

- **Scope:** Comprehensive plan addressing all-hazards emergency scenarios affecting healthcare operations
- **Command Structure:** Establishment of incident command structure with clear lines of authority
- **Continuity of Operations:** Procedures ensuring continued delivery of essential patient care services during emergencies

- **Staff Roles and Responsibilities:** Clear assignment of emergency roles and responsibilities to staff members
- **Utility Failures:** Procedures addressing loss of utilities (power, water, gas, communications)
- **Staffing and Supplies:** Plans for maintaining staffing and supplies during prolonged disruptions
- **Patient Evacuation:** Procedures for orderly patient evacuation if facility becomes untenable

Communication Plan

- **Internal Communications:** Systems for communicating with staff regarding emergency status and assignments
- **External Communications:** Procedures for communicating with patients, families, media, and emergency management authorities
- **Backup Communications:** Redundant communication systems available if primary systems fail
- **Alert System:** Methods for rapidly notifying staff of emergencies and recall procedures

Cybersecurity in Emergency Preparedness

- **IT Recovery:** Plans for recovery of critical IT systems supporting patient care and clinical decision-making
- **Data Backup:** Procedures for protecting patient data and maintaining ability to access records during disruptions
- **Ransomware Response:** Specific procedures addressing ransomware attacks and system recovery
- **Testing Requirements:** Regular testing of IT recovery capabilities and backup systems

Training and Drills

- **Annual Training:** All staff must receive training in emergency preparedness roles and procedures annually
- **Facility Drills:** Full-scale exercises involving the entire facility at least annually
- **Departmental Drills:** Departmental or unit-level drills focusing on specific scenarios and procedures
- **Documentation:** Training attendance and drill participation must be documented

CMS Survey and Enforcement

CMS conducts unannounced surveys of Medicare-participating hospitals and other providers, specifically evaluating emergency preparedness compliance. Survey focus includes:

- Existence and currency of written emergency operations plan
- Evidence of regular committee meetings and plan updates
- Documentation of training and drill participation
- Ability to demonstrate command structure and staff understanding of emergency roles
- Adequacy of utility backup systems (generators, water storage, etc.)
- IT recovery capabilities and backup procedures

Deficiencies in emergency preparedness can result in Condition Level findings, leading to termination of Medicare participation if not remediated.

The Joint Commission (TJC) Standards

The Joint Commission is an independent, nonprofit organization that accredits and certifies nearly 21,000 healthcare organizations. TJC emergency management standards are enforceable conditions for accreditation.

TJC Emergency Management Standards

TJC Standards address emergency management across healthcare organizations, including hospitals, ambulatory care centers, and long-term care facilities.

Emergency Planning (EM.01.01)

- **Policy and Procedures:** Comprehensive written policies and procedures for emergency management
- **All-Hazards Approach:** Plans must address natural disasters, technological hazards, human-caused incidents, and pandemic/biological threats
- **Coordination with Community:** Integration with community emergency response and public health agencies
- **Regular Review:** Plans must be reviewed and updated at least annually and after any actual emergency event

Incident Command System (EM.01.02)

- **Organizational Structure:** Incident command system or equivalent structure for managing emergency response
- **Roles and Responsibilities:** Clear definition of roles and responsibilities for all emergency management positions
- **Chain of Command:** Clear lines of authority and succession planning for emergency leadership
- **Staff Awareness:** All staff should understand the incident command structure and their roles

Utility Systems Management (EM.02.01)

- **Emergency Power:** Emergency generator systems with capacity to support all critical operations
- **Generator Maintenance:** Regular maintenance, testing, and inspection of generator systems
- **Fuel Management:** Adequate fuel supply to support extended power outages (minimum 48 hours on-site, supply contracts for additional)
- **Utility Monitoring:** Systems to monitor utility availability and automatically switch to backup systems

Communication Systems (EM.02.02)

- **Emergency Communications:** Redundant communication systems for emergency communications
- **Staff Alert System:** Procedures for rapid notification and recall of staff during emergencies

- **External Communications:** Protocols for communicating with external agencies and media

Training and Exercises (EM.03.01)

- **Initial Training:** All new staff receive emergency preparedness training during orientation
- **Annual Training:** All staff receive refresher training annually addressing their emergency roles
- **Full-Scale Exercises:** At least one facility-wide exercise annually involving all departments
- **Targeted Drills:** Additional drills addressing specific scenarios or departments

TJC Accreditation Surveys

TJC surveyors evaluate emergency management during accreditation surveys, with specific focus on:

- **Currency and appropriateness of emergency operations plans**
- **Incident command structure and staff understanding of emergency roles**
- **Utility systems and generator testing and maintenance records**
- **Training records and attendance documentation**
- **Drill participation and exercise after-action reports**

Accreditation can be withheld or revoked if emergency management standards are not met.

HIPAA Security and Contingency Planning Requirements

The Health Insurance Portability and Accountability Act (HIPAA) establishes federal standards for privacy and security of protected health information. HIPAA's Security Rule includes specific requirements for contingency planning and business continuity.

HIPAA Contingency Planning Requirements

HIPAA Security Rule 45 CFR §164.308(a)(7) requires covered entities to establish and implement policies and procedures to address emergency access to electronic protected health information (ePHI) and to ensure that ePHI is properly protected during emergencies.

Data Backup Plan

- **Regular Backups:** Automated daily or more frequent backups of all ePHI and critical systems
- **Backup Storage:** Backup data stored separately from primary systems and facilities to protect against facility-wide disasters
- **Backup Testing:** Regular testing to ensure backups are complete and can be successfully restored
- **Offsite Storage:** Secure offsite storage of backup media with appropriate access controls and encryption

Disaster Recovery Plan

- **System Recovery:** Detailed procedures for recovering critical systems and data within acceptable timeframes
- **Alternative Processing:** Plans for continuing operations if primary processing facilities are destroyed or inaccessible

- **Testing Requirements:** Annual testing of disaster recovery procedures to ensure operability
- **Recovery Priorities:** Prioritization of system recovery based on criticality to patient care

Emergency Access Procedures

- **Access During Emergencies:** Procedures ensuring authorized staff can access ePHI during emergencies despite system failures
- **Temporary Procedures:** Manual or temporary procedures for accessing, maintaining, and transmitting ePHI if systems are unavailable
- **Documentation:** Procedures for documenting emergency access for audit trail purposes
- **Termination of Emergency Access:** Procedures for terminating emergency access procedures once normal operations are restored

Testing and Evaluation

- **Annual Testing:** Contingency plan must be tested at least annually
- **Testing Documentation:** Results of testing must be documented including any failures or deficiencies
- **Remediation:** Identified deficiencies must be remediated before plan is considered adequate
- **Plan Updates:** Plans must be updated based on testing results and organizational changes

HIPAA Business Associate Contracts

Covered entities must ensure that business associates (vendors and service providers handling ePHI) maintain equivalent security and contingency planning. Business Associate Agreements must require:

- **Implementation of required security measures and contingency planning**
- **Regular testing of contingency plans with results provided to covered entity**
- **Notification procedures for security incidents affecting ePHI**
- **Destruction or return of ePHI when services end**

HIPAA Enforcement

HIPAA compliance is enforced by the Department of Health and Human Services Office for Civil Rights (OCR). HIPAA violations can result in:

- **Civil monetary penalties ranging from \$100 to \$50,000 per violation**
- **Criminal penalties for willful neglect of HIPAA requirements**
- **Corrective action requirements and ongoing monitoring**

Integrating CMS, Joint Commission, and HIPAA Requirements

Overlapping Requirements

CMS emergency preparedness, Joint Commission emergency management, and HIPAA contingency planning requirements are substantially aligned, allowing organizations to develop a unified emergency preparedness and business continuity program satisfying all three frameworks. Key alignment areas

include:

- Emergency operations planning addressing all-hazards scenarios
- Training and drill requirements for all staff
- Generator and utility backup requirements
- Communication system redundancy
- Data backup and IT recovery procedures
- Annual testing and documentation requirements

Integrated Program Development

Effective healthcare emergency preparedness programs integrate CMS, TJC, and HIPAA requirements into a unified framework:

- Establish single emergency operations plan addressing requirements of all three frameworks
- Develop unified training program covering all required competencies
- Implement comprehensive drill and exercise schedule satisfying all testing requirements
- Maintain centralized documentation demonstrating compliance with all frameworks
- Assign clear accountability for program administration and maintenance

State and Local Requirements

In addition to federal requirements, healthcare organizations must comply with state-specific emergency preparedness requirements, which may include:

State Health Department Requirements

- State-mandated emergency preparedness planning requirements
- State-specific licensing and certification conditions
- State emergency management integration requirements
- State-specific hazard planning (e.g., hurricane preparedness in coastal states)

Local Emergency Management Coordination

- Memoranda of understanding with local emergency management and public health agencies
- Participation in community emergency response plans
- Integration with local mutual aid agreements and resource sharing
- Regular coordination with emergency managers and public health officials

Pandemic and Biological Threat Planning

CMS emergency preparedness requirements and TJC standards specifically address pandemic planning and biological threat scenarios. Healthcare organizations must have plans addressing:

Pandemic Preparedness

- **Infection Control:** Isolation and quarantine procedures for infectious disease patients
- **Personal Protective Equipment (PPE):** Stockpiles and supply chain plans for adequate PPE
- **Staffing:** Plans for maintaining staffing despite illness absence rates
- **Surge Capacity:** Procedures for expanding patient capacity during pandemic surges
- **Triage Protocols:** Ethical frameworks for allocating scarce resources (ventilators, ICU beds)

Communication During Pandemics

- **Public health coordination and communication**
- **Staff communication regarding infection control measures**
- **Patient communication regarding visiting restrictions and isolation procedures**
- **Community communication regarding facility status and patient acceptance**

Interrelationships with Business Continuity Planning and Risk Assessment

Healthcare continuity compliance builds upon fundamental frameworks covered in related guides:

- **Business Continuity Planning: Complete Professional Guide** provides foundational BC&DR planning principles applicable within healthcare regulatory frameworks
- **Risk Assessment: Complete Professional Guide** details business impact analysis processes essential for healthcare emergency preparedness planning
- **Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026)** surveys regulatory requirements across all sectors
- **Operational Resilience: Complete Professional Guide** explores emerging frameworks emphasizing operational resilience in healthcare settings

Frequently Asked Questions

FAQ 1: What is the difference between CMS and Joint Commission emergency preparedness requirements?

CMS establishes federal regulatory requirements for Medicare and Medicaid participating providers through conditions of participation. These are enforceable requirements, and violations can result in loss of Medicare/Medicaid participation. Joint Commission establishes accreditation standards for organizations seeking TJC accreditation. While the requirements are substantially similar, CMS requirements are mandatory for Medicare/Medicaid participation, while TJC requirements apply only to accredited organizations. Many hospitals pursue both Medicare participation and TJC accreditation, so they must meet both sets of requirements.

FAQ 2: How often should healthcare organizations conduct emergency preparedness drills?

Both CMS and TJC require at least one facility-wide full-scale exercise annually. Additionally, organizations should conduct departmental drills and targeted exercises addressing specific scenarios at more frequent intervals. Best practice suggests quarterly or semi-annual exercises in addition to the

annual full-scale drill. Exercises should vary scenario types to test different emergency response procedures and ensure all departments understand their emergency roles.

FAQ 3: What backup power systems are required by CMS and TJC?

Both CMS and TJC require emergency power systems (typically diesel generators) with capacity to support all critical operations. Generators must be tested regularly (typically monthly or quarterly), maintained in operational condition, and have sufficient fuel supply on-site. Standards typically require minimum 48 hours of fuel on-site, with contracts or agreements for additional fuel supply during extended outages. Testing procedures and maintenance records must be documented and available for survey.

FAQ 4: How should healthcare organizations approach HIPAA contingency planning compliance?

HIPAA contingency planning requirements should be integrated with overall emergency preparedness planning. Key elements include automated daily backups of all ePHI, offsite secure storage of backup media, documented procedures for disaster recovery and emergency access to ePHI, and annual testing of contingency plans with documented results. Organizations should maintain comprehensive documentation of all contingency planning activities demonstrating compliance with HIPAA requirements.

FAQ 5: What are state and local coordination requirements for healthcare emergency preparedness?

Healthcare organizations should establish coordination with state health departments and local emergency management agencies through memoranda of understanding (MOUs) that address information sharing, mutual aid, resource coordination, and emergency response integration. Organizations should participate in community emergency response planning and exercises, and should maintain regular communication with public health and emergency management officials to ensure alignment of healthcare emergency preparedness with community emergency plans.

FAQ 6: How should healthcare organizations address pandemic preparedness requirements?

Pandemic preparedness is specifically addressed in CMS and TJC standards. Organizations should develop detailed plans addressing infection control measures, PPE supply and stockpiling, staffing procedures for managing illness-related absences, surge capacity procedures for expanding patient care capacity, and ethical frameworks for allocating scarce resources. Plans should be tested and updated regularly, and should be coordinated with public health agencies and community pandemic plans.

Publisher: Continuity Hub | Published: March 18, 2026

For more information about healthcare regulatory compliance, explore our comprehensive resources on Regulatory Compliance.

Related: Hub: Regulatory Compliance for Business Continuity: The Complete Professional Guide (2026). Continuity Hub home.

Financial Services Continuity Regulation: OCC, FFIEC, SEC, and Basel Requirements

Source: <https://continuityhub.org/financial-services-continuity-regulation-occ-ffiec-sec-basel/> Published: March 18, 2026

Published: March 18, 2026 | Publisher: Continuity Hub

- Home
- Regulatory Compliance
- Financial Services Continuity Regulation: OCC, FFIEC, SEC, and Basel Requirements

Introduction: The Financial Services Regulatory Framework

Financial institutions face the most comprehensive and exacting business continuity regulatory requirements of any sector. These requirements stem from the systemic importance of financial institutions, the interconnected nature of modern financial systems, and the critical need for uninterrupted access to capital markets, payment systems, and credit facilities.

Financial Services Continuity Regulation: The comprehensive set of federal and international regulatory requirements mandating that banks, investment firms, market infrastructure providers, and other financial institutions develop, maintain, test, and document business continuity and disaster recovery plans that ensure critical financial services remain available during disruptions and can be restored within specified time frames, with explicit approval of recovery objectives and demonstrated testing of recovery capabilities.

This guide explores the major regulatory frameworks governing financial services business continuity, including requirements from the Office of the Comptroller of the Currency (OCC), the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC), the Federal Reserve Board, and international standards from the Basel Committee on Banking Supervision.

Office of the Comptroller of the Currency (OCC) Requirements

The OCC regulates and supervises national banks and federal savings associations. OCC guidance on business continuity is contained in OCC Bulletin 2013-26, “Business Continuity Planning,” which supersedes and consolidates prior guidance.

OCC Regulatory Authority

The OCC’s authority to require business continuity planning derives from:

- 12 U.S.C. § 93a (Safety and Soundness), which permits the OCC to prescribe regulations to ensure safety and soundness of national banks

- Gramm-Leach-Bliley Act (GLBA) §501(b), which requires financial institutions to establish administrative, technical, and physical safeguards including business continuity planning
- The Bank Service Company Act (12 U.S.C. § 1867(c)), which extends safety and soundness requirements to service providers

OCC Business Continuity Requirements

OCC guidance requires national banks to establish business continuity planning addressing:

Planning Requirements

- **Senior Management Oversight:** Board of Directors and executive management must approve business continuity strategies and policies
- **Business Impact Analysis:** Formal assessment identifying critical functions, interdependencies, and recovery priorities
- **Recovery Objectives:** Explicit Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical functions, approved by senior management
- **Geographic Redundancy:** Facilities and processing resources located in geographically separated locations to address location-dependent disruptions
- **Supplier and Vendor Management:** Business continuity agreements with all critical service providers specifying continuity capabilities and testing requirements

Testing Requirements

- **Annual Full-Scale Testing:** At minimum, annual tests involving all critical business lines and support functions, including recovery site activation
- **Quarterly Component Testing:** Testing of critical systems and procedures on a quarterly basis at minimum
- **Third-Party Testing:** Annual testing of critical third-party service providers' continuity capabilities
- **Documentation of Results:** Comprehensive documentation of all testing activities, results, deficiencies, and corrective actions

Customer Notification and Communications

- Policies and procedures for communicating with customers regarding operational disruptions
- Communication protocols with regulatory authorities during actual disruptions
- Media and public communications planning for significant disruptions

OCC Examination Focus

During regular examinations, OCC examiners evaluate:

- Adequacy of business continuity planning relative to institution size and complexity
- Appropriateness of recovery objectives based on function criticality
- Effectiveness of testing programs and remediation of identified deficiencies
- Management's commitment to maintaining adequate continuity capabilities

- Ability to recover within approved RTOs and RPOs based on testing results

Federal Financial Institutions Examination Council (FFIEC) Guidance

The FFIEC is an interagency body comprising representatives of the Federal Reserve Board, OCC, FDIC, Consumer Financial Protection Bureau (CFPB), and state banking regulators. FFIEC guidance is typically coordinated across these agencies, providing consistent expectations to supervised institutions.

FFIEC Business Continuity Guidance

FFIEC guidance documents provide detailed expectations for business continuity planning, including:

Business Continuity Planning (BCP) Guidance

- Comprehensive planning framework addressing all business lines and support functions
- Regular plan updates and maintenance procedures
- Appropriate recovery site locations and facilities
- Data backup and recovery procedures ensuring RPO achievement
- Cybersecurity considerations in continuity planning

Disaster Recovery (DR) Planning

- Focus on technology systems critical to business operations
- Redundant systems and backup procedures
- Testing of recovery procedures and failover mechanisms
- Documentation of system dependencies and recovery sequences

Third-Party Risk Management

- Ongoing due diligence of critical service providers' continuity capabilities
- Contractual requirements for business continuity service levels
- Periodic audit and testing of third-party capabilities
- Contingency arrangements for critical services

FFIEC Interagency Examination Procedures

FFIEC examination procedures guide examiners across all federal banking agencies in evaluating business continuity programs. These procedures address:

- Assessment of planning procedures and documentation
- Evaluation of recovery objectives appropriateness
- Review of testing schedules and results
- Assessment of corrective actions taken to address deficiencies
- Evaluation of third-party due diligence processes

Securities and Exchange Commission (SEC) Requirements

The SEC regulates investment advisers, broker-dealers, national securities exchanges, clearing agencies, and other market participants. SEC requirements for business continuity derive from Rule 17a-4 and related provisions of the Securities Exchange Act of 1934.

SEC Business Continuity Requirements

SEC requirements for broker-dealers and investment advisers include:

Written Business Continuity Plan

- **Plan Scope:** Plans must address all material aspects of business operations and must be customized to the specific business model
- **Disaster Recovery:** Specific procedures for recovery of critical technology systems supporting trading, clearing, and settlement
- **Financial Records Recovery:** Procedures ensuring recovery of financial records and books within specified time frames
- **Notification Procedures:** Procedures for notifying customers, counterparties, exchanges, and other regulatory agencies

Plan Maintenance and Testing

- Annual review and update of business continuity plans
- Annual testing of business continuity procedures
- Testing must validate ability to meet all plan objectives within required timeframes
- Documentation of testing results and corrective actions

Specific SEC Guidance for Market Infrastructure

- **Exchanges and Clearing Agencies:** Rules 11a-1 and 17a-1 establish enhanced requirements for market infrastructure providers
- **Recovery Time Objective:** Recovery of critical systems within 1 hour is industry standard for equities trading platforms
- **Redundancy Requirements:** Geographic dispersal of processing capabilities and data backup facilities
- **Alternative Trading Systems (ATS):** Must comply with Regulation SHO and maintain business continuity procedures comparable to registered exchanges

Regulatory Filings and Notifications

SEC rules require firms to:

- File Form BD updates when business continuity plans materially change
- Report any operational disruptions affecting customer services or financial market integrity
- Provide business continuity plan summaries during regulatory examinations

Federal Reserve Board Requirements

The Federal Reserve Board regulates and supervises state member banks, bank holding companies, and certain financial services holding companies. The Federal Reserve has issued guidance on business continuity planning that is coordinated with OCC and FDIC guidance.

Recovery and Resolution Planning

For large financial institutions, the Federal Reserve implemented enhanced requirements for “recovery and resolution planning” (commonly called “living wills”) under section 165(d) of the Dodd-Frank Act.

Recovery Planning Requirements

- **Recovery Plan:** Detailed plans identifying how the organization would recover from stress scenarios through internal measures such as asset sales, funding adjustments, or operational changes
- **Rapid Recovery Options:** Pre-identified actions and capability to implement within 30 days to address operational stress
- **Business Line and Jurisdictional Analysis:** Identification of critical business lines and key dependencies by jurisdiction
- **Funding Resilience:** Procedures for accessing contingency funding and maintaining liquidity during stress scenarios

Resolution Planning Requirements

- **Orderly Resolution:** Plans for orderly resolution under bankruptcy or other legal insolvency proceedings
- **Critical Infrastructure Continuity:** Identification of critical operations that must be maintained for financial system stability
- **Operational Resilience:** Procedures ensuring critical operations remain available during resolution proceedings

Operational Resilience Guidance

The Federal Reserve has issued guidance on operational resilience expectations, including:

- **Impact tolerance thresholds** defining maximum acceptable service degradation
- **Scenario-based resilience testing** including cyber and operational scenarios
- **Third-party and interdependency resilience management**
- **Governance structures** ensuring executive accountability for operational resilience

Basel Committee on Banking Supervision Standards

The Basel Committee on Banking Supervision, coordinating banking regulators from major economies, has issued international standards for business continuity and operational resilience that influence supervisory approaches globally.

Basel Committee Principles

The Basel Committee has established principles for sound business continuity management in banking:

Board and Management Responsibilities

- **Board of Directors oversight of business continuity strategy and risk tolerance**
- **Executive management responsibility for business continuity program implementation**
- **Adequate resources and skilled personnel assigned to continuity functions**
- **Regular reporting to board regarding continuity program status and testing results**

Risk Assessment and Business Impact Analysis

- **Comprehensive identification of critical business functions and interdependencies**
- **Assessment of potential disruption scenarios affecting different business areas**
- **Quantification of business impact of service disruptions**
- **Establishment of recovery objectives based on impact analysis**

Planning, Testing, and Maintenance

- **Comprehensive business continuity plans addressing all critical operations**
- **Regular testing of plans at frequency appropriate to risk profile**
- **Full-scale tests including actual recovery site activation at least annually**
- **Regular plan updates reflecting organizational and operational changes**

Communication and Training

- **Clear communication of employee roles and responsibilities during disruptions**
- **Regular training for employees in their continuity roles**
- **Communication protocols with customers, counterparties, and regulatory authorities**
- **Public disclosure of material business continuity capabilities**

Operational Resilience Framework

The Basel Committee released guidance on “operational resilience” as evolution of traditional business continuity frameworks:

- **Impact Tolerance:** Organizations should define the maximum tolerable impact (in terms of service degradation duration or magnitude) that can be sustained during severe but plausible disruptions
- **Scenario-Based Testing:** Testing should use scenarios representing severe but plausible operational disruptions, including multiple-week outages and concurrent disruptions
- **Third-Party Resilience:** Organizations must assess and manage resilience of critical third parties and interdependencies
- **Regulatory Expectations:** Regulators expect organizations to operate within impact tolerance thresholds and to demonstrate resilience through realistic testing

Critical Business Functions and Recovery Priorities

Financial institutions must identify and prioritize critical business functions based on business impact analysis. Typical critical functions include:

Revenue-Generating Functions

- Trading and market-making operations
- Lending and credit services
- Deposit-taking and customer account services
- Asset management and investment advisory services

Critical Operations and Support Functions

- Payment and settlement processing
- Clearing and custody operations
- Financial reporting and regulatory compliance systems
- Risk management and internal audit functions

Recovery Objectives

Organizations establish recovery objectives for critical functions based on business impact. Typical RTOs range from:

- Tier 1 (Critical): 4-8 hours for revenue-generating functions and critical payment systems
- Tier 2 (Important): 24 hours for important but non-critical support functions
- Tier 3 (Standard): 72 hours or more for less critical functions

RPOs typically mandate full recovery within 24 hours for most critical functions, with some requiring real-time or near-real-time data recovery.

Regulatory Examination and Compliance Assessment

Examination Scope

During regulatory examinations, examiners evaluate:

- Completeness and accuracy of business continuity plans and supporting documentation
- Appropriateness of recovery objectives relative to function criticality
- Adequacy of backup facilities and redundant systems
- Effectiveness of testing programs
- Remediation of deficiencies identified in previous examinations or testing
- Third-party due diligence and vendor management procedures

Regulatory Findings and Corrective Actions

When examiners identify deficiencies in business continuity programs, they issue findings requiring corrective action. Common findings include:

- Inadequate recovery objectives not reflecting business impact
- Insufficient testing frequency or scope
- Failure to update plans for organizational changes
- Inadequate third-party continuity agreements
- Inability to demonstrate RTO achievement through testing

Regulatory agencies expect expeditious remediation of identified deficiencies, typically within 30-90 days depending on severity.

Interrelationships with Risk Assessment and Business Continuity Planning

Financial services business continuity regulations build upon fundamental frameworks covered in related guides:

- **Risk Assessment:** Complete Professional Guide details the business impact analysis processes essential for determining recovery objectives and testing priorities
- **Business Continuity Planning:** Complete Professional Guide provides foundational BC&DR planning principles applicable within financial services regulatory frameworks
- **Regulatory Compliance for Business Continuity:** The Complete Professional Guide (2026) surveys regulatory requirements across all major sectors
- **Operational Resilience:** Complete Professional Guide explores emerging operational resilience frameworks that will complement or supersede traditional BC&DR requirements

Frequently Asked Questions

FAQ 1: What is the difference between OCC and Federal Reserve business continuity requirements?

The OCC regulates national banks and federal savings associations, issuing business continuity requirements through OCC Bulletin 2013-26. The Federal Reserve regulates state member banks and bank holding companies, issuing coordinated guidance aligned with OCC requirements. The guidance is substantially similar, though the Federal Reserve emphasizes recovery and resolution planning for large institutions subject to Dodd-Frank requirements. Both agencies conduct examinations of business continuity programs and expect comparable capabilities across institutions of similar size and complexity.

FAQ 2: How should financial institutions determine appropriate recovery time objectives?

Recovery time objectives should be determined through formal business impact analysis examining the financial, operational, and reputational consequences of service disruption for each critical function. The analysis should quantify losses at different durations (e.g., loss per hour at 4 hours, 8 hours, 24 hours, 72

hours). RTOs should be set at the maximum disruption duration the organization can absorb without unacceptable business impact, then approved by senior management or the board. RTOs must be validated through testing demonstrating the organization can actually achieve recovery within the approved timeframe.

FAQ 3: What is the difference between SEC and banking regulator business continuity requirements?

Banking regulators (OCC, Federal Reserve, FDIC) focus on overall business continuity and disaster recovery for financial institutions, emphasizing testing and third-party management. The SEC focuses specifically on technology systems supporting trading, clearing, and settlement, as well as financial records recovery. For organizations subject to both regimes (e.g., broker-dealer subsidiaries of banks), both sets of requirements apply and must be integrated into a comprehensive business continuity program.

FAQ 4: How frequently should critical third-party service providers be tested?

Regulatory guidance requires testing of critical third-party continuity capabilities at least annually. However, organizations should consider testing frequency based on the criticality of the service and the third party's risk profile. Some organizations test critical service providers semi-annually or quarterly. Testing may be conducted by the third party independently and results provided to the organization, or by the organization itself. Results should be documented and reviewed with senior management to assess whether the third party's capabilities meet requirements.

FAQ 5: What role does geographic redundancy play in meeting regulatory requirements?

Geographic redundancy is fundamental to meeting financial services regulatory requirements. Regulatory guidance expects critical processing facilities to be located in geographically separated locations (typically at least 50 miles apart) to ensure that location-dependent disruptions do not affect both primary and backup facilities simultaneously. Geographic redundancy should extend to power supplies, telecommunications, and personnel to ensure comprehensive resilience. The specific geographic separation requirements depend on organizational risk profile and critical business functions, but organizations should demonstrate through testing that recovery can be achieved from a realistic disruption scenario.

FAQ 6: How should financial institutions approach recovery and resolution planning required under Dodd-Frank?

Dodd-Frank recovery and resolution planning, commonly called "living wills," requires large financial institutions to develop detailed plans for orderly resolution if the institution becomes insolvent. Recovery planning addresses how the institution would recover from severe stress scenarios through internal measures. Resolution planning addresses how critical operations would be maintained if the institution entered bankruptcy or receivership. These requirements build on traditional business continuity planning but extend to legal and operational challenges of resolving a large complex financial institution. Organizations should integrate recovery and resolution planning with traditional business continuity planning to ensure comprehensive operational resilience.

Publisher: Continuity Hub | Published: March 18, 2026

For more information about financial services regulatory compliance, explore our comprehensive resources on Regulatory Compliance.

EU DORA Compliance: Digital Operational Resilience for Financial Services

Source: <https://continuityhub.org/eu-dora-compliance-digital-operational-resilience-financial-services/>

Published: March 18, 2026

Published on March 18, 2026 | Updated: March 18, 2026

Publisher: Continuity Hub

Home > Operational Resilience > EU DORA Compliance

EU DORA Definition

EU DORA (Digital Operational Resilience Act) is European Union legislation that took full effect on January 17, 2025, establishing comprehensive requirements for digital operational resilience across the EU financial sector. DORA applies to banks, investment firms, insurance companies, and other financial entities operating in or serving EU customers. The regulation mandates establishment of Information and Communications Technology (ICT) risk management frameworks, reporting of major ICT incidents, digital operational resilience testing (DORT) including advanced methods like red-team testing, governance of critical ICT third-party service providers, and documentation of critical functions and important data assets. DORA represents the EU's primary legal framework for operational resilience and supersedes or supplements previous guidance, creating binding obligations for all covered financial institutions.

Overview of EU DORA

The Digital Operational Resilience Act represents a fundamental shift in how EU financial regulators approach digital resilience. Adopted by the European Commission following the COVID-19 pandemic and escalating cyber threats, DORA establishes minimum standards for all financial institutions in the EU and significantly elevates digital resilience as a regulatory priority.

DORA compliance became mandatory on January 17, 2025, creating immediate obligations for all covered financial institutions. The regulation takes a comprehensive approach covering ICT risk management, incident reporting, testing methodologies, third-party risk management, and governance structures. Unlike some regulatory guidance that is subject to interpretation, DORA is binding law with enforcement mechanisms and potential penalties for non-compliance.

Scope and Applicability

Covered Financial Institutions

DORA applies to a broad range of financial entities including:

- Credit institutions (banks)
- Investment firms (brokers, traders)
- Insurance and reinsurance undertakings
- Pension funds
- Asset managers
- Credit rating agencies
- Centrally authorized payment institutions
- E-money institutions

Scope Thresholds

Some DORA requirements apply differently based on organization size and risk profile. Smaller institutions may have scaled application of certain requirements, but the core ICT risk management and incident reporting obligations apply broadly. Organizations operating in or serving EU customers must assess whether DORA applies to their operations.

DORA Requirements: The Five Pillars

Pillar 1: ICT Risk Management

DORA mandates establishment of comprehensive ICT risk management frameworks covering:

- **ICT Risk Identification:** Regular identification and assessment of ICT risks including cybersecurity threats, operational risks, and third-party dependencies
- **Risk Assessment:** Evaluation of impact and likelihood of identified ICT risks
- **Risk Mitigation:** Implementation of controls to reduce risk to acceptable levels
- **Monitoring and Reporting:** Ongoing monitoring of ICT risk indicators and escalation to senior management and boards

Organizations must document their ICT risk management framework, including policies, procedures, and governance structures. Assessment of cloud computing risks receives specific emphasis given the reliance of modern financial institutions on cloud service providers.

Pillar 2: ICT Incident Reporting

DORA establishes mandatory reporting requirements for major ICT incidents affecting critical functions or important data assets:

- **Major Incident Definition:** Incidents impacting the confidentiality, integrity, or availability of critical functions or important data for more than 15 minutes (or meeting financial impact thresholds)
- **Reporting Timeline:** Initial notification within 4 hours of discovery, detailed report within 1 business day
- **Reporting Recipients:** National financial authority, national cybersecurity authority, and affected customers

- **Documentation Requirements:** Detailed incident descriptions, timeline, remediation steps, and lessons learned

The reporting requirements represent significant elevation from previous guidance and obligate organizations to invest in incident detection, reporting, and documentation capabilities.

Pillar 3: Digital Operational Resilience Testing (DORT)

DORA mandates rigorous digital operational resilience testing including:

- **Scenario Testing:** Testing of critical functions and important data assets under realistic stress scenarios
- **Advanced Methods:** Red-team testing, penetration testing, and security assessment of ICT systems
- **Testing Frequency:** Regular testing appropriate to risk profile (at least annual for critical functions)
- **Third-Party Testing:** Assessment of critical third-party service providers' capabilities to deliver under stress
- **Documentation:** Comprehensive testing documentation demonstrating ongoing validation of resilience capabilities

See our comprehensive guide to operational resilience testing for detailed testing methodologies.

Pillar 4: Critical ICT Third-Party Services

DORA establishes governance requirements for critical ICT third-party service providers, including cloud service providers:

- **Identification:** Formal identification of critical ICT service providers based on importance to delivering critical functions
- **Contractual Requirements:** Service level agreements defining recovery objectives, testing requirements, and incident notification
- **Due Diligence:** Assessment of third-party capability to meet DORA requirements before engagement
- **Ongoing Monitoring:** Regular monitoring of third-party performance and compliance
- **Audit Rights:** Contractual rights to audit third-party operations and resilience capabilities
- **Contingency Planning:** Documented plans for transitioning away from critical third parties in event of service failure

The third-party governance requirements recognize that financial institutions' resilience depends fundamentally on resilience of critical service providers.

Pillar 5: Governance and Documentation

DORA requires establishment of governance structures and comprehensive documentation:

- **Board Accountability:** Board oversight of digital operational resilience strategy and regular reporting on ICT risk
- **Management Accountability:** Senior management responsibility for ICT risk management implementation

- **Critical Functions Documentation:** Identification and documentation of critical functions essential to financial services delivery
- **Important Data Assets:** Identification and protection of important data assets including customer data and financial records
- **Recovery Objectives:** Definition of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical functions
- **Mapping and Inventory:** Maintenance of detailed inventory of critical systems, infrastructure, and dependencies

Key Implementation Considerations

Timeline for Full Compliance

DORA became fully applicable on January 17, 2025. Organizations that were not compliant at that date face regulatory enforcement action. Implementation of DORA requirements typically requires 12-24 months depending on organization size and existing resilience capabilities. Organizations should have assessed compliance gaps and begun remediation efforts by now.

Integration with Existing Frameworks

DORA complements and extends other regulatory requirements including the Bank of England Operational Resilience Framework, Basel Committee guidelines, and existing cybersecurity regulations. Organizations should integrate DORA compliance into overall operational resilience programs rather than treating it as a separate initiative. See our Operational Resilience guide for comprehensive framework alignment.

Cloud Computing Considerations

DORA contains specific provisions governing use of cloud computing services. Financial institutions must assess cloud provider resilience capabilities, establish contractual requirements reflecting DORA obligations, and maintain ability to migrate away from cloud providers in event of service failure or regulatory concerns. Single cloud provider dependencies receive particular regulatory scrutiny.

Testing Under DORA

DORA's advanced testing requirements significantly exceed previous guidance. Organizations must move beyond basic tabletop exercises and scenario testing to include red-team testing and penetration testing. Our detailed testing guide covers DORA testing requirements comprehensively.

DORA Compliance Implementation Roadmap

Phase 1: Assessment (Months 1-2)

- Conduct compliance gap analysis against DORA requirements
- Identify critical functions and important data assets
- Assess current ICT risk management capabilities
- Inventory critical third-party service providers

Phase 2: Planning (Months 2-4)

- Develop ICT risk management framework and policies
- Establish incident reporting procedures and crisis communication protocols
- Design digital operational resilience testing program
- Develop third-party governance framework

Phase 3: Implementation (Months 4-18)

- Deploy ICT risk management systems and processes
- Conduct initial major incident reporting capability testing
- Execute digital operational resilience testing for critical functions
- Formalize critical third-party service provider contracts and SLAs
- Build governance and documentation infrastructure

Phase 4: Validation (Months 18-24)

- Validate compliance readiness through internal audit or external assessment
- Complete advanced testing (red-team exercises) for highest-criticality functions
- Demonstrate ongoing testing program and remediation of gaps
- Prepare for regulatory examination and reporting obligations

Regulatory Expectations and Enforcement

National financial regulators across the EU have published DORA guidance and supervisory expectations. Regulators expect:

- Demonstrated understanding of DORA requirements and applicability to organization
- Board-level commitment to digital operational resilience and adequate resourcing
- Comprehensive documentation of critical functions, recovery objectives, and third-party dependencies
- Evidence of regular digital operational resilience testing demonstrating capability to deliver critical functions under stress
- Robust incident reporting processes with demonstrated capability to detect and report major incidents
- Effective third-party governance with documented SLAs reflecting DORA requirements

Non-compliance can result in regulatory enforcement action, formal enforcement notices, fines, and reputational impact. Regulators have indicated DORA compliance will be a priority examination focus.

Integration with Related Frameworks

- Operational Resilience: The Complete Professional Guide – Core framework and requirements
- Important Business Services: Identification, Mapping, and Impact Tolerances – Critical functions identification

- **Operational Resilience Testing: Scenario Testing and Severe but Plausible Scenarios – Testing methodologies**
- **Disaster Recovery Planning: Complete Professional Guide – Recovery infrastructure planning**
- **Risk Assessment: Complete Professional Guide – ICT risk identification and assessment**

Key Takeaways

- EU DORA is binding law that took full effect January 17, 2025, establishing comprehensive digital operational resilience requirements
- DORA applies broadly to all EU financial institutions and requires board-level commitment
- Five pillars cover ICT risk management, incident reporting, testing, third-party governance, and documentation
- Advanced testing methodologies including red-team exercises are mandatory requirements
- Critical third-party service provider governance is essential given reliance on cloud and external providers
- Regulatory expectations are high, with examination focus and enforcement mechanisms for non-compliance

EU DORA Requirements: The Five Pillars and Who Must Comply (2026)

The EU Digital Operational Resilience Act (DORA) is a binding regulation that has applied directly across all 27 EU member states since 17 January 2025. It requires virtually every regulated EU financial entity, plus the critical ICT providers they depend on, to manage technology risk, report major ICT incidents on a strict clock, test their digital resilience, and control third-party risk under five mandatory pillars. In 2026, supervisors have moved from reviewing policies to enforcing them, demanding real-time, data-driven evidence of operational resilience rather than paperwork.

Pillar	What it requires	Key obligation
1. ICT Risk Management	A board-owned framework to identify, protect, detect, respond to, and recover from ICT risks across all critical and important functions.	Maintain an ICT risk management framework, including an ICT business continuity policy plus backup, restoration, and recovery procedures, reviewed at least annually.
2. ICT-Related Incident Reporting	Classify and report major ICT-related incidents to the competent authority on harmonized templates, with significant cyber threats reported voluntarily.	Meet the four-stage clock: initial notification within 4 hours of classification (and within 24 hours of detection), intermediate report within 72 hours, and final report within 1 month.
3. Digital Operational Resilience Testing	A risk-based testing program for all entities, escalating to advanced testing for those whose disruption would be systemically significant.	Run threat-led penetration testing (TLPT) on live systems supporting critical functions at least every 3 years for designated entities, using the TIBER-EU-aligned methodology.

Pillar	What it requires	Key obligation
4. ICT Third-Party Risk Management	Manage the full lifecycle of ICT outsourcing and enforce mandatory contractual clauses; designated critical providers fall under a new EU-level oversight regime.	Maintain a complete Register of Information on all ICT third-party arrangements; critical ICT third-party providers (CTPPs) are directly overseen by a Lead Overseer.
5. Information Sharing	Voluntary exchange of cyber threat intelligence, indicators of compromise, and best practices among trusted financial entities.	Participate in information-sharing arrangements within trusted communities, where doing so improves resilience without breaching confidentiality or data-protection rules.

Who Is in Scope and Key Dates

DORA covers roughly 20 categories of financial entity, including credit institutions (banks), payment and e-money institutions, investment firms, crypto-asset service providers, insurance and reinsurance undertakings, pension institutions, central counterparties, trading venues, central securities depositories, credit rating agencies, and crowdfunding service providers. It applies proportionately, so smaller entities are not held to the same intensity as major institutions, but the core obligations apply broadly.

DORA also reaches the technology supply chain. ICT third-party service providers that financial entities rely on are pulled in contractually, and those judged systemically important are formally designated as critical ICT third-party providers (CTPPs) under a dedicated EU-level oversight regime led by one of the three European Supervisory Authorities (EBA, ESMA, or EIOPA).

- 16 January 2023: DORA entered into force as EU Regulation 2022/2554.
- 17 January 2025: DORA began to apply; financial entities must be compliant from this date.
- 2025: The technical standards (RTS and ITS) underpinning incident reporting, the Register of Information, ICT risk management, and TLPT entered into application.
- 18 November 2025: The ESAs published the first official list of designated CTPPs (19 providers, including major cloud and data-service firms such as AWS, Microsoft, Google Cloud, IBM, and Bloomberg).
- 2026: Enforcement matures. National competent authorities and the ESAs conduct active supervisory reviews, the first annual oversight plans for designated CTPPs are issued, and the European Central Bank has integrated DORA into the SREP for significant institutions.

How DORA Connects to Business Continuity and Operational Resilience Programs

DORA is, in effect, EU law that mandates a digital operational resilience program for the financial sector. Its first pillar explicitly requires each financial entity to maintain an ICT business continuity policy with tailored response and recovery procedures, plus backup, restoration, and recovery measures, all integrated into the wider business continuity management (BCM) framework rather than run as a siloed IT exercise.

That makes DORA a regulatory backbone for business continuity and disaster recovery (BCDR) teams in scope. It aligns naturally with internationally recognized standards such as ISO 22301 (business continuity management) and ISO 27031 (ICT readiness for business continuity), and it pushes

organizations to prove resilience through testing, defined recovery time and recovery point objectives, and evidence of restoration, not just documented plans. For continuity and resilience leaders, DORA elevates ICT continuity from a technical control to a board-level, supervised obligation with reporting deadlines and audit-ready evidence requirements.

Frequently Asked Questions

When did DORA come into force?

DORA (EU Regulation 2022/2554) entered into force on 16 January 2023 and began to apply on 17 January 2025. Financial entities and their critical ICT providers have been required to comply since that 2025 application date, and 2026 marks the shift into active enforcement and supervisory review.

Who does DORA apply to?

DORA applies to roughly 20 categories of EU financial entity, including banks, payment and e-money institutions, investment firms, crypto-asset service providers, insurers and reinsurers, pension institutions, trading venues, central counterparties, central securities depositories, and credit rating agencies. It also reaches the ICT third-party providers these entities rely on, with the most systemically important designated as critical ICT third-party providers (CTPPs) under direct EU oversight.

What are the five pillars of DORA?

The five pillars are: (1) ICT risk management, (2) ICT-related incident reporting, (3) digital operational resilience testing (including threat-led penetration testing), (4) ICT third-party risk management with the critical-provider oversight regime, and (5) information sharing of cyber threat intelligence. Together they form a single framework for managing, testing, and reporting on technology risk across the financial sector.

What is TLPT under DORA?

TLPT stands for threat-led penetration testing, the most advanced form of resilience testing under DORA's third pillar. It uses real-world threat intelligence to drive red-team attack simulations against live production systems that support critical or important functions. Entities designated by their supervisors must conduct TLPT at least every 3 years, following a methodology aligned with the TIBER-EU framework.

Does DORA apply to non-EU firms?

Yes, DORA has extraterritorial reach. A non-EU financial entity operating in the EU through a branch or subsidiary is in scope, and ICT third-party providers based outside the EU are pulled in when their services are critical to EU financial entities. A non-EU provider designated as a critical ICT third-party provider must establish an EU-based subsidiary within 12 months of designation to continue serving EU financial institutions.

How does DORA differ from a directive like NIS2?

DORA is a regulation, so it applies directly and uniformly across all EU member states without needing national transposition, whereas a directive such as NIS2 must be written into each country's own law. DORA is also *lex specialis* for the financial sector: where its requirements overlap with broader

cybersecurity rules, DORA's sector-specific provisions take precedence for the financial entities it covers.

Frequently Asked Questions

When did EU DORA become effective and what organizations must comply?

EU DORA took full effect on January 17, 2025, and all covered financial institutions must be in compliance. Covered entities include banks, investment firms, insurance companies, pension funds, asset managers, credit rating agencies, payment institutions, and e-money institutions operating in or serving EU customers. Organizations not in compliance by the effective date may face immediate regulatory enforcement action.

What is the difference between DORA and the Bank of England Operational Resilience Framework?

DORA is binding EU law establishing minimum digital operational resilience requirements for all EU financial institutions. The Bank of England Operational Resilience Framework applies to UK financial institutions and establishes broader operational resilience requirements (not limited to digital/ICT aspects). EU institutions are subject to DORA; UK institutions follow Bank of England framework. Some requirements overlap (testing, impact tolerances), but DORA is broader in scope and more specific in digital operational resilience requirements including ICT risk management and incident reporting.

What are the major ICT incident reporting requirements under DORA?

Major ICT incidents affecting critical functions or important data assets must be reported within strict timelines: initial notification within 4 hours of discovery, detailed report within 1 business day. Major incidents include those lasting more than 15 minutes or meeting financial impact thresholds. Reporting must be made to national financial authority, national cybersecurity authority, and affected customers. This represents a significant elevation from previous guidance and requires robust incident detection and reporting infrastructure.

What does DORA require for critical ICT third-party service providers?

DORA requires identification of critical ICT service providers and establishment of governance frameworks including: contractual requirements defining service levels and recovery objectives, due diligence assessment before engagement, regular monitoring of performance and compliance, audit rights to assess resilience capabilities, and contingency planning for provider failure. For cloud service providers (which often qualify as critical providers), organizations must ensure contractual terms reflect DORA requirements and maintain ability to migrate away if necessary.

What testing methodologies does DORA require?

DORA mandates digital operational resilience testing (DORT) including advanced methodologies. Required testing approaches include scenario testing of critical functions, red-team testing, penetration

testing of ICT systems, and assessment of critical third-party capabilities. Testing frequency should be appropriate to risk profile with at least annual testing for critical functions. The requirement for advanced testing methodologies significantly exceeds previous regulatory guidance and represents a key implementation challenge for many organizations.

How should organizations handle DORA compliance if they use cloud providers?

DORA specifically addresses cloud computing. Organizations must identify which cloud services support critical functions, assess cloud provider resilience capabilities, and establish contractual requirements including service level agreements reflecting DORA obligations. Contracts should specify recovery objectives, testing rights, incident notification requirements, and exit provisions. Organizations must maintain ability to migrate from cloud providers if service resilience proves inadequate or regulatory concerns emerge. Given cloud provider concentration, regulators pay particular attention to single-provider dependencies.

What penalties apply for DORA non-compliance?

DORA non-compliance can result in regulatory enforcement action including formal enforcement notices, fines proportional to organization size and violation severity (potentially up to 10% of annual turnover for serious violations), requirement to implement remediation plans, and reputational damage. National regulators have indicated DORA compliance will be a priority examination focus. Non-compliance is not a minor regulatory matter; organizations should prioritize DORA implementation as a critical regulatory obligation.

© 2026 Continuity Hub (continuityhub.org). All rights reserved.

Category: Operational Resilience | ID: 7

Related: Hub: Operational Resilience: The Complete Professional Guide (2026). Continuity Hub home.

Risk Appetite, Tolerance, and Threshold Frameworks for Business Continuity

Source: <https://continuityhub.org/risk-appetite-tolerance-threshold-frameworks-business-continuity/>

Published: March 18, 2026

Home / Risk Assessment / Risk Appetite & Tolerance

Risk Appetite Definition: The amount and type of risk an organization is willing to accept to achieve strategic objectives, set by the board of directors. Risk tolerance is the acceptable variance around that appetite (e.g., “Target annual loss: \$500K; acceptable range: \$350K-650K”). Risk thresholds are operational limits that trigger escalation, mitigation, or executive decision (e.g., “Any single incident exceeding \$1M requires CFO approval”).

Why Risk Appetite Governance Matters for Business Continuity

Without explicit risk appetite, organizations face a governance vacuum. Recovery spending is either excessive (defensive over-investment in redundancy) or insufficient (hoping nothing bad happens). Business continuity teams operate in ambiguity: Are we doing enough? Too much?

The 2025 Board Governance & Risk Survey found that organizations with explicit, board-approved risk appetite statements achieve:

- 2.5x faster executive approval of recovery investments
- 40% higher consistency in recovery investment across business units
- 34% better business continuity-to-strategy alignment (recovery spending supports strategic objectives)
- 48% faster escalation and response to risks exceeding appetite

Risk appetite translates abstract board strategy (“We are a stable, risk-averse financial institution”) into concrete operational decisions. Example: Risk appetite of \$10M annual loss drives recovery investment decisions: “We will invest \$3M/year in recovery infrastructure to keep expected annual loss below \$10M threshold.”

Core Definitions: Appetite vs. Tolerance vs. Threshold

Risk Appetite

The amount of risk the board is willing to accept. Typically expressed as a strategic statement:

- **Conservative appetite:** “We prioritize stability and predictability. Annual loss should be minimized; we avoid high-impact, low-probability scenarios. Focus on cost-effective redundancy.”
- **Moderate appetite:** “We accept measured risk to support growth. We invest in recovery proportional to business value. Losses up to \$50M annually are acceptable if they support strategic initiatives.”
- **Aggressive appetite:** “We pursue growth aggressively. We accept higher operational risk in exchange for market speed. Annual losses up to \$100M+ are acceptable if outweighed by growth opportunity.”

Risk appetite is a board decision, not a risk team decision. It reflects organizational values and strategy. A fintech startup pursuing aggressive growth will have different appetite than a utility company managing critical infrastructure.

Risk Tolerance

The acceptable variance around risk appetite. While appetite is a target, tolerance acknowledges that actual outcomes vary. Tolerance bands define acceptable fluctuation:

Example:

- **Risk appetite:** \$50M annual loss (target)
- **Risk tolerance:** \$40M-60M (acceptable range)
- **Interpretation:** If actual annual loss falls between \$40M-60M, governance is on track. Below \$40M is over-cautious (unnecessary spending). Above \$60M requires investigation and response.

Tolerance bands reflect realistic uncertainty. Organizations cannot hit targets exactly; tolerance acknowledges this.

Risk Threshold

Operational limits that trigger specific actions (mitigation, escalation, executive decision). Thresholds are typically narrower than tolerance bands and cascade through the organization:

- **Green Zone (Below Threshold):** Risk is within acceptable range; routine monitoring
- **Yellow Zone (Caution):** Risk is elevated but not critical; enhanced monitoring, mitigation planning
- **Red Zone (Critical):** Risk exceeds appetite; immediate escalation and executive action required

Example thresholds for a \$50M annual loss appetite:

- **Green Zone:** Expected annual loss < \$35M
- **Yellow Zone:** Expected annual loss \$35M-50M
- **Red Zone:** Expected annual loss > \$50M (requires board approval to proceed)

Establishing Board-Level Risk Appetite

Board Accountability

Risk appetite is a board prerogative and responsibility. The Chief Risk Officer advises; the board decides. Key board activities:

- **Annual Risk Appetite Setting:** Board reviews organizational strategy and establishes risk appetite aligned with strategic objectives
- **Risk Appetite Communication:** Board communicates appetite to management through formal charter or policy
- **Appetite Monitoring:** Board receives quarterly reporting on whether actual risk is within appetite
- **Appetite Adjustment:** If strategy changes materially, board revisits and may adjust appetite

Framework for Setting Appetite

Risk appetite is typically defined across multiple dimensions:

1. Financial Risk Appetite

“What is the acceptable annual loss from operational incidents (data center failures, security breaches, supply chain disruption)?”

- **Conservative organization:** 0.1% of annual revenue (e.g., \$500M revenue -> \$500K acceptable loss)
- **Moderate organization:** 0.3-0.5% of annual revenue
- **Aggressive organization:** 1-2% of annual revenue

2. Operational Risk Appetite

“What is the acceptable downtime per year before system unavailability triggers escalation?”

- **Mission-critical systems:** 4 hours/year (99.95% availability)

- **Important systems:** 24 hours/year (99.73% availability)
- **Routine systems:** 168 hours/year (98.1% availability)

3. Reputational Risk Appetite

“What customer or regulator impact is acceptable? Under what circumstances do we proactively disclose incidents?”

- **Zero-tolerance:** Any customer data exposure requires disclosure
- **Threshold-based:** Disclosure required if >1% of customer base affected or >1,000 customers
- **Materiality-based:** Disclosure if incident threatens financial reporting or regulatory compliance

4. Recovery Time Appetite

“What is acceptable Recovery Time Objective (RTO) for critical systems?”

- **Payment processing:** 15 minutes RTO (world-class SLA)
- **Customer-facing systems:** 1-4 hours RTO (enterprise standard)
- **Internal tools:** 4-24 hours RTO (standard)

Board Appetite Documentation

Risk appetite must be documented and communicated. Typical format:

Risk Appetite Charter (Example)

Approved by Board of Directors, March 2026

Statement: Our organization pursues sustainable growth while maintaining operational stability. We accept measured risk to achieve strategic objectives.

Financial Appetite: Annual loss from operational incidents acceptable up to \$50M (1% of revenue). Expected loss should be maintained below \$35M through active mitigation.

Operational Appetite: Critical customer systems: <4 hours downtime/year. Important systems: <24 hours/year. Routine systems: <200 hours/year. **Reputational Appetite:** Zero tolerance for customer data exposure. Any suspected breach triggers investigation and, if confirmed, proactive disclosure within 72 hours.

Recovery Investment: We invest up to 4% of annual revenue in business continuity, disaster recovery, and risk mitigation to achieve this appetite.

Cascading Risk Appetite Through the Organization

From Board Appetite to Operational Thresholds

Board-level appetite must cascade into operational thresholds that guide business unit and functional decisions. This requires translation:

Board Appetite: “We accept \$50M annual loss”

Executive Thresholds (C-level):

- **Cybersecurity risk budget: \$15M/year (30% of appetite)**
- **Infrastructure risk budget: \$12M/year (24% of appetite)**
- **Supply chain risk budget: \$8M/year (16% of appetite)**
- **Operational risk budget: \$10M/year (20% of appetite)**
- **Reserve: \$5M/year (10% of appetite, for unknown/emerging risks)**

Operational Thresholds (Business Unit Level):

- **Finance systems downtime: Alert if >2 hours unplanned; escalate if >4 hours**
- **Customer database breach: Alert if <100 records exposed; escalate if >100**
- **Supplier disruption: Alert if single supplier unavailable >48 hours; escalate if >72 hours**

This cascade ensures board appetite translates into actionable guidance for managers.

Risk Appetite by Business Unit

Different business units may have different appetites aligned with their function:

Business Unit	Function	Risk Appetite	Rationale
Payments Operations	Mission-critical transaction processing	Lowest appetite; <2 hours downtime/year	Downtime = lost revenue; regulatory requirements
Product Development	Software engineering, feature releases	Higher appetite; <24 hours downtime acceptable	Lower impact; dev systems are not customer-facing
Marketing/Analytics	Campaign execution, reporting	Highest appetite; <72 hours downtime acceptable	No real-time customer impact; work can be deferred

Risk Threshold Governance Models

Three-Color Risk Threshold Model

The most common model uses three zones (green/yellow/red) that trigger specific governance actions:

Green Zone (Within Appetite)

- **Trigger: Risk is within acceptable range**
- **Action: Routine monitoring; no escalation required**
- **Review Cycle: Quarterly risk dashboard reporting**

Yellow Zone (Elevated Risk)

- **Trigger: Risk approaches or slightly exceeds appetite**
- **Action: Enhanced monitoring; mitigation planning; monthly review by Risk Committee**
- **Timeline: Develop mitigation plan within 2 weeks; implement within 60 days**
- **Escalation: Inform CFO and COO; brief board Risk Committee at next meeting**

Red Zone (Critical Risk)

- **Trigger: Risk significantly exceeds appetite or is in critical incident phase**
- **Action: Immediate escalation to CEO/Board; emergency response team activation**

- **Timeline:** Escalate within 2 hours of detection; board notification same day
- **Resolution:** Executive decision on risk acceptance, mitigation, or business model change

Practical Example: Data Security Risk Thresholds

For an organization with \$100M annual revenue and \$1M/year cybersecurity loss appetite:

Risk Metric	Green Zone	Yellow Zone	Red Zone	Action
Unpatched Critical Vulnerabilities	0-5	6-15	>15	Red: CISO escalates; remediation plan required within 48 hours
Failed Backup Tests	0-2/quarter	3-5/quarter	>5/quarter	Yellow: Investigate root cause; Red: CTO + BCSO escalation
Expected Annual Data Breach Loss	<\$300K	\$300K-\$700K	>\$700K	Yellow: Risk Committee review; Red: Board approval required
Customer Data Exposure Incident Size	<100 records	100-1,000 records	>1,000 records	Yellow: Notify Legal; Red: CEO + General Counsel + Board

Risk Appetite Governance Structures

Board Risk Committee

- **Frequency:** Monthly or quarterly
- **Responsibilities:**
 - Monitor whether actual risk is within board-approved appetite
 - Review yellow/red zone escalations
 - Approve significant risk mitigation investments
 - Recommend adjustments to risk appetite if strategy changes
- **Reporting:** Risk dashboard showing actual risk vs. appetite, trend, emerging risks

Executive Risk Steering Committee

- **Members:** CRO, CIO, COO, CFO, Chief Compliance Officer, Chief Continuity Officer
- **Frequency:** Monthly
- **Responsibilities:**
 - Translate board appetite into operational thresholds
 - Manage yellow zone escalations (develop mitigation plans)
 - Allocate risk budget across business units
 - Coordinate cross-functional risk response

Risk Champions / Business Unit Risk Owners

- **Role:** Embedded within each business unit/function
- **Responsibilities:**
- **Monitor risks within their domain against thresholds**
- **Alert when risks approach yellow/red zones**
- **Develop and implement mitigation plans**
- **Support continuous risk monitoring**

Connecting Risk Appetite to Business Continuity Decisions

Example 1: Disaster Recovery Architecture Decision

Decision: Should we invest in hot standby (active/active) or warm standby (active/passive) recovery architecture?

Risk Appetite Input: Board has set \$5M expected annual loss appetite for critical payment systems; RTO of <4 hours. **Analysis:**

- **Hot standby cost:** \$3M/year; RTO = 15 minutes; reduces expected loss to \$500K/year
- **Warm standby cost:** \$1.5M/year; RTO = 4 hours; reduces expected loss to \$2M/year
- **Cold standby cost:** \$300K/year; RTO = 24+ hours; expected loss = \$8M/year (exceeds appetite)

Decision: Risk appetite of \$5M expected loss justifies warm standby (\$1.5M/year cost, \$2M expected loss) but not necessarily hot standby unless strategic importance is higher. If board wants <\$500K expected loss, hot standby is required.

Example 2: Recovery Investment Prioritization

Decision: We have \$2M annual recovery budget. How do we allocate?

Risk Appetite Input: Board appetite of \$50M total organizational loss; expected losses are currently \$45M. We have \$5M capacity to accept risk.

Analysis: Using quantitative risk assessment, we calculate mitigation ROI for each recovery initiative:

Initiative	Cost/Year	ALE Reduction	RORI	Cumulative Cost	Cumulative ALE Reduction
Database replication	\$600K	\$1.8M	3.0	\$600K	\$1.8M
Backup automation	\$400K	\$1.2M	3.0	\$1M	\$3M
Network redundancy	\$700K	\$700K	1.0	\$1.7M	\$3.7M
Cloud-based recovery	\$500K	\$600K	1.2	\$2.2M	\$4.3M

Decision: With \$2M budget and goal to reduce expected loss by \$3M (meeting appetite), fund database replication (\$600K), backup automation (\$400K), and cloud-based recovery (\$500K). Defer network redundancy; revisit if budget increases.

Risk Appetite and Crisis Response

Accepting Risk During Crisis

Risk appetite can be temporarily elevated during crisis response. Example:

A data center facility fails unexpectedly. Normal recovery would take 16 hours. However, business interruption loss is \$1M/hour. The Chief Risk Officer recommends:

“Normal risk appetite is \$5M annual loss. This incident will cost \$16M in immediate losses. We approve temporary exceeding of appetite to \$25M, authorizing emergency expense of \$8M for airlifted equipment, emergency staffing, and expedited recovery to 4-hour timeline. This reduces total loss from \$16M to \$8M.”

This decision—accepting temporary appetite exceedance to limit total loss—is board-level. The CRO documents the decision; board ratifies after the fact.

Key Takeaways

- Risk appetite is a board decision: Not a risk team decision; reflects organizational values and strategy
- Appetite must be explicit and documented: Vague guidance (“be risk-aware”) is insufficient for operational decision-making
- Tolerance bands reflect realistic variance: Organizations cannot hit targets exactly; tolerance acknowledges this
- Thresholds enable escalation: Green/yellow/red zones provide clear triggers for action and escalation
- Appetite cascades through organization: Board appetite translates into executive thresholds, which become operational guidance
- Appetite informs investment decisions: Recovery architecture, business continuity budgets, and mitigation strategies all hinge on risk appetite
- Appetite evolves with strategy: When organization changes strategy, risk appetite should be re-evaluated and may shift

Frequently Asked Questions

How do I establish board risk appetite when board members have limited risk sophistication?

Start with education: present case studies of peers’ risk appetites (e.g., “Most Fortune 500 financial institutions accept 0.5-1% of revenue as annual loss appetite”). Frame appetite in business terms: “Accepting \$50M annual loss means we invest \$5M/year in recovery infrastructure.” Use board retreat format (full-day session with expert facilitator) to develop appetite collaboratively. Start conservative; adjust as board gains confidence. Document appetite in writing; revisit annually.

What if actual risk exceeds risk appetite? Who decides?

If risk exceeds appetite, three options: (1) Accept the risk (board decision; documented in meeting minutes; may require disclosure to regulators). (2) Mitigate risk (implement recovery controls to bring risk back within appetite). (3) Transfer risk (insurance, outsourcing, or divesting the business unit). The decision is escalated to the board unless it's a well-known risk with pre-agreed mitigation. Examples: "We know data center outage risk exceeds appetite; board has approved \$3M/year investment to reduce it below appetite within 18 months."

How do I set risk appetite for small or startup organizations without formal board governance?

Start with executive team (CEO, CFO, operations lead) instead of board. Define appetite informally but document it. Example: "Our startup accepts higher risk tolerance to move fast. Downtime up to 48 hours is acceptable for non-payment systems. Temporary data loss of <24 hours is acceptable if recovery cost is <\$50K." As organization grows and adds board, formalize and board-approve. Risk appetite should evolve with organizational maturity.

How do risk appetite, risk tolerance, and risk thresholds relate to RTO/RPO?

RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are manifestations of risk appetite. Appetite of "minimal downtime" translates to aggressive RTO/RPO (e.g., 1-hour RTO, 15-minute RPO for critical systems). Appetite of "acceptable downtime <24 hours" translates to relaxed RTO/RPO (e.g., 24-hour RTO, 4-hour RPO). Thresholds are monitored during incidents: if recovery is tracking toward 6-hour RTO but appetite is <4 hours, escalate and consider contingency plans. See Business Impact Analysis: Methodology, RTO/RPO Framework for RTO/RPO details.

How should we adjust risk appetite in response to major organizational changes?

Major changes (M&A, new market entry, major system deployment, regulatory changes) warrant risk appetite re-assessment within 60 days. Convene board Risk Committee; present scenario analysis: "If we acquire this company, our risk profile changes from \$30M expected loss to \$80M expected loss. Should we adjust appetite accordingly or invest in integration controls?" Board decides whether to adjust appetite or mitigate new risks. Document decision and communicate to organization.

What metrics should we use to monitor whether actual risk is within appetite?

Financial metrics (expected annual loss, ALE by risk category), operational metrics (system uptime %, failed recovery tests), and leading indicators (unpatched vulnerabilities, backup success rate). Report quarterly to board with actual vs. appetite: "Expected annual loss is \$42M, within our \$50M appetite. However, cybersecurity risk is trending upward; if current trajectory continues, we'll exceed \$60M appetite in 6 months. Recommend enhanced mitigation." Use dashboard with red/yellow/green zones for quick visualization.

Related: Hub: Risk Assessment: The Complete Professional Guide. Continuity Hub home.

Enterprise Risk Assessment Frameworks: ISO 31000, COSO ERM, and NIST

Source: <https://continuityhub.org/enterprise-risk-assessment-frameworks-iso-31000-coso-erm-nist/>

Published: March 18, 2026

Why a framework is on a continuity site

A continuity program needs a way to decide which risks get a plan. ISO 31000, COSO ERM, and the NIST Cybersecurity Framework are three common ways to do that. They are not three copies of a business continuity plan. They are methods for finding, ranking, and assigning risk. The continuity plan is one response after that ranking.

ISO 31000

ISO 31000 is a general risk-management approach: establish the context, identify risks, analyze them, evaluate them, and treat them, then monitor. On this site, the threat-analysis page is the continuity version of that middle step. It looks at hazards to operations, including suppliers, cloud services, concentration in one provider, and geopolitical disruption.

COSO ERM

COSO's enterprise risk management frame ties risk to strategy and performance, not only to a risk register. For continuity, that means a recovery gap is an enterprise risk when it can stop a service the organization has promised to keep running. The register should show the owner, the risk appetite tolerance, and the treatment. A list of threats with no owner is not ERM.

NIST

NIST's cybersecurity framework is aimed at cyber risk: identify, protect, detect, respond, and recover. Use it for technology and information risks that can trigger a continuity event. Do not treat it as the whole continuity program. A flood, a supplier failure, or a site loss can sit outside a cyber framework and still need a recovery plan.

Use one ranking, not three piles

Running all three as separate programs produces three lists. Pick one place where a risk is accepted, treated, or transferred, and point the continuity plan at that decision. The threat-analysis page already asks for concentration risk and third-party continuity. That is the practical test: if a framework does not change a recovery priority, it is not yet connected to this site's work.

Crisis Communication Protocols: Incident Command, Stakeholder Management, and Notification Frameworks

Source:

<https://continuityhub.org/crisis-communication-protocols-incident-command-stakeholder-management/>

Published: March 18, 2026

Crisis Communication in Business Continuity is the structured framework of protocols, channels, roles, and message templates that enables an organization to coordinate internal response, notify regulators, inform stakeholders, and manage public messaging during and after a disruptive event. Under ISO 22301:2019 Clause 8.4.3, organizations must establish, implement, and maintain procedures for internal and external communications during disruptions, including what to communicate, when, to whom, and

through which channels.

Why Communication Fails First

In post-incident reviews across industries, communication breakdown is consistently cited as the primary amplifier of operational disruption. The disruption itself causes the initial damage; the failure to communicate effectively multiplies it. Teams work at cross-purposes because they lack situational awareness. Customers receive no information and assume the worst. Regulators learn about the incident from media reports instead of from the organization. Executives make decisions based on incomplete or contradictory information. The business continuity plan may have technically sound recovery procedures, but if the people executing them cannot coordinate effectively under stress, those procedures fail in practice.

The Incident Command Structure

Effective crisis communication requires clear authority. The Incident Command System (ICS), originally developed by FEMA for emergency management, provides a scalable command structure that most organizations adapt for business continuity. The key roles are the Incident Commander (ultimate decision authority during the event), the Operations Section Chief (directs tactical recovery activities), the Planning Section Chief (collects and analyzes situational information), the Logistics Section Chief (manages resources and support), and the Communications Officer (manages all internal and external messaging).

The critical principle is unity of command—every person in the response knows exactly who they report to, and every message to external audiences flows through a single authorized channel. Organizations that allow multiple spokespeople to communicate independently during a crisis invariably produce contradictory messages that erode stakeholder confidence.

Notification Trees and Escalation Triggers

The notification tree defines who gets contacted, in what order, through which channels, when a disruptive event is detected. It must be designed for speed and redundancy—because the primary communication channels (email, VoIP, corporate messaging platforms) may themselves be affected by the disruption. Best practice requires at least three independent notification methods: automated mass notification system (such as Everbridge, AlertMedia, or OnSolve), mobile phone calls and SMS to personal devices, and a physical or analog fallback (posted procedures, radio, satellite phone for severe scenarios).

Escalation triggers define the thresholds at which notification escalates from the operational team to management, from management to executive leadership, and from executive leadership to the board. These triggers should be objective and measurable: “If system recovery exceeds RTO by more than 2 hours, escalate to C-suite.” “If customer-facing services are unavailable for more than 4 hours, activate

the external communications protocol.” Subjective escalation criteria (“when it seems serious”) consistently produce delayed responses.

Internal Communication During Disruptions

Employees are the first audience and the most neglected. During a disruption, employees need three things immediately: what happened (situational awareness), what they should do (clear instructions), and when they will receive the next update (predictable cadence). The most effective internal communication protocol establishes a fixed update cadence—every 30 minutes during the acute phase, every 2 hours during recovery, daily during restoration—and adheres to it even when there is no new information to share. Saying “no change since last update, next update in 30 minutes” is infinitely better than silence, because silence forces people to fill the information vacuum with speculation.

Internal communication must also account for employees who are personally affected by the disruption—especially in regional disasters where employees may be dealing with property damage, family safety concerns, or displacement. The communication plan should include welfare check procedures and clear guidance on employee assistance resources.

External Stakeholder Communication

External communication during a crisis serves four distinct audiences, each with different information needs and legal implications.

Customers and Clients

Customers need to know how the disruption affects their service, what the organization is doing to resolve it, and what the expected timeline for restoration is. The golden rule is proactive disclosure—customers should learn about the disruption from the organization before they discover it themselves. Proactive communication preserves trust; reactive communication (responding only after customers complain) destroys it.

Regulators

Many industries have mandatory incident notification timelines. Financial services firms must notify OCC and state regulators within defined windows. Healthcare organizations must report under HIPAA breach notification rules (60 days for breaches affecting 500+ individuals, with notification to HHS and media). Critical infrastructure operators have CISA reporting obligations under CIRCIA (72 hours for significant cyber incidents, 24 hours for ransomware payments). The communication plan must document every regulatory notification requirement, the responsible individual, and the specific timeline—because missed regulatory notifications compound the original disruption with compliance violations.

Media

Media communication requires a designated spokesperson trained in crisis media relations. The organization should have pre-drafted holding statements—templated messages that can be customized

quickly to acknowledge the incident, express concern, describe the response, and commit to updates. Media communication should never speculate on causes, assign blame, or provide specific timelines that may prove incorrect. The principle is: say what you know, say what you're doing, say when you'll say more.

Business Partners and Vendors

Partners and vendors need to know how the disruption affects joint operations, whether their own systems or data are at risk, and what coordination is needed. This communication is frequently overlooked in crisis plans, leading to cascading disruptions through the supply chain. The risk assessment should have identified critical third-party dependencies; the communication plan must include notification procedures for each one.

Pre-Drafted Communication Templates

Under stress, people write poorly. The crisis communication plan should include pre-drafted templates for every major scenario identified in the risk assessment: cyber incident notification, facility closure announcement, service disruption advisory, regulatory notification, employee welfare check, and recovery completion announcement. Templates should be written at an 8th-grade reading level, avoid jargon, and include clear placeholders for event-specific details. They should be reviewed and updated annually alongside the rest of the continuity plan.

Testing Communication Independently

Communication procedures must be tested separately from operational recovery procedures. A tabletop exercise that tests recovery workflows but uses normal meeting communication to coordinate has not tested the communication plan at all. Communication-specific exercises should test notification tree activation (does everyone get notified within the target timeframe?), channel redundancy (what happens when the primary channel is down?), message accuracy (does the situational information reach decision-makers without distortion?), and regulatory notification compliance (can the team draft and submit required notifications within mandatory timelines?).

Social Media in Crisis Communication

Social media is both a communication channel and a threat vector during crises. Misinformation about the organization's disruption can spread faster than the organization's official communications. The crisis communication plan must include social media monitoring (tracking mentions and correcting misinformation), official social media messaging protocols (who is authorized to post, what approval process applies), and response guidelines for direct inquiries received through social channels. Organizations that ignore social media during a crisis cede the narrative to others.

Frequently Asked Questions

What should the first communication say during a business disruption?

The first communication should acknowledge the disruption, describe what is known at that moment (without speculation), state what the organization is doing in response, and commit to a specific time for the next update. It should not speculate on causes, estimate recovery timelines before they are validated, or assign blame. Speed matters more than completeness—a brief, accurate initial message sent quickly is far more effective than a comprehensive message sent late.

How many communication channels should be included in the crisis plan?

A minimum of three independent channels: an automated mass notification system, mobile phone (calls and SMS to personal devices), and an analog or out-of-band fallback. The channels must be truly independent—if all three rely on the same network infrastructure, a single network failure disables the entire notification system. Organizations in high-risk environments (critical infrastructure, healthcare, financial services) typically maintain four or more channels including satellite communication capability.

Who should serve as the crisis spokesperson?

The spokesperson should be a senior leader with media training, calm demeanor under pressure, and the authority to speak on behalf of the organization. This is typically the CEO, COO, or a designated VP of Communications. The spokesperson should not be the Incident Commander—the IC needs to focus on managing the response, not managing the media. Backup spokespersons should be designated and trained for situations where the primary is unavailable.

What are the regulatory notification requirements for cyber incidents?

Requirements vary by industry and jurisdiction. Under CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act), critical infrastructure entities must report significant cyber incidents to CISA within 72 hours and ransomware payments within 24 hours. HIPAA requires breach notification within 60 days for breaches affecting 500+ individuals. Financial services firms have OCC, SEC, and state-level notification requirements. The crisis communication plan must document every applicable requirement with specific timelines, responsible individuals, and submission procedures.