Witboek

De nieuwe ISO-norm ISO/IEC 27031:2025

Hoe technische noodplanning succesvol kan worden aangepast aan strategisch, organisatiebreed veerkrachtmanagement.

controllit
Business Continuity Management

Inhalt

Inleiding

ISO/IEC 27031 is in mei 2025 grondig herzien en vervangt de editie van 2011. In plaats van puur technische IT-herstelplanning hanteert de nieuwe norm een alomvattende benadering van veerkracht. ICT Readiness for Business Continuity (IRBC) wordt beschouwd als een integraal onderdeel van de bedrijfsstrategie en moet nauw worden gekoppeld aan bedrijfscontinuïteit, informatiebeveiliging, incidentrespons en risicobeheer.

Nieuw is de duidelijke strategische verankering van IRBC in management- en controlestructuren. Rollen, verantwoordelijkheden en competenties moeten op bindende wijze worden gedefinieerd. De eisen gelden ook onder omstandigheden van actieve cyberaanvallen (bijv. ransomware, APT), waardoor de rol van de IRBC-manager aanzienlijk wordt uitgebreid – tot die van medeontwerper van veerkrachtige ICT-architecturen.

Bedrijven moeten gedocumenteerde oplossingen bieden die rekening houden met redundantie, cloud- en supply chain-afhankelijkheden en die zijn afgestemd op RTO, RPO en de nieuw geïntroduceerde Final MBCO. De norm vereist ook een gestructureerd test-, trainings- en auditprogramma met prestatie-indicatoren, systematische evaluatie en geleerde lessen.

Bestaande ITSCM/IRBC-systemen kunnen blijven worden gebruikt zolang ze functioneel aan de nieuwe eisen voldoen. Deze omvatten duidelijke governance-koppelingen, integratie in bestaande managementsystemen, vaststelling van de Final MBCO en continue verbeteringsprocessen. De norm vermeldt niet expliciet de PDCA-cyclus, maar blijft het principe van continue verbetering volgen: van planning tot implementatie en testen tot strategische evaluatie door het management.

Deze whitepaper presenteert de belangrijkste wijzigingen ten opzichte van ISO/IEC 27031:2011, classificeert deze strategisch en analyseert de impact ervan op gereguleerde bedrijven en bestaande managementsystemen op het gebied van IT-service-continuïteitsbeheer (ITSCM) en IRBC. Er wordt rekening gehouden met elementen uit verwante normen zoals ISO/IEC 22301 (bedrijfscontinuïteitsbeheer), ISO/IEC 27001 (informatiebeveiligingsbeheer), het NIST Cybersecurity Framework en beproefde ITSCM-methoden.

Verdieping van de centrale veranderingen

De nieuwe ISO/IEC 27031:2025 heeft een merkbare impact op de strategische en operationele praktijk van IRBC en ITSCM. De focus ligt op een nauwere integratie met BCM volgens ISO 22301. IRBC-doelstellingen worden nu samen met de resultaten van de BIA gedefinieerd, zodat RTO, RPO en de nieuwe Final MBCO te allen tijde op een traceerbare manier aan elkaar zijn gekoppeld.

Tegelijkertijd verbreedt de nieuwe norm zijn focus naar aanverwante normen. De norm zelf verwijst uitsluitend naar ISO/IEC-normen (bijv. ISO 22301, 27002). Bedrijven kunnen de controles echter in kaart brengen aan de hand van wettelijke vereisten zoals DORA of NIS-2 en kaders zoals NIST-CSF of NIST SP 800-61 om synergieën te creëren tussen informatiebeveiliging, continuïteit en incidentrespons processen. Bedrijven kunnen bijvoorbeeld controles zoals ISO 27002 Control 5.30 opnemen in hun IRBC-kader en deze documenteren voor regelgevingsdoeleinden.

Een belangrijk element is geformaliseerd bestuur. De rol van de IRBC-manager krijgt duidelijk omschreven bevoegdheden, rapporteert aan een op te richten interdisciplinaire IRBC-stuurgroep en beheert een geconsolideerde set van key performance indicators (KPI's). Deze indicatoren variëren van naleving van IT-hersteltijden tot metingen uit tests en audits. De IRBC-manager zal dus in de toekomst fungeren als schakel tussen IT-implementatie en het topmanagement.

De BIA blijft de spil, maar wordt uitgebreid met een consistente traceerbaarheidsaanpak. Technische ICT RTO en ICT RPO leiden tot technische IT-streefwaarden. Hiaten worden ofwel gedicht door investeringen, ofwel geaccepteerd als een risico en gedocumenteerd in de Final MBCO (Minimum Business Continuity Objective). Deze Final MBCO definieert het laagste aanvaardbare prestatieniveau na voltooiing van het IT-herstel, waardoor de transparantie wordt vergroot in situaties waarin de ideale streefwaarden op korte termijn niet kunnen worden bereikt.

Strategische heroriëntatie en integratie met ISO 22301

ISO/IEC 27031:2025 verankert IRBC veel sterker in de strategische context dan voorheen en benadrukt het belang van IT-veerkracht als integraal onderdeel van een bedrijfscontinuïteitsbeheersysteem (BCMS). IRBC wordt niet langer gezien als een puur technische reactie op kritieke IT-incidenten, maar als een strategisch verankerd controle-instrument binnen het BCMS in overeenstemming met ISO 22301. Dit omvat gezamenlijke doelstellingen, gecoördineerde (IT-)risico- en bedrijfseffectanalyses (BIA's), gecoördineerde bestuursstructuren en een consistente (IT-)test- en oefenstrategie. De raakvlakken met BCM, zoals bedrijfseffectanalyse (BIA), (IT-)risicobeoordeling, gecoördineerde bestuursstructuren en een consistente (IT-)test- en oefenstrategie, worden expliciet benadrukt.

Deze heroriëntatie komt tot uiting in de expliciete vraag naar strategische integratie en onderlinge afhankelijkheid tussen de disciplines. Het doel is niet langer alleen om de IT opnieuw op te starten, maar om de veerkrachtige werking van tijdkritische IT-diensten te waarborgen in overeenstemming met de eisen van tijdkritische bedrijfsprocessen. IT wordt gepositioneerd als een waardetoevoegende factor met hoge veerkrachtseisen.

De strategische oriëntatie komt tot uiting in verschillende elementen:

- In de toekomst moet IRBC strategisch worden vormgegeven en geïntegreerd in de veerkrachtstrategie van het bedrijf.
- Integratie met het BCMS is een belangrijk element.
- De norm formuleert duidelijke eisen voor controle, coördinatie en wederzijdse afleiding van streefwaarden zoals RTO, RPO en Final MBCO.
- De scheiding tussen technische en organisatorische veerkrachtmaatregelen wordt opgeheven ten gunste van een geïntegreerde aanpak.
- De verantwoordelijkheid voor IRBC ligt niet langer primair bij IT, maar vereist interdisciplinair bestuur.

Strategische heroriëntatie en integratie met ISO 22301

Wat vereist de norm concreet?

Terwijl ISO/IEC 27031:2011 slechts indirect integratie in BCM vereiste, schrijft de herziene versie uit 2025 dit nu expliciet en bindend voor. De norm vereist met name:

- een gezamenlijke definitie van doelstellingen in het BCMS
- gecoördineerde (IT-)risico- en bedrijfseffectanalyses
- gecoördineerde bestuursstructuren
- geïntegreerde IT-test- en oefenstrategieën

Wat betekent dit voor de implementatie?

Bedrijven moeten ervoor zorgen dat IRBC-maatregelen niet afzonderlijk worden ontwikkeld en uitgevoerd, maar als onderdeel van BCM. Dit omvat gezamenlijke planningsprocessen, geïntegreerde documentatie en regelmatige coördinatie tussen IRBC- en BCM-managers. IT-continuïteitsvereisten worden rechtstreeks afgeleid uit BIA-resultaten. De norm vereist een gecoördineerd beheer van beide disciplines. Dit omvat onder andere:

- gezamenlijk overeengekomen streefwaarden (RTO, RPO, Final MBCO)
- Gesynchroniseerde (IT-)risico- en BIA-processen
- Onderling gekoppelde bestuursstructuren en rapportagelijnen
- gecoördineerde (IT) noodcommunicatie- en escalatieprocessen
- Consistente en traceerbare documentatie (inclusief de interfaces tussen IRBC en bedrijfscontinuïteitsplannen)

Bedrijven met reeds op elkaar afgestemde IRBC/BCM-beheersystemen zijn over het algemeen goed gepositioneerd. De eisen voor het volgende worden echter steeds strenger:

- **Traceerbaarheid en methodologie:** Bij audits wordt steeds vaker gedocumenteerd bewijs gevraagd van hoe IRBC-maatregelen zijn afgeleid van BCM-resultaten.
- **Governance en rolstructuur: H**et moet duidelijk zijn wie verantwoordelijk is voor welke IRBC-resultaten en hoe de samenwerking met BCM en ISM is georganiseerd.
- **Consistentie in audits:** In de toekomst zullen audits zich meer specifiek richten op hoe IRBC-maatregelen methodisch zijn afgeleid van BCM-resultaten, hoe rollen zijn gedefinieerd en hoe de interactie tussen BCM, IRBC en ISM is georganiseerd. De norm vraagt niet alleen om meer samenwerking tussen deze disciplines, maar stelt ook hogere eisen aan de gedocumenteerde consistentie ervan.

Strategische heroriëntatie en integratie met ISO 22301

Praktijkvoorbeeld: Example Ltd – BIA & IRBC met volledige documentatie

In de toekomst moeten bedrijven kunnen documenteren en uitleggen hoe BIA-resultaten methodisch zijn vertaald naar IRBC-oplossingen en hoe de samenwerking tussen BCM, IRBC en ISM is georganiseerd.

Example Ltd. exploiteert een cloudplatform met hoge beschikbaarheid voor lokale overheidsinstanties. Uit een BIA bleek dat het uitvallen van het selfserviceplatform voor klanten na maximaal twee uur zou leiden tot aanzienlijke administratieve vertragingen en reputatieschade. Het BCM definieert daarom een RTO van twee uur. In de vorige planning werd uitgegaan van een warm stand-byscenario met een IT-hersteltijd van zes uur.

Als onderdeel van de strategische heroriëntatie in overeenstemming met ISO/IEC 27031:2025 werd IRBC volledig geïntegreerd in het BCMS. De IT-hersteldoelstellingen (ICT-RTO, ICT-RPO) werden op traceerbare wijze afgeleid uit de BIA-resultaten, technisch gevalideerd en vastgelegd in gestructureerde planningsdocumentatie.

De platformarchitectuur werd omgezet naar hot standby, de ICT-RTO werd teruggebracht tot 90 minuten = doel bereikt, documentatie controleerbaar.

De afleiding werd op begrijpelijke wijze gedocumenteerd, met inbegrip van:

- Verwijzing naar de betreffende BIA-vereiste (inclusief proces-ID)
- de toewijzing van ICT-diensten aan kritieke bedrijfsprocessen
- de afleiding van ICT RTO/RPO op basis van de BIA
- Technische oplossingsopties, inclusief evaluatie en afweging van restrisico's
- Bepaling van de Final MBCO in geval van afwijkingen
- Beoordelingsdatum, evaluatie en goedkeuring door het management

Voor interne audits dient deze documentatie nu als enige bron van waarheid voor de afleidingslogica tussen bedrijfsvereisten en de geïmplementeerde IRBC-oplossing.

Uitgebreide governance- en managementvereisten

De nieuwe norm benadrukt het belang van duidelijk en gestructureerd bestuur voor IRBC. Voorheen waren veel bestuurselementen (bijv. beleid, handleiding, jaarverslagen, enz.), best practices of interpretaties onderhevig aan interpretatie. ISO/IEC 27031:2011 zelf bleef nogal vaag in zijn uitspraken over governance. In de versie van 2025 wordt governance echter expliciet vereist door de norm, met gedefinieerde minimumvereisten voor rollen, controle en betrokkenheid van het management.

Wat vereist de norm concreet?

Terwijl de ISO-norm van 2011 slechts governance-elementen noemde, schrijft de nieuwe norm de formele integratie van IRBC in de management- en controlestructuren van het bedrijf voor. IRBC wordt een managementtaak met betrokkenheid van commissies, rapportageverplichtingen en interfaces met BCMS, ISMS en (IT-)risicomanagement.

De norm benadrukt expliciet dat het topmanagement niet alleen verantwoordelijkheid draagt, maar ook actief beslissingen moet nemen over de toewijzing van middelen, doelstellingen zoals de Final MBCO en risicoacceptatie op basis van IRBC-rapporten.

De rol van de IRBC-manager wordt versterkt, zowel strategisch als operationeel.

Belangrijke vereisten zijn onder meer:

- Formele aanstelling van een IRBC-manager met duidelijke taken, plaatsvervangers en bevoegdheden
- Regelmatige evaluaties door het senior management, inclusief KPI-rapportage
- gedocumenteerde richtlijnen en processen, evenals escalatie- en communicatie-kanalen
- Zorgen voor voldoende financiële en personele middelen voor IRBC-activiteiten
- Vaste audit- en evaluatiecycli om de effectiviteit van governance-structuren te beoordelen

Wat betekent dit voor de implementatie?

IRBC moet niet langer worden gezien als louter een instrument voor IT-herstelplanning, maar als een integraal controleproces dat actief bijdraagt aan de veerkrachtstrategie van het bedrijf. De norm vereist een systematische verankering in het bestuursmodel, met duidelijk gedocumenteerde verantwoordelijkheden, gecoördineerde escalatieroutes en gestructureerde interfaces met het BCMS, ISMS en crisismanagement.

Uitgebreide governance- en managementvereisten

Er wordt ook bijzondere aandacht besteed aan de traceerbaarheid en controleerbaarheid van rolmodellen, communicatiestructuren en besluitvormingsprocessen. Deze moeten consistent worden gedocumenteerd en traceerbaar zijn in het kader van interne en externe audits.

De norm schrijft geen specifieke vorm voor, maar vereist een commissie met passende controlebevoegdheid en interdisciplinariteit. In de praktijk kan dit bijvoorbeeld een veerkrachtraad zijn, waarin IRBC, BCM, ISM, risicobeheer, IT-operaties en bedrijfsmanagement regelmatig IRBC-kwesties coördineren. IRBC-beslissingen mogen niet geïsoleerd worden genomen, maar moeten worden ingebed in het algemene beheer van de veerkracht van de onderneming.

Bedrijven moeten ervoor zorgen dat:

- IRBC-rollen (eigenaar, manager, enz.) met taken, bevoegdheden en vertegenwoordiging schriftelijk worden vastgelegd
- een interdisciplinaire stuurgroep (bijvoorbeeld een veerkrachtraad) regelmatig, bijvoorbeeld elk kwartaal, managementbeoordelingen uitvoert
- Prestatiecriteria worden als KPI's geïntegreerd in de managementrapportage
- Er bij de budget- en investeringsplanning rekening wordt gehouden met de benodigde middelen voor IRBC
- Governancestructuren, communicatie- en escalatiekanalen regelmatig worden geëvalueerd en centraal worden beheerd
- IRBC is opgenomen in een intern audit- en evaluatieprogramma en de effectiviteit ervan kan worden aangetoond

Uitgebreide governance- en managementvereisten

Praktijkvoorbeeld: Example Ltd – Opzetten van een IRBC-governancestructuur in een gereguleerde omgeving

Example Ltd is een financiële dienstverlener en is onderworpen aan de regelgevings-vereisten van NIS-2 en DORA. Uit een interne compliance-audit bleek dat er weliswaar een basis-ITSCM bestond, maar dat er geen formele governance-structuur voor IRBC was. Rollen, verantwoordelijkheden en escalatiepaden waren alleen bekend in afzonderlijke IT-gebieden en waren niet centraal gedocumenteerd.

Mogelijke maatregelen voor de implementatie van de standaardvereisten:

1. **Oprichting van een Resilience Board**
   - Taken: driemaandelijkse evaluaties, goedkeuring van IRBC-doelstellingen, beslissingen over middelen, beslissingen over risicoacceptatie
   - Samenstelling: IRBC-manager, BC-manager, CISO, IT-operations, risicobeheer, management

2. **Formele benoeming van een IRBC-manager**
   - Schriftelijke omschrijving van taken, bevoegdheden en vertegenwoordigingsregelingen
   - Instelling van rapportagelijnen

3. **Integratie van KPI's in managementrapportages**
   - Kwartaalrapportage aan de Resilience Board en jaarlijkse presentatie aan de Raad van Commissarissen (indien van toepassing)
   - Definitie van KPI's: bijv. doelbereiking ICT-RTO/ICT-RPO/Final MBCO, afwijkingen in tests, auditbevindingen, voortgang bij de implementatie van maatregelen

4. **Controleerbaarheid**
   - Uitvoeren van jaarlijkse effectiviteitsbeoordelingen
   - Regelmatige audits (intern/extern)

Harmonisatie met bestaande normen/standaarden

De nieuwe norm is duidelijk gepositioneerd als aanvulling op bestaande managementnormen en regelgevingskaders. Er wordt gepleit voor nauwe integratie en coördinatie met verwante normen om inconsistenties te voorkomen, redundantie tot een minimum te beperken en synergieën te creëren bij de ontwikkeling en werking van veerkrachtstructuren.

De focus ligt met name op de raakvlakken met:

- ISO/IEC 22301 (BCM): bedrijfsimpactanalyse, strategieontwikkeling, risicobeheer, doelbepaling
- ISO/IEC 27001 (ISMS): bijv. controles 5.30 (ICT-gereedheid voor bedrijfscontinuïteit) en 8.16 (monitoringactiviteiten) van ISO/IEC 27002:2022 of A 5.30 en A 8.16 in ISO/IEC 27001:2022
- ISO/IEC 27005:2022 (risicobeheer): IRBC-strategieafleiding en scenarioanalyses (bijv. bijlage B – CFIA/FMEA) zijn gebaseerd op een geconsolideerde risicosituatie in overeenstemming met ISO/IEC 27005
- ISO/IEC 27035 (incidentbeheer): integratie van incident- en herstelprocessen
- NIST SP 800-61 r3: Levenscyclus van incidentafhandeling, geleerde lessen
- NIST CSF 2.0: Detectie-, respons- en herstelfuncties
- NIS-2, DORA, BSI-norm 200-4: Wettelijke veerkracht- en verificatievereisten

Wat vereist de norm concreet?

In het ISMS volgens ISO 27002 beschermt controle 5.30 de beschikbaarheid van kritieke ICT-diensten. De nieuwe ISO 27031 biedt hiervoor de implementatierichtlijnen. De norm verwijst naar informatiebeveiligingsincidenten en vereist een gecoördineerde aanpak tussen incidentrespons, IRBC en BCM:

- Een geharmoniseerde risico- en planningsbasis tussen ISMS, BCMS en IRBC met duidelijke bewoordingen als verplichte eis, waardoor de implementatie onderworpen is aan een audit
- Gemeenschappelijke doelstellingen voor ICT-RTO, ICT-RPO en Final MBCO, consistent gedocumenteerd en gecontroleerd via uniforme documentcontrole
- Een bindende strategie voor tests, oefeningen en audits met gedefinieerde prestatiecriteria
- Uniforme, auditbestendige auditbewijzen voor interne en externe audits

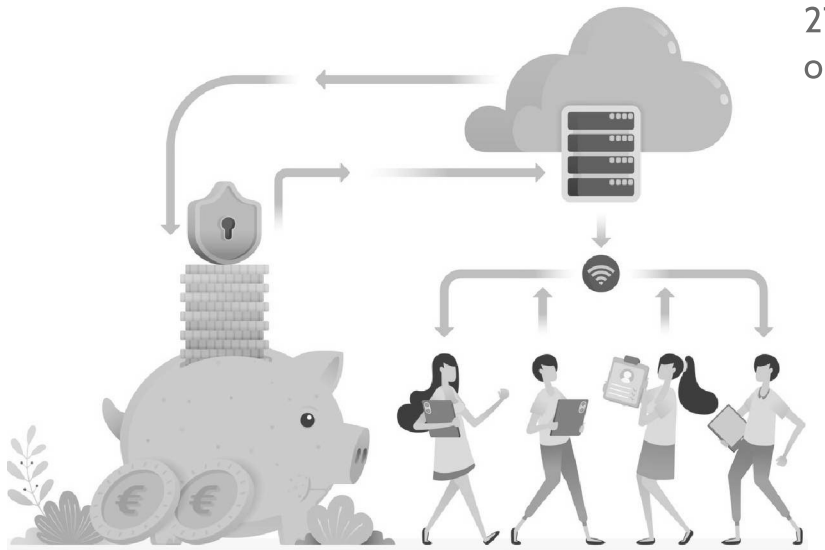
Harmonisatie met bestaande normen/standaarden

Wat betekent dit voor de implementatie?

- **ISMS/BCMS-harmonisatie:** In kaart brengen van controles en processen
- **Synergirapportering:** Gebruik van gemeenschappelijke kerncijfers en auditresultaten
- **GRC-model:** Uitgebreid governance-, risico- en compliance-model dat veerkracht als een transversaal thema integreert

Praktijkvoorbeeld: Example Ltd – gereguleerde geharmoniseerde controle

Als aanbieder van clouddiensten voor financiële en administratieve klanten valt Beispiel GmbH onder zowel DORA als NIS-2. Tot nu toe functioneerden ISMS, ITSCM en BCM zonder uitgebreid (IT-)risicobeheer.



Als onderdeel van de invoering van ISO/IEC 27031:2025 wordt een geïntegreerd kader opgezet. De onderdelen daarvan zijn:

- de consolidatie van (IT-)risicobeoordelingen op basis van ISO/IEC 27005
- standaardtoewijzing aan DORA en NIS-2 (bijv. toewijzing van controles aan ISO/IEC 27002 A 5.30)
- de harmonisatie van ICTRTO/RPO-hersteldoelstellingen tussen BIA, BCM en IRBC
- de definitie van een uniforme auditstructuur

Alle maatregelen worden in één document gebundeld en aangevuld met scope, contactpersonen, controledata en leercycli. Dit betekent dat interne en externe auditvereisten nu volledig kunnen worden gedocumenteerd – met consistente, auditbestendige documentatie.

Interface met ITIL 4 en onderscheid met IRBC

ITIL 4 zet de praktijk van IT Service Continuity Management (ITSCM) voort, die zijn oorsprong vindt in de jaren negentig. In het verleden werden de termen ITSCM en IRBC vaak als synoniemen gebruikt, omdat beide gericht waren op IT-herstel.

Harmonisatie met bestaande normen/standaarden

Met de nieuwe standaard verschuift de focus aanzienlijk van een puur servicegericht herstel (ITIL) naar een organisatiebrede veerkrachtbenadering (IRBC). In de toekomst zal het daarom belangrijk zijn om duidelijk aan te geven of men verwijst naar operationele ITIL-praktijken of naar het strategische IRBC-raamwerk. De veranderingen in de nieuwe standaard betekenen dat de disciplines op sommige gebieden uiteenlopen, maar dat ze nog steeds een gecoördineerde interactie vereisen.

Gevolgen voor wettelijke vereisten

Voor gereguleerde bedrijven (bijvoorbeeld financiële of KRITIS-sectoren) die moeten voldoen aan de eisen van ISO/IEC 27031, is een pure ITSCM-implementatie volgens ITIL niet langer voldoende. ITIL blijft de operationele IT-continuïteitsprocessen voor tijdkritische IT-diensten dekken, maar voldoet niet aan de nieuwe strategische governance-, risico- en veerkrachteisen van de herziene norm.

Het is mogelijk om een bestaand ITSCM uit te breiden om te voldoen aan de eisen van ISO/IEC 27031:2025. ITSCM blijft van kracht voor IT-herstel en krijgt een strategische bovenbouw. Deze bovenbouw vereist geformaliseerd bestuur, regelmatige managementbeoordelingen en een risicogericht test- en auditprogramma. Hierdoor verschuiven sommige taken van technisch IT-herstel naar commissiewerk, beheer van belangrijke prestatie-indicatoren en risicobeoordeling.

Een groot nadeel vloeit voort uit de verschillende proceslogica van de twee werelden. ITIL volgt een servicegerichte levenscyclus, terwijl ISO 27031 de nadruk legt op strategische, risicogebaseerde controle. Als ISO-vereisten slechts oppervlakkig worden 'geflenst' op ITIL-processen, is het resultaat een hybride die niet volledig voldoet aan de ITIL-efficiëntievereisten of de ISO-documentatieverplichtingen. Er bestaat ook een risico op permanent dubbel onderhoud. Testresultaten, geleerde lessen en KPI-rapporten vloeien gelijktijdig in ITIL-continue verbetering en IRBC-rapportage. Dit creëert het risico van mediabroken en inconsistente informatie.

Daarom moet ITSCM worden uitgevoerd als een subproces onder IRBC. Dit betekent dat gereguleerde bedrijven bestaande ITSCM moeten integreren in de governance- en teststructuur van IRBC, zodat volledig wordt voldaan aan de audit- en verificatie-eisen van de norm. ITSCM blijft fundamenteel relevant voor het operationele IT-herstel van tijdkritische IT-diensten, terwijl IRBC het strategische kader vormt voor organisatiebrede IT-veerkracht. Beide managementdisciplines moeten worden gesynchroniseerd door middel van bindende, uitgebreide governance.

Harmonisatie met bestaande normen/standaarden

Zelfs zonder ITSCM kunnen bedrijven ISO 27031-compliance bereiken als IRBC zelf de taken van ITIL overneemt. Geïmplementeerde ITSM of ITIL vergemakkelijkt de operationele implementatie, maar is geen verplichte vereiste. De nieuwe norm verwacht echter dat IRBC alle ontbrekende processen functioneel vervangt.

	IRBC (ISO 27031:2025)	ITSCM-praktijk volgens ITIL 4
Doel	Het waarborgen van de veerkracht van tijdkritische ICT-diensten (inclusief governance en strategie)	Herstarten van IT-diensten in overeenstemming met overeengekomen tijdsdoelstellingen
Scope	Organisatie (BCMS) & IT-infrastructuur, governance, risico, IT-dienstverleners en leveranciers, gegevens	Tijdkritische IT-diensten
Planning	Strategieën (vaardigheden, faciliteiten, technologie, enz.)	Service SLA's, IT-infrastructuur, datacenter
Focus	Cyber, toeleveringsketen, compliance, gegevens en veerkracht van (IT-)dienstverleners	IT-infrastructuur, IT-service SLA's
Governance	Rolmatrix inclusief IRBC-manager/eigenaar en managementbeoordeling Best practice: veerkrachtraad	Praktijkeigenaar, praktijkmanager en service-eigenaarr

De nieuwe ISO/IEC 27031:2025 stelt duidelijk dat IRBC en ITSCM niet synoniem zijn. Terwijl ITSCM een operationele ITIL-praktijk is die verantwoordelijk is voor het herstel van ICT-diensten, definieert IRBC een strategisch kader voor bedrijfsbreed beheer van ICT-veerkracht. Aan regelgevende vereisten – met name die van DORA en NIS-2 – kan alleen worden voldaan als IRBC wordt geïmplementeerd. ITSCM kan hierin worden geïntegreerd, maar kan niet op zichzelf worden gebruikt.

Uitgebreide rol van de IRBC-manager

De herziene ISO/IEC 27031:2025 verandert de rol van de IRBC-manager fundamenteel. Waar zij voorheen voornamelijk verantwoordelijk waren voor het plannen en implementeren van IT-herstelmaatregelen in overeenstemming met de BCM-continuïteitsvereisten, is hun takenpakket nu aanzienlijk uitgebreid. Zij zijn niet langer in de eerste plaats planners van IT-herstelmaatregelen, maar ontwikkelen actief veerkrachtige IT-structuren, analyseren IT-risico's, plannen alternatieve IT-bedrijfsmodellen en coördineren passende maatregelen en processen met BCM, ISM, incidentrespons en crisismanagement.

Dit vereist het vermogen om met vooruitziende blik veerkrachtige IT-structuren te ontwerpen, alternatieve IT-bedrijfsmodellen aan te bieden en de functionaliteit van tijdkritische ICT-diensten te waarborgen, zelfs in het geval van complexe cyberaanvallen. In de toekomst zullen zij niet alleen moeten plannen voor IT-herstel in geval van een kritiek IT-incident, maar ook moeten zorgen voor voortdurende IT-bruikbaarheid in nauwe samenwerking met BCM, incidentbeheer, cyberresponsplanning en crisisbeheer, bijvoorbeeld in geval van een cyberaanval.

Daarbij fungeren zij als technische integrator tussen technische, organisatorische en strategische vereisten en moeten zij over cross-functionele vaardigheden beschikken. Naast technologische expertise omvat dit kennis van (IT-)risicomanagement, bedrijfsprocesanalyse, informatiebeveiliging, testmanagement en communicatie.

Een belangrijk nieuw verantwoordelijkheidsgebied is het definiëren en onderhouden van de Final MBCO in samenwerking met het BCM, inclusief technische haalbaarheidsstudies en het afleiden van geschikte (IT-)herstelstrategieën. Tot zijn taken behoort ook het beheer van externe (IT-)dienstverleners, inclusief het contractueel vastleggen van veerkrachtmaatregelen om risico's uit toeleveringsketens te minimaliseren.

Hij is verantwoordelijk voor de controleerbaarheid, beheersbaarheid en traceerbaarheid van alle IRBC-maatregelen. Deze aspecten worden gespecificeerd als vereisten die onderworpen zijn aan controle en worden tijdens de controle gecontroleerd.

Uitgebreide rol van de IRBC-manager

Wat vereist de norm concreet?

- Strategische verantwoordelijkheid voor het helpen vormgeven van veerkrachtdoelstellingen, budgetplanning en rapportage aan het topmanagement
- Architecturale expertise voor het evalueren en ontwerpen van veerkrachtige IT-landschappen (redundantie, zero trust, cloud failover)
- Coördinatie met BCM & Incident Management/Cyber Incident Response om ervoor te zorgen dat IT-herstel alleen plaatsvindt na forensische goedkeuring, inclusief coördinatie van escalaties
- Verantwoordelijkheid voor de levenscyclus met betrekking tot de ontwikkeling, het onderhoud, het testen en de controle van alle IT-continuïteitsplannen
- Verantwoordelijkheid voor de vereiste vaardigheden, training en middelen voor veerkrachtmaatregelen
- Planning en controle van tests, KPI-tracking en het proces van geleerde lessen voor meting en verbetering
- Beheer van externe (IT-)dienstverleners en vaststelling van contractuele veerkrachtvereisten

Wat houdt dit in?

De IRBC-manager is verantwoordelijk voor de implementatie van de volledige IRBC-levenscyclus – van analyse en oplossingsopties tot het beheer van oefeningen en audits. Bovendien wordt hij in de toekomst de centrale planner van een veerkrachtig IT-landschap dat cyberweerbaarheid integreert en is ontworpen voor het robuuste onderhoud van tijdkritische IT-diensten. Dit omvat het vermogen om alternatieve IT-omgevingen te onderhouden en te activeren voor kritieke IT-incidenten.

Met name in de context van cyberdreigingen (bijv. ransomware, APT) zal hij in de toekomst operationele en strategische verantwoordelijkheid op zich nemen. Dit omvat:

- Ontwikkeling van veerkrachtige (IT-)architecturen: ontwerp met meerdere zones, geautomatiseerde failover, onveranderlijk back-upraamwerk, cloud-exitstrategieën
- Regelmatige Resilience Architecture Reviews (RAR) voor nieuwe of gewijzigde systemen
- Technische beoordeling van de naleving van ICT-RTO, ICT-RPO en Final MBCO – met name in geval van cyberincidenten
- Integratie en coördinatie van respons- en IT-herstelprocessen voor tijdkritische IT-diensten

Uitgebreide rol van de IRBC-manager

Praktijkvoorbeeld: Example Ltd – gereguleerde geharmoniseerde controle

Oorspronkelijk coördineerde de ITSC-manager bij Example Ltd de herstelplanning in overeenstemming met ITIL. Met de introductie van ISO/IEC 27031:2025 werd een speciale IRBC-manager aangesteld met uitgebreide verantwoordelijkheid voor analyse, planning, IT-architectuur, testen en documentatie.

De IRBC-manager introduceerde een jaarlijkse Resilience Architecture Review (RAR), plande een virtuele cloud-failoverzone en liet onveranderlijke back-ups implementeren. Voor elk kritisch IT-systeem

- de BIA-specificaties (bijv. RTO twee uur),
- de technische opties,
- en organisatorische processen

methodisch gecoördineerd.

De afleiding van de IRBC-hersteldoelstellingen uit de BIA is nu gedocumenteerd in:

- het IRBC-oplossingsconcept (met RTO/RPO-mapping)
- het register van maatregelen met evaluatie en goedkeuring
- het protocol met lessen die uit tests zijn getrokken
- het escalatieprotocol voor cyberincidenten

De rol van de IRBC-manager is stevig verankerd in de Resilience Board, met directe verantwoordelijkheid voor het behalen van doelstellingen, effectiviteit en traceerbaarheid van de veerkrachtige IT-architectuur.

Focus op digitale veerkracht en cyberweerbaarheid

SO/IEC 27031:2025 markeert een belangrijke verschuiving in de focus van IRBC. Waar de focus voorheen vooral lag op het herstel van tijdkritische IT-diensten na een kritiek IT-incident, verschuift de focus nu naar het vermogen van IT-systemen en -structuren om functioneel te blijven, adaptief te reageren en gericht te leren, zelfs onder dynamische, onzekere en potentieel destructieve omstandigheden zoals cyberaanvallen. Hierdoor komt het concept van veerkracht centraal te staan in de IRBC-aanpak. Veerkracht wordt niet alleen gezien als een technisch doel, maar als een organisatiebreed, strategisch verankerd managementprincipe.

Deze nieuwe oriëntatie komt met name tot uiting in de eisen voor proactieve planning, continue verbetering, adaptieve organisaties en de ontwikkeling van robuuste maar ook adaptieve systemen. Veerkracht heeft invloed op IT-systemen, maar ook op processen, medewerkers, toeleveringsketens en organisatorische controlemechanismen. Dit maakt IRBC tot een essentieel onderdeel van uitgebreid veerkrachtmanagement, waarbij technische, organisatorische en culturele aspecten evenveel aandacht moeten krijgen.

Bovendien vraagt de norm expliciet om technische maatregelen zoals netwerksegmentatie, redundante gegevensopslag, zero-trust-architecturen, gegevensintegriteitscontroles en herstelmechanismen die zelfs onder actieve aanvalsomstandigheden betrouwbaar functioneren. Deze specificaties zijn gekoppeld aan tijdcontroleparameters en toegewezen aan een gedefinieerd minimaal prestatieniveau (Final MBCO).

Wat betekent dit concreet?

IRBC wordt opgezet als onderdeel van een bedrijfsbrede veerkrachtstrategie. De focus verschuift van pure IT-continuïteitsplanning naar het strategisch veiligstellen van de bedrijfscapaciteit door middel van gecontroleerde respons, aanpassing, robuustheid, redundantie en leervermogen. De focus ligt niet langer op IT-herstel, maar op het behouden van het vermogen om te handelen en op een veerkrachtige manier om te gaan met onzekerheid volgens de volgende principes:

- **Aanpassing:** vermogen om zich aan te passen aan veranderende dreigingssituaties
- **Robuustheid:** weerstand tegen kritieke IT-incidenten of aanvallen
- **Redundantie:** beschikbaarheid van alternatieve middelen en IT-systemen
- **Leervermogen:** het opzetten van feedbackloops op basis van incidenten en oefeningen

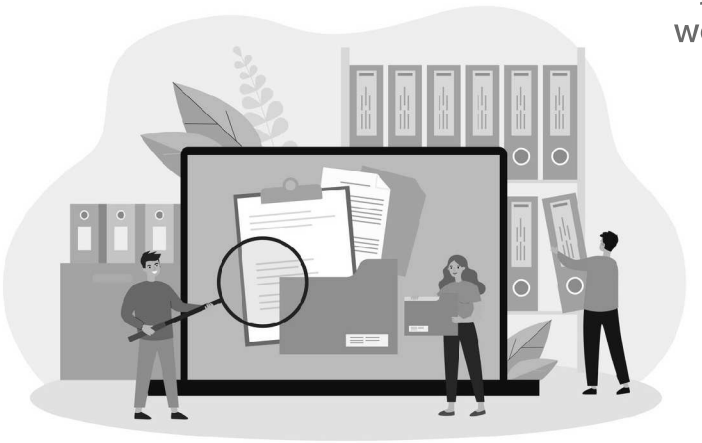
Focus op digitale veerkracht en cyberweerbaarheid

Digitale veerkracht wordt gezien als een strategische doelstelling die moet worden gewaarborgd door middel van technische, organisatorische en strategische maatregelen die veel verder gaan dan klassiek IT-herstel.

Implementatie:

- Afleiding van (IT-)veerkrachtvereisten uit strategische bedrijfsdoelstellingen en (IT-)risicoanalyses
- Integratie van veerkrachtbevorderende principes in IT-architectuur, processen en bedrijfscultuur
- Opzetten van feedback- en leercirkels op basis van oefeningen, IT-tests en kritieke IT-incidenten
- Ontwikkeling van meetbare (IT-)veerkracht-KPI's en regelmatige evaluatie daarvan als onderdeel van managementbeoordelingen

Praktijkvoorbeeld
Example Ltd. exploiteert een platform voor gemeentelijke administratieve processen. Een red team-test simuleerde een ransomware-aanval op het DMS. Hoewel er IT-herstelplannen waren, bleek dat er geen forensisch veilige beslissing over gegevensherstel was genomen.



Tijdens de implementatie van ISO/IEC 27031:2025 werd een cyberweerbaarheidsstrategie ontwikkeld:

- De gegevensback-up werd uitgebreid met onveranderlijke back-ups met geografische redundantie.
- Er werd een gesegmenteerd noodnetwerk technisch geïmplementeerd als een afzonderlijke herstelzone.
- De IT-herstelen gegevensherstelprocessen werden afgestemd op het beheer van cyberincidenten, inclusief forensische vrijgaveprocedures.

Het platform kan nu ook op een gecontroleerde manier worden hersteld tijdens actieve aanvallen, met gedocumenteerde naleving van ICT-RTO en ICT-RPO en traceerbare managementbeslissingen.

Technologische en datagerelateerde focus

De nieuwe norm legt sterk de nadruk op de technologische onderbouwing en gegevensgerelateerde vereisten binnen het kader van IRBC. Veerkracht wordt niet langer alleen op procesniveau bekeken, maar ook expliciet op het niveau van de benodigde IT-middelen, d.w.z. IT-infrastructuren, systemen en applicaties.

De norm vereist dat technologische afhankelijkheden systematisch worden geïdentificeerd, alternatieve leverings- en voorzieningskanalen worden gedefinieerd en de gegevensintegriteit wordt gewaarborgd, zelfs in geval van kritieke IT-incidenten, zoals cyberaanvallen.

De focus ligt op het vermogen om tijdkritische IT-diensten beschikbaar te stellen binnen aanvaardbare hersteltijden. Dit omvat het maken van back-ups en het herstellen van systeemconfiguraties, databases, communicatie-infrastructuren en toegang tot cloudgebaseerde applicaties. Aspecten zoals geografische redundantie, segmentatie van dataverbindingen, beveiliging van SaaS-platforms en de veerkracht van interfaces komen ook expliciet aan bod.

Wat vereist de norm concreet?

De veerkracht van IT-omgevingen en de integriteit van bedrijfskritische gegevens staan steeds meer centraal in de IRBC-planning. De norm vereist een gedetailleerd inzicht in technische afhankelijkheden en een passende en geschikte IT-herstelplanning, met name voor fysieke en virtuele IT-infrastructuren, applicaties, gegevens en cloudgebruik.

Technisch gezien betekent dit dat IT-architecturen vanaf het begin veerkrachtig moeten worden ontworpen en geëxploiteerd, door middel van redundantie, gedistribueerde systemen, geautomatiseerde failover-mechanismen, microsegmentatie of cloudgebaseerde strategieën voor hoge beschikbaarheid. In organisatorisch opzicht vereist de norm het vaststellen van duidelijke verantwoordelijkheden, continue monitoring- en escalatieprocessen en de betrokkenheid van personeel met specifieke expertise om tijdkritische ICT-diensten onder moeilijke omstandigheden in stand te houden.

Technologische en datagerelateerde focus

ISO/IEC 27031:2025 benadrukt in verschillende paragrafen de volgende eisen:

- Documentatie van alle tijdkritische ICT-diensten, inclusief toegewezen hersteltijdwaarden (ICT-RTO, ICT-RPO, Final MBCO) en hun rol in het bedrijfsproces
- IT-componenten (bijv. IT-infrastructuur, IT-systemen, applicaties en interfaces) moeten worden gedocumenteerd voor zowel normale bedrijfsvoering als alternatieve IT-omgevingen, inclusief hun configuratie.
- De norm vereist het gebruik van geschikte IT-technologieën om veerkracht te garanderen, bijvoorbeeld redundantieontwerp, geautomatiseerde failover, cloudclusters en RPO-conforme back-upprocedures met gedefinieerde opslaglocaties en toegangspaden.
- Voor elke tijdkritische ICT-dienst moet duidelijk worden aangetoond welk bedrijfskritisch proces deze ondersteunt en hoe de bijbehorende technologie en IT-architectuurstructuur is ontworpen.
- Afwijkingen tussen de technische IT-prestaties (bijvoorbeeld haalbare ICT-RTO) en de door het BCM gedefinieerde streefwaarden moeten worden geïdentificeerd, op risico's worden beoordeeld, in het managementrapport worden behandeld en worden goedgekeurd.

Implementatie (aanbevolen maatregelen)

Veerkracht door ontwerp:

- Planning van veerkrachtige IT-systeemarchitecturen met redundantie, segmentatie, geautomatiseerde failover-mechanismen, cloudgebaseerde strategieën voor hoge beschikbaarheid

Veerkrachtig gegevensbeheer:

- Beveiligen, isoleren en waarborgen van de beschikbaarheid van gegevens ondanks compromittering

Detectie en controle:

- Integratie van forensische, detectieve en preventieve componenten voor vroege detectie en isolatie

Technologische en datagerelateerde focus

Daarnaast behandelt ISO/IEC 27031:2025 IRBC ook digitale en cybergerelateerde bedreigingen. De norm ondersteunt daarmee de ontwikkeling van een uitgebreid begrip van veerkracht, zoals ook beschreven in

- **DORA**
  - Art. 10: ICT-risicobeheerkader
  - Art. 11: ICT-beleid voor bedrijfscontinuïteit en respons- en herstelplannen

- **NIST Cybersecurity Framework**
  - Functie "Herstellen" (RC.IM-1 tot RC.IM-3)
  - Functies "Reageren" ("Respond", RS) en "Identificeren" ("Identify", ID)

Hierdoor vormt IRBC een integraal onderdeel van IT-risicobeheer en structurele en operationele IT-veerkracht tegen complexe dreigingsscenario's, waaronder die welke worden veroorzaakt door cyberaanvallen.

De tabel geeft een overzicht van de belangrijkste onderwerpen:

Thema	Kerninhoud
Veerkrachtige IT-architectuur	Ontwerp met meerdere zones en regio's, automatische failover-mechanismen, "diepgaande verdediging"
Veerkrachtig gegevensbeheer	Air gap/onveranderlijke back-ups, bescherming tegen crypto-shredding, regelmatige hersteloefeningen
Detectie en controle	Forensische tools, detectie van afwijkingen, mechanismen voor vroegtijdige waarschuwing
Zero Trust & microsegmentatie	Handhaving van minimaal privilege, continue authenticatie, isolatie van gecompromitteerde segmenten
Cloud- en SaaS-afhankelijkheden	Exitstrategieën, multicloudclustering, contractueel bindende RTO/RPO-garanties
Observeerbaarheid en telemetrie	Uniforme logpijplijn, AI-gestuurde detectie van afwijkingen, vroegtijdige waarschuwingsindicatoren voor gegevenscorruptie
Naleving, versleuteling en sleutelbeheer	GDPR/DORA-conforme beleidsregels, controle van de levenscyclus van sleutels, gebruik van HSM

Technologische en datagerelateerde focus

Voor bedrijven betekent dit dat ze niet alleen een IT-noodplan moeten hebben voor IT-herstel, maar ook dat ze moeten zorgen voor de continue werking van hun tijdkritische ICT-diensten en IT-infrastructuren, zelfs onder stress, en dat ze deze capaciteit permanent moeten aantonen door middel van passende maatregelen en documentatie. Veerkracht wordt zo een strategisch doel en IRBC een centrale bouwsteen van digitale bedrijfsveerkracht.

Wat betekent dit voor de implementatie?

- Identificatie van kritieke IT-technologie en data-afhankelijkheden als onderdeel van (IT-)risicoanalyse
- Definitie van redundante datapaden en IT-herstelconcepten voor hybride IT-omgevingen
- Planning van scenario's voor gegevens- en applicatieherstel, inclusief een IT-teststrategie
- Waarborging van de integriteit en beschikbaarheid van gegevens, zelfs in aanvalsscenario's

Alleen IT-herstelplanning en/of back-upscripts zijn niet langer voldoende. Bedrijven moeten hun IT-technologieën consequent afstemmen op hun doelstellingen op het gebied van veerkracht.

Typische stappen zijn onder meer:

- Resilience Architecture Review (RAR) voor elk groot IT/OT-project, inclusief controle van geografische redundantie, segmentatie-indeling en afhankelijkheidsmapping
- Onveranderlijk back-upraamwerk en afzonderlijke inloggegevens, eenmalig-schrijvenbeleid, regelmatige geautomatiseerde hersteltests in een geïsoleerde sandbox
- Continue hardening & patch-pijplijn, infrastructuur-als-code
- Cloud-exit-oefeningen naar alternatieve provider/on-prem cluster, inclusief gedocumenteerde RTO-meting
- Op telemetrie gebaseerde vroegtijdige waarschuwing – gegevensvertraging, snapshot-gezondheidsscore, gemiddeld succespercentage van failover; rechtstreeks rapporteren aan de Resilience Board

Technologische en datagerelateerde focus

Praktisch voorbeeld: Example Ltd – Veerkrachttechnologie als IT-architectuurprincipe

Example Ltd exploiteert een hybride datacenter met SaaS- en platformdiensten. Uit een audit bleek dat de hersteldoelstellingen voor het gegevensarchief niet in overeenstemming waren met de BIA. Vereiste RPO volgens BCM: twee uur; technisch haalbaar: acht uur

Als gevolg hiervan werd een Resilience Architecture Review (RAR) opgesteld:

- Segmentatie van de databaseverbinding voor isolatie in geval van een aanval
- Introductie van onveranderlijke back-up, afzonderlijke opslag van inloggegevens, geautomatiseerde hersteltest
- Cloud exit-oefening inclusief RTO-meting en documentatie
- Gap-analyse in een IRBC-technologiematrix; rapportage aan de Resilience Board

De maatregelen werden vastgelegd als een technologisch veerkrachtkader in het IRBC-documentatiesysteem, inclusief de gap-status voor BIA-RTO/BIA-RPO en lessen die zijn geleerd uit oefenscenario's.

Bedrijfsvereisten en op BIA gebaseerde controle

Niet nieuw in de praktijk, maar een belangrijke eis van ISO/IEC 27031:2025 is de consistente afleiding van alle IRBC-maatregelen uit zakelijke vereisten. In plaats van alleen IT-hersteltijden te specificeren, vereist de norm dat de bedrijfsimpactanalyse (BIA), risicobeoordeling en ICT-hersteldoelstellingen nauw met elkaar worden verbonden.

Nieuw is de duidelijke scheiding tussen bedrijfscontinuïteitsdoelstellingen (BIA-RTO/RPO) en technische IT-doelstellingen (ICT-RTO/RPO). Het volgende geldt: ICT-RTO/RPO ≤ BIA-RTO/RPO. Afwijkingen moeten worden weggewerkt door investeringen of worden gedocumenteerd als een risico in het Final MBCO-proces.

De nieuwe norm vereist volledige traceerbaarheid (bewijsketen) van het bedrijfsproces tot het IT-testbewijs. Elke opdracht moet worden gedocumenteerd en jaarlijks of bij belangrijke wijzigingen worden herzien.

Dit creëert een gesloten keten van:

Bedrijfsproces → Kritikaliteits-/BIA-beoordeling → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → Final MBCO → Strategie &pPlan

Wat vereist de norm precies?

ICT-diensten moeten worden geanalyseerd op basis van procesafhankelijkheid, kriticiteit en herstelprioriteit. Hieruit worden streefwaarden (RTO, RPO, MBCO), herstelstrategieën en middelen afgeleid, waarbij rekening wordt gehouden met externe vereisten.

Organisaties moeten ervoor zorgen dat elk IT-middel aantoonbaar zo is ingericht dat wordt voldaan aan de door de gespecialiseerde afdeling gedefinieerde BIA-RTO/RPO. De belangrijkste passages van de normtekst kunnen als volgt worden gegroepeerd:

Hoofdstuk	Kernvereiste
Zakelijke verwachtingen voor IRBC	• Identificatie van kritieke bedrijfsprocessen en hun ICT-afhankelijkheden • Bepaling van initiële MBCO & prioriteiten • Documentatie van externe/wettelijke vereisten
Definitie van voorwaarden voor IRBC	• Afleiding van ICT-RTO/RPO uit BIA-resultaten • Bepaling van Final MBCO na risico- en haalbaarheidscontrole • Validatie van doelstellingen door het management
IT-continuïteitsplan	• Plannen moeten RTO/RPO, tijdelijke oplossingen en de overgang van IT-noodsituatie naar normale IT-werking (Final MBCO → volledig herstel) weerspiegelen

Bedrijfsvereisten en op BIA gebaseerde controle

De norm vereist ook:

- Elke toewijzing van proces → IT-middel → RTO/RPO moet worden opgeslagen in een traceerbare traceerbaarheidsmatrix.
- Ten minste eenmaal per jaar – of in geval van belangrijke wijzigingen – moeten BIA-RTO/RPO, MBCO en ICT-RTO/RPO gezamenlijk worden geverifieerd.
- Als er hiaten bestaan, moeten technische maatregelen, alternatieve strategieën of formele risicoacceptatie (Final MBCO) worden gedocumenteerd en goedgekeurd door het topmanagement.
- Elke ICT-RTO moet worden geverifieerd door middel van geplande oefeningen of failover-tests; de resultaten worden verwerkt in de geleerde lessen.

Wat betekent dit voor de implementatie?

Door de consistente scheiding van BIA-RTO/RPO en ICT-RTO/RPO verschuift de focus van puur technische IT-herstelplanning naar bedrijfsgestuurd veerkrachtmanagement. Bovenal vereist de norm een consistent bewijsketenprincipe. Dit betekent dat elke technische vereiste traceerbaar moet zijn naar de uiteindelijke IT-systeemconfiguratie en het uiteindelijke testbewijs.

Bedrijven moeten daarom hun continuïteitsbeheer zodanig afstemmen dat

- de gespecialiseerde afdelingen bindende procestolerantietijden specificeren,
- het IRBC-team deze waarden direct vertaalt naar uitvoerbare IT-doelstellingen,
- alle tussenstappen (MBCO → ICT-RTO/RPO → Final MBCO) op een transparante, versiebeheerde en controleerbare manier worden gedocumenteerd.

Dit vereist niet alleen een nauwe afstemming tussen BCM, IRBC en (IT-)risicomanagement, maar ook investeringsplanning om technische hiaten te dichten of risico's formeel te accepteren. Alleen wanneer deze traceerbaarheidsketen volledig is gedocumenteerd, wordt aan de normvereiste geacht te zijn voldaan.

Er moeten gestructureerde methoden voor kriticiteitsbeoordeling, afhankelijkheidsanalyse en doelafleiding worden vastgesteld. IRBC wordt zo een integraal onderdeel van de operationele (IT-)risico- en veerkrachtbeoordeling.

Bedrijfsvereisten en op BIA gebaseerde controle

Praktijkvoorbeeld: Example Ltd

Example Ltd exploiteert clouddiensten voor gemeentelijke belastingportalen. De BIA heeft vastgesteld dat de afdelingen die verantwoordelijk zijn voor het belastingcontroleportaal een maximale onderbreking van vier uur accepteren (BIA-RTO). Uit de gap-analyse bleek echter dat bij een volledige storing het herstel van de cloudinfrastructuur ongeveer zes uur duurt (ICT-RTO).

Als gevolg hiervan zijn de volgende maatregelen genomen:

- Technische upgrade van de opslaglaag met snapshot-replicatie
- Aanpassing van de IRBC-oplossingsoptie (bijv. failover)
- Formele risicoacceptatie door het topmanagement tot aan de implementatie

Alle stappen werden gedocumenteerd in een traceerbaarheidsmatrix:

- Bedrijfsproces → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → Final MBCO → Strategie & Herstelplan
- Bovendien werd de nieuwe waarde geverifieerd in de IT-functietest en geïntegreerd in het IRBC-testrapport.

Dit betekent dat de BIA-koppeling technisch, organisatorisch en documentair is geverifieerd.

Risicogebaseerde planning en Final MBCO

De MBCO (Minimum Business Continuity Objective) is geen nieuwe uitvinding in de huidige norm. Nieuw is echter de uitgebreide aanpak in ISO/IEC 27031:2025, waarin de zogenaamde definitieve MBCO wordt geïntroduceerd. De MBCO beschrijft het minimaal vereiste prestatieniveau van een tijdkritisch bedrijfsproces of de ondersteunende ICT-dienst die bij een kritiek (IT-)incident moet worden gehandhaafd of binnen de RTO moet worden bereikt om ernstige gevolgen te voorkomen. De MBCO is afgeleid van de BIA.

De Final MBCO is het gevalideerde resultaat van een planningsproces waarin niet alleen het pure BIA-resultaat wordt afgeleid, maar ook de BIA-resultaten op risicogebaseerde basis worden afgeleid, rekening houdend met:

- technische en organisatorische haalbaarheid
- technische en organisatorische afhankelijkheden (bijv. toeleveringsketens, (IT-)dienstverleners)
- dreigingsscenario's en kwetsbaarheden
- bevindingen uit tests, oefeningen en audits

De Final MBCO dient als plannings- en controlevariabele voor alle (IT-) en organisatorische maatregelen die verder gaan dan directe IT-noodoperaties en bedoeld zijn om een stabiele bedrijfsvoering te waarborgen. Daarnaast is een risicogebaseerde afleiding en validatie van continuïteitsdoelstellingen vereist.

Dit betekent dat RTO-, RPO- en MBCO-waarden niet statisch moeten worden vastgesteld, maar regelmatig moeten worden herzien en aangepast in het kader van mogelijke dreigingsscenario's, waarschijnlijkheid van optreden en schade-effecten.

De Final MBCO moet formeel worden gedocumenteerd, op risicogebaseerde wijze worden gevalideerd en door het management worden goedgekeurd. Het is daarom bindend voor de planning van kritieke IT-incidenten en de IT-herstelstrategie. De Final MBCO is dus niet alleen een analyseresultaat, maar een gespecificeerd en gedocumenteerd doel.

Risicogebaseerde planning en Final MBCO

Wat vereist de norm concreet?

De norm vereist een expliciet onderscheid tussen tijdelijke IT-noodoperaties (MBCO) en de definitieve (IT-)operationele doelstelling (Final MBCO). Deze streefwaarde is cruciaal voor (IT-)herstelplanning, prioritering van middelen en het ontwerp van (IT-)herstel-strategieën. De Final MBCO dient als plannings- en controlevariabele voor alle maatregelen die verder gaan dan onmiddellijke noodvoorzieningen en bedoeld zijn om stabiele bedrijfsactiviteiten te herstellen. In één oogopslag:

- Expliciete scheiding tussen MBCO en Final MBCO
- Risicogebaseerde validatie: technische haalbaarheid, afhankelijkheden, leveranciers, personeel
- Goedkeuring door het management van de Final MBCO, inclusief gedocumenteerde risicoacceptatie
- Afleiding van plan en strategie: herstelstappen moeten aangeven hoe de overgang van noodsituatie naar Final MBCO zal plaatsvinden.
- Herziening ten minste eenmaal per jaar of bij belangrijke wijzigingen; verificatie in managementbeoordeling

De hersteldoelstellingen worden niet afzonderlijk gedefinieerd, maar worden geanalyseerd en gevalideerd in de context van een realistisch, op risico's gebaseerd totaalbeeld. Dit is bedoeld om de strategische betrokkenheid bij de IT-herstel-doelstellingen te vergroten en inconsistenties tussen het bedrijfs- en IT-perspectief te minimaliseren. De validatie van de Final MBCO is bedoeld om ervoor te zorgen dat alle IT-herstelplannen organisatorisch, technisch en contractueel haalbaar zijn.

Wat betekent dit voor de implementatie?

De implementatie van risicogebaseerde planning begint met een uitgebreide analyse op basis van de uitgevoerde BIA. Ook moet rekening worden gehouden met de waarschijnlijkheid van optreden, afhankelijkheden van leveranciers en dreigingsscenario's. Dit detailniveau is bedoeld om duidelijk te maken waar puur technische IT-herstelcapaciteiten alleen niet voldoende zijn.

- Risicogebaseerde planning = BIA + (IT-)risico- en afhankelijkheidsfactoren (bedreigingsscenario's, IT-dienstverleners, haalbaarheid)

De norm beschrijft dit onder "Inputs uit business impact analysis" en vereist dat het topmanagement de op deze manier vastgestelde resultaten en vereisten formeel bevestigt.

Risicogebaseerde planning en Final MBCO

De implementatiestappen in detail:

1. **Uitgebreide analyse**
Op basis van de BIA worden bedreigingen, waarschijnlijkheid van optreden en afhankelijkheden vastgelegd.

2. **Haalbaarheidsanalyse**
Er worden hiaten vastgesteld tussen de doelstelling (BIA-RTO/RPO) en de feitelijke technische/organisatorische mogelijkheden (ICT-RTO/RPO).

3. **Risicogebaseerde beslissing**
Investering of formele risicoacceptatie door goedkeuring van hogere definitieve MBCO door de Resilience Board.

4. **Documentatie en versiebeheer**
Update van de Final MBCO in de traceerbaarheidsmatrix, het IT-herstelplan, het risicoregister en de auditdocumentatie.

5. **Testen en beoordelen**
Voer scenariotests uit en valideer de overgang van MBCO naar Final MBCO. Neem de resultaten op in het KPI-dashboard en de geleerde lessen.

Praktisch voorbeeld: Example Ltd – MBCO versus Final MBCO

Example Ltd exploiteert een centraal claim-verwerkingssysteem voor klanten in de verzekeringssector. De BIA specificeert de MBCO als volgt: noodbedrijf door middel van handmatige verwerking, beperkte gegevens-opvraging gedurende maximaal 48 uur.

Uit een gap-analyse blijkt dat volledig herstel van de ICT-dienst (met klantenportaal, databasereplicatie en CRM-integratie) pas na 72 uur mogelijk is.

Dit resulteert in een Final MBCO: systeemwerking met 80 procent functionaliteit na 72 uur, inclusief actuele gegevensstatus

De Resilience Board aanvaardt de gap door middel van een formeel besluit. De Final MBCO wordt gedocumenteerd, getest en meegenomen in de IT-herstelplanning.

Herstelplanning en documentatievereisten

IRBC-plannen moeten niet alleen technische IT-herstelprocessen omvatten, maar ook organisatorische procedures, tijdelijke oplossingen en communicatiekanalen. In de editie van 2011 werden continuïteitsplannen aanbevolen, maar deze werden voornamelijk beschouwd als aanvullende technische hulpmiddelen voor DR-projecten. In de herziening van 2025 worden ze verheven tot een centrale "effectiviteitscontrole". Een plan voldoet alleen aan de norm als het

- duidelijk het onderscheid weergeeft tussen zakelijke RTO/RPO en ICT-RTO/RPO,
- verwijst naar de Final MBCO als een bindende streefwaarde,
- aantoonbaar up-to-date wordt gehouden via een gecontroleerde levenscyclus met versiebeheer, tests en beoordelingen.

Statische handleidingen moeten worden omgezet in versiebeheer, ongeacht het medium. De verifieerbare koppeling van inhoud, goedkeuring, testen en geleerde lessen is cruciaal.

Plannen moeten rolgebonden, scenario-gerelateerd, volledig gedocumenteerd, regelmatig getest, bijgewerkt en geïntegreerd zijn in de BCM-documentatie. Communicatie-, escalatie- en besluitvormingsprocessen moeten op bindende wijze worden geregeld. De norm definieert zeven verplichte inhoudsblokken.

Sectie	Inhoud
Doel en reikwijdte	Koppeling met BIA, kritieke diensten, triggercriteria
Herstelorganisatie	Rollen, escalatiepaden, contactgegevens, plaatsvervangers
Doelmatrix	Bewijs dat ICT-RTO/RPO ≤ BIA-RTO/RPO, inclusief Final MBCO-referentie
Stapsgewijze runbooks	Technische procedures, tijdelijke oplossingen, overgang naar noodbedrijf
Communicatiekanalen	Goedkeuringsstroom, coördinatie met incidentrespons & BCM
Leveranciers en afhankelijkheden	Contacten, SLA's, testrapporten, ontsnappingsclausules
Levenscyclusverificatie	Versiebeheer, tests, beoordelingen, geleerde lessen

Het is van cruciaal belang dat alle informatie op een auditbestendige manier wordt opgeslagen en snel beschikbaar is, zelfs in het geval van een IT-storing.

Herstelplanning en documentatievereisten

Wat betekent dit voor de implementatie?

In de praktijk vertaalt deze eis zich in een afzonderlijk, controleerbaar **document-beheerproces** binnen de IRBC. Bedrijven moeten een uniform plansjabloon definiëren, een versiebeheer- en goedkeuringslogica vaststellen en een bindende testkalender vastleggen. Of ze nu een DMS, een auditbestendige Git-repository of een fysiek beheerde noodmap gebruiken, is van ondergeschikt belang. Belangrijk is dat wijzigingen, tests en beoordelingen op een traceerbare manier worden geregistreerd en dat er altijd een **kopie offline beschikbaar** is. Daarnaast is het zeer zinvol om een automatische koppeling met wijzigings- en incidentbeheer in te stellen, zodat elke relevante wijziging in IT-systemen of -processen automatisch een planbeoordeling activeert en testresultaten worden opgenomen in een KPI-dashboard voor veerkracht.

Implementatiestappen

1. Plan-sjabloon definiëren – uniforme structuur voor auditbewijs
2. Documentcontrole opzetten, inclusief goedkeuringsworkflow
3. Koppel wijzigingstriggers – relevante wijzigingen leiden automatisch tot herzieningen van het plan
4. Zorg voor offline beschikbaarheid – kopieën in IT-nood- en/of crisiskamers, noodlaptops of beveiligde cloudomgeving

Levenscyclus van het plan

Creatie → Versiebeheer → Testen → Beoordeling → Geleerde lessen → Bijwerken

- Versiebeheer: elke wijziging met release-opmerking (eigenaar en datum)
- Voer regelmatig tests uit, op vaste tijdstippen of wanneer er wijzigingen in het systeem worden aangebracht
- Neem de resultaten van de beoordeling op in het managementrapport
- Geleerde lessen: verbeteringen en KPI-vergelijkingen documenteren

IRBC-strategieën en herstelontwerp

ISO 27031:2025 structureert de selectie van IRBC-strategieën aan de hand van zes impactcategorieën. Het doel is om een holistisch veerkrachtontwerp te realiseren dat technische, organisatorische en leveranciersgerelateerde aspecten integreert. Strategieën mogen niet afzonderlijk worden bekeken, maar moeten in hun onderlinge samenhang worden gezien om consistente en economisch haalbare oplossingen te creëren.

Er moeten strategieën of oplossingen worden afgeleid voor de categorieën vaardigheden, faciliteiten, technologie, gegevens, processen en leveranciers. De selectie moet risicogebaseerd, economisch haalbaar en gecoördineerd zijn. Interacties moeten worden geanalyseerd en strategieën op een begrijpelijke manier worden gedocumenteerd.

Wat vereist de norm concreet?

Voor elk van de zes categorieën moeten strategieën of oplossingsconcepten worden ontwikkeld, geëvalueerd en gedocumenteerd:

Categorie	Typische opties	Selectiecriteria
Vaardigheden en kennis	Cross-training, redundantie van vaardigheden, certificeringen	Kritieke vaardigheden, beschikbaarheid van experts
Faciliteiten	Tweede locatie, carrier-neutraal datacenter, mobiel datacenter	Geo- en klimaatrisico's, connectiviteit
Technologie	Actief-actief cluster, geautomatiseerde failover, zero-trust segmenten	RTO/RPO, complexiteit, licentiemodellen
Data	Onveranderlijke back-ups, air gap, realtime replicatie	RPO-vereisten, gegevensvolume, latentie
Processen	Geautomatiseerde runbooks, SOAR-playbooks, escalatiematrix	Proceskriticiteit, automatiseringsvolwassenheid
Leveranciers	Multi-cloudstrategieën, failover van providers, exitclausules	Afhankelijkheidsrisico's, SLA-kwaliteit, contractuele boetes

IRBC-strategieën en herstelontwerp

Wat betekent dit voor de implementatie?

- Strategieën moeten worden gekozen op basis van risico en economische haalbaarheid.
- Interacties en afhankelijkheden moeten worden geanalyseerd en gedocumenteerd.
- Elke strategie moet worden afgestemd op de gedefinieerde RTO/RPO/MBCO-doelstellingen.
- De implementatie moet regelmatig worden geëvalueerd en bijgestuurd.

Bedrijven moeten een gestructureerd proces voor strategieontwikkeling opzetten. Dit omvat ten minste:

- Beoordelingsschema voor risico's, kosten, complexiteit en haalbaarheid
- Scenariovergelijkingen (bijv. technisch versus organisatorisch herstelontwerp)
- Economische analyses (CAPEX, OPEX, levenscycluskosten)
- Een centraal document met de veerkrachtstrategie dat als referentie dient voor planning, tests en audits

Praktijkvoorbeeld

Voor een cruciaal klantenserviceplatform wordt een combinatie van cloud-failover, gedecentraliseerde IT-noodoperaties en handmatige workarounds ontwikkeld. De strategie wordt regelmatig gevalideerd en gedocumenteerd met belanghebbenden.

Implementatieaanbevelingen voor bedrijven

Overgang van ISO 27031:2011 naar de versie van 2025

Voor bedrijven die eerder volgens ISO/IEC 27031:2011 of een klassiek IT-rampherstel-raamwerk hebben gewerkt, wordt een migratiemodel in drie fasen aanbevolen. Het doel is om de nieuwe governancevereisten, uitgebreide documentatieverplichtingen en het concept van Final MBCO geleidelijk te integreren zonder de lopende IT-activiteiten te overbelasten.

Stap 1 – Gap-analyse

Doelstelling: de huidige status vastleggen en hiaten identificeren ten opzichte van ISO/IEC 27031:2025

Procedure:

- Verzamel alle relevante documenten: ICT-continuïteitsplannen, noodhandleidingen, testrapporten, BIA-resultaten, auditrapporten
- Vergelijk de documenten met de 13 hoofdstukken van de norm
- Veelvoorkomende hiaten:
  - Ontbreken van IRBC-beleid
  - Onvolledige traceerbaarheid van BIA-doelstellingen naar ICT-RTO/RPO
  - Geen veerkrachtraad
  - Ontbrekende KPI's voor RTO/RPO-meting
- Opstellen van een volwassenheidsoverzicht (0–5) en afleiden van quick wins:
  - Aanstelling van een IRBC-manager
  - Eenvoudig KPI-dashboard
  - Eerste versie van de traceerbaarheidsmatrix

Implementatieaanbevelingen voor bedrijven

Stap 2 – Prioritaire hiaten dichten

Governance:

- Publicatie van het IRBC-beleid met goedkeuring van het management
- Oprichting van de Resilience Board (BCM, IRBC, ISMS, risicobeheer, ICT-operaties)
- Goedkeuring van het begrotingskader voor IRBC-maatregelen

Documentatie:

- Volledige traceerbaarheidsmatrix: Bedrijfsproces → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → Final MBCO → testverificatie
- Integratie in documentbeheer

Technische maatregelen:

- Versiebeheer van alle ICT-continuïteitsplannen
- Offline voorzieningen (crisisruimte, noodlaptops, beveiligde cloud)
- Testkalender (minstens één live failover- of hersteloefening per jaar)
- Initiële onveranderlijke back-up- en air gap-strategieën

Stap 3 – Optimalisatie en auditgereedheid

Optimalisatie:

- KPI-dashboards in reguliere bedrijfsvoering
- Systematisch proces voor het leren van lessen
- Scenario-oefeningen (bijv. ransomware, leveranciersfalen, uitval van de belangrijkste cloudregio)
- Bewijs van het vermogen om over te stappen op MBCO → Final MBCO

Auditgereedheid:

- Volledige bewijsketen
- Auditrepository met IRBC-beleid, traceerbaarheidsmatrix, plannen, testrapporten, protocollen voor managementbeoordeling

Implementatieaanbevelingen voor bedrijven

Implementatietabel

Actie	Verantwoordelijk
IRBC-beleid opstellen en goedkeuren	IRBC-manager, management
Opzetten van een Resilience Board	Management
Implementatie van traceerbaarheidsmatrix	IRBC-manager, BCM
Testkalender opstellen	IRBC-manager, ICT-operaties
Onveranderlijke back-up implementeren	ICT-operaties
Oefening met ransomware-scenario	IRBC-manager, ISMS
Documenteren en goedkeuren van Final MBCO	IRBC-manager, management
Controle uitvoeren op gereedheid voor audit	IRBC-manager, interne audit

Implementatieaanbevelingen voor bedrijven

Overgang van klassiek ITSCM naar ISO/IEC 27031:2025

Bedrijven die voorheen klassiek IT-servicecontinuïteitsbeheer (ITSCM) volgens ITIL-principes hebben toegepast, moeten hun aanpak strategisch uitbreiden. Terwijl ITSCM zich richt op het technische IT-herstel van individuele ICT-diensten, integreert ISO 27031 IRBC in het BCMS als een strategisch onderdeel van de veerkracht.

1. **Governance**
   - Oprichting van een veerkrachtraad
   - Aanpassing van de rol van ITSCM-manager aan die van IRBC-manager
   - Invoering van driemaandelijkse managementbeoordelingen
2. **Documentatie**
   - Omzetting van DR-plannen in volledige ICT-continuïteitsplannen
   - Invoering van een traceerbaarheidsmatrix
   - Versiebeheer en auditbestendige opslag
3. **Integratie**
   - Integratie van ITSCM met BCM, ISMS en incidentrespons
   - Afstemming op ISO 27002 A.5.30 en A.8.16
   - Uniforme escalatie- en goedkeuringsprocessen
4. **Aanpassing van teststrategie**
   - Technische failover-tests handhaven
   - Toevoeging van scenario-gebaseerde oefeningen (cyberaanval, cloudstoring, leverancierssstoring)
   - Lessen integreren in plannen en KPI's

Vooruitzichten

ISO/IEC 27031:2025 vertegenwoordigt de overgang van technische noodplanning naar strategisch, organisatiebreed veerkrachtmanagement. Bedrijven moeten hun structuren, processen en rollen hierop aanpassen om aan de uitgebreide eisen te voldoen.

Heeft u vragen over dit onderwerp? Neem dan gerust contact met ons op!

Controllit AG
Kühnehöfe 20
22761 Hamburg
Duitsland
www.controll-it.de

Vanaf september 2025

Controllit AG is uw partner voor bedrijfscontinuïteitsbeheer (BCM). Sinds onze oprichting ontwikkelen we integratieve concepten en producten voor bedrijfscontinuïteitsbeheer, IT-servicecontinuïteitsbeheer en crisisbeheer. Wij helpen u met strategische, organisatorische en technische concepten om uw bedrijfsprocessen te beveiligen tegen bedreigingen en u voor te bereiden op noodsituaties.

Foto-/grafische credits: Omslag: iStock.com/treety ; S. 3: iStock.com/pishit; S. 7: iStock.com/TCmake_photo; S. 10: iStock.com/BRO Vector; S. 12: iStock.com/Imam Fathoni; S. 17: iStock.com/Alexey Yaremenko; S. 20: iStock.com/BRO Vector; S. 25: iStock.com/BRO Vector; S. 28: iStock.com/TCmake_photo; S. 31: iStock.com/TCmake_photo; S. 35: iStock.com/Iryna Spodarenko