Whitepaper

Der neue ISO-Standard ISO/IEC 27031:2025

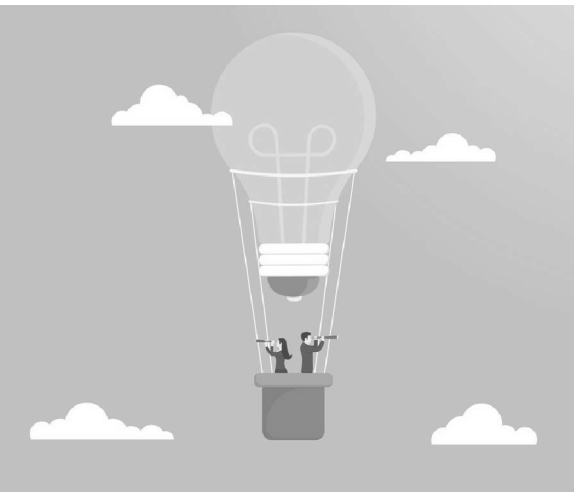
So gelingt die Anpassung von technischer Notfallplanung zu einem strategischen, organisationsweiten Resilienzmanagement.

controllit
Business Continuity Management

Inhalt

Einleitung

Die ISO/IEC 27031 wurde im Mai 2025 grundlegend überarbeitet und ersetzt die Ausgabe von 2011. Statt einer rein technischen IT-Wiederanlaufplanung verfolgt die neue Norm einen umfassenden Resilienzansatz. ICT Readiness for Business Continuity (IRBC) wird dabei als integraler Bestandteil der Unternehmensstrategie verstanden und soll eng mit Business Continuity, Informationssicherheit, Incident Response und Risikomanagement verzahnt sein.



Neu ist die klare strategische Verankerung von IRBC in Führungs- und Steuerungsstrukturen. Rollen, Verantwortlichkeiten und Kompetenzen sind verbindlich zu definieren. Die Anforderungen gelten auch unter Bedingungen aktiver Cyberangriffe (z. B. Ransomware, APT), was die Rolle des IRBC-Verantwortlichen deutlich erweitert – hin zum Mitgestalter resilienter ICT-Architekturen.

Unternehmen müssen dokumentierte Lösungen bereitstellen, die Redundanz, Cloud- und Lieferkettenabhängigkeiten berücksichtigen und auf RTO, RPO und das neu eingeführte Final-MBCO abgestimmt sind. Die Norm fordert außerdem ein strukturiertes Test-, Übungs- und Auditprogramm mit Leistungskennzahlen, systematischer Auswertung und Lessons Learned.

Bestehende ITSCM-/IRBC-Systeme können weiterhin verwendet werden, sofern sie die neuen Anforderungen funktional abdecken. Dazu gehören eine klare Governance-Anbindung, die Einbindung in bestehende Managementsysteme, die Bestimmung des Final-MBCO sowie kontinuierliche Verbesserungsprozesse. Die Norm verzichtet auf eine explizite Nennung des PDCA-Zyklus, folgt jedoch weiterhin dem Prinzip der kontinuierlichen Verbesserung: von Planung über Umsetzung und Prüfung bis zur strategischen Bewertung durch das Management.

Dieses Whitepaper stellt die wesentlichen Änderungen im Vergleich zur ISO/IEC 27031:2011 dar, ordnet diese strategisch ein und analysiert deren Auswirkungen auf regulierte Unternehmen sowie auf bestehende Managementsysteme im Bereich des IT Service Continuity Management (ITSCM) und IRBC. Dabei werden Elemente aus angrenzenden Standards wie ISO/IEC 22301 (Business Continuity Management), ISO/IEC 27001 (Information Security Management), dem NIST Cybersecurity Framework sowie bewährte ITSCM-Methoden berücksichtigt.

Vertiefung der zentralen Veränderungen

Die neue ISO/IEC 27031:2025 wirkt sich spürbar auf die strategische und operative Praxis des IRBC bzw. des ITSCM aus. Im Mittelpunkt steht die stärkere Verzahnung mit dem BCM nach ISO 22301. IRBC-Ziele werden jetzt gemeinsam mit den Ergebnissen der BIA festgelegt, so dass RTO, RPO und das neue Final-MBCO jederzeit nachvollziehbar miteinander verknüpft sind.

Gleichzeitig erweitert die neue Norm ihren Fokus auf benachbarte Standards. Die Norm selbst verweist ausschließlich auf ISO-/IEC-Standards (z. B. ISO 22301, 27002). Unternehmen können aber die Controls auf regulatorische Vorgaben wie DORA oder NIS-2 sowie Frameworks wie NIST-CSF oder NIST SP 800-61 abbilden, um Synergien zwischen Informationssicherheits-, Kontinuitäts- und Incident-Response-Prozessen zu schaffen. Unternehmen können z. B. dadurch Kontrollen wie ISO 27002 Control 5.30 in ihr IRBC-Framework übernehmen und sie regulatorisch belegen.

Ein zentrales Element ist die formalisierte Governance. Die Rolle des IRBC-Managers erhält klar definierte Befugnisse, berichtet an ein zu etablierendes interdisziplinäres IRBC-Lenkungsgremium und steuert ein konsolidiertes Kennzahlenset (KPI). Diese Kennzahlen reichen von der Einhaltung der IT-Wiederanlaufzeiten bis zu Messwerten aus Tests und Audits. Der IRBC-Manager agiert damit zukünftig als Schnittstelle zwischen IT-technischer Umsetzung und Top-Management.

Die BIA bleibt weiter Dreh- und Angelpunkt, wird jedoch um einen durchgängigen Traceability-Ansatz erweitert. Fachliche ICT-RTO und ICT-RPO leiten IT-technische Zielwerte ab. Lücken werden entweder durch Investitionen geschlossen oder als Risiko akzeptiert und im Final-MBCO dokumentiert. Dieser Final-MBCO definiert das niedrigste akzeptable Leistungsniveau nach Abschluss der IT-Wiederanlaufs und erhöht so die Transparenz in Situationen, in denen Idealziele kurzfristig nicht erreichbar sind.

Strategische Neuausrichtung und Integration mit ISO 22301

Die ISO/IEC 27031:2025 verankert IRBC deutlich stärker im strategischen Kontext als bisher und betont die Relevanz von IT-Resilienz als integralen Bestandteil eines Business-Continuity-Management-Systems (BCMS). IRBC wird nicht mehr nur als rein technische Reaktion auf kritische IT-Vorfälle verstanden, sondern als strategisch verankertes Steuerungsinstrument innerhalb des BCMS gemäß ISO 22301. Das umfasst gemeinsame Zieldefinitionen, abgestimmte (IT-)Risiko- und Business-Impact-Analysten (BIAs), koordinierte Governance-Strukturen sowie eine konsistente (IT-)Test- und Übungsstrategie. Die Schnittstellen zu BCM wie der Business-Impact-Analyse (BIA), der (IT-)Risikobewertung, koordinierten Governance-Strukturen sowie einer konsistenten (IT-)Test- und Übungsstrategie sind explizit herausgearbeitet.

Diese Neuausrichtung manifestiert sich in der expliziten Forderung nach strategischer Integration und gegenseitiger Abhängigkeit der Disziplinen. Ziel ist nicht mehr allein der Wiederanlauf der IT, sondern die resiliente Betriebsfähigkeit zeitkritischer IT-Services im Einklang mit den Anforderungen der zeitkritischen Geschäftsprozesse. IT wird dabei als wertschöpfungsrelevanter Faktor mit hoher Resilienzanforderung positioniert.

Die strategische Ausrichtung schlägt sich in mehreren Elementen nieder:

- IRBC ist künftig strategisch mitzugestalten und in die Resilienzstrategie des Unternehmens einzubinden.
- Die Integration mit dem BCMS ist ein zentrales Element.
- Die Norm formuliert klare Anforderungen an Steuerung, Koordination und gegenseitige Ableitung von Zielgrößen wie RTO, RPO und Final-MBCO.
- Die Trennung von technischen und organisatorischen Resilienzmaßnahmen wird zugunsten eines integrierten Ansatzes aufgehoben.
- Die Verantwortung für IRBC liegt nicht mehr primär in der IT, sondern erfordert eine interdisziplinäre Governance.

Strategische Neuausrichtung und Integration mit ISO 22301

Was fordert die Norm konkret?

Während die ISO/IEC 27031:2011 die Integration in das BCM nur indirekt voraussetzte, schreibt die überarbeitete Fassung von 2025 diese nun explizit und verbindlich vor. Die Norm verlangt insbesondere:

- gemeinsame Zieldefinitionen im BCMS
- abgestimmte (IT-)Risiko- und Business-Impact-Analysen
- koordinierte Governance-Strukturen
- integrierte IT-Test- und -Übungsstrategien

Was bedeutet das für die Umsetzung?

Unternehmen müssen sicherstellen, dass IRBC-Maßnahmen nicht losgelöst, sondern als Teil des BCM entwickelt und betrieben werden. Dazu gehören gemeinsame Planungsprozesse, integrierte Dokumentation sowie regelmäßige Abstimmung zwischen IRBC- und BCM-Verantwortlichen. Die IT-Kontinuitätsanforderungen leiten sich direkt aus BIA-Ergebnissen ab. Die Norm fordert eine koordinierte Steuerung beider Disziplinen. Das umfasst unter anderem:

- gemeinsame abgestimmte Zielwerte (RTO, RPO, Final-MBCO)
- synchronisierte (IT-)Risiko- und BIA-Prozesse
- verzahnte Governance-Strukturen und Reporting-Linien
- abgestimmte (IT-)Notfallkommunikation und Eskalationsprozesse
- konsistente und nachvollziehbare Dokumentation (auch der Schnittstellen zwischen IRBC-Plänen und GFPs)

Unternehmen mit bereits interagierenden IRBC/BCM-Managementsystemen sind grundsätzlich gut aufgestellt. Jedoch verschärfen sich die Anforderungen an:

- **Nachvollziehbarkeit und Methodik:** Audit-Prüfungen verlangen zunehmend einen dokumentierten Nachweis, wie IRBC-Maßnahmen aus BCM-Ergebnissen abgeleitet wurden.
- **Governance und Rollenstruktur:** Es muss klar ersichtlich sein, wer für welche IRBC-Deliverables verantwortlich ist und wie die Zusammenarbeit mit BCM und ISM organisiert ist.
- **Kohärenz in Audits:** Im Rahmen von Audits wird künftig gezielter geprüft werden, wie IRBC-Maßnahmen methodisch aus BCM-Ergebnissen abgeleitet wurden, wie Rollen abgegrenzt sind und wie die Interaktion zwischen BCM, IRBC und ISM organisiert ist. Die Norm fordert nicht nur das stärkere Zusammenwirken dieser Disziplinen, sondern erhöht auch die Erwartungshaltung an deren dokumentierte Kohärenz.

Strategische Neuausrichtung und Integration mit ISO 22301

Praxisbeispiel: Beispiel GmbH – BIA & IRBC mit lückenloser Dokumentation

Ein Unternehmen muss künftig dokumentieren und darlegen können, wie Ergebnisse aus der BIA methodisch in IRBC-Lösungen übersetzt wurden und wie die Zusammenarbeit zwischen BCM, IRBC und ISM organisatorisch geregelt ist.

Die Beispiel GmbH betreibt eine hochverfügbare Cloud-Plattform für Kommunalverwaltungen. Bei einer BIA wurde festgestellt, dass der Ausfall der Mandanten-Selfservice-Plattform nach maximal zwei Stunden zu erheblichen Verwaltungsverzögerungen und Reputationsschäden führt. Das BCM definiert daher einen RTO von zwei Stunden. Die bisherige Planung sah ein Warm-Standby-Szenario mit sechs Stunden IT-Wiederanlaufzeit vor.

Im Zuge der strategischen Neuausrichtung nach ISO/IEC 27031:2025 wurde IRBC vollständig in das BCMS eingebettet. Die IT-Wiederanlaufziele (ICT-RTO, ICT-RPO) wurden nachvollziehbar aus den BIA-Ergebnissen abgeleitet, technisch validiert und in einer strukturierten Planungsdokumentation erfasst.

Die Plattformarchitektur wurde auf Hot-Standby umgestellt, der ICT-RTO auf 90 Minuten reduziert = Ziel erfüllt, Dokumentation revisionsfähig.

Die Ableitung wurde nachvollziehbar dokumentiert – inklusive:

- Referenz zur jeweiligen BIA-Anforderung (inkl. Prozess-ID)
- die Zuordnung der ICT-Services zu den kritischen Geschäftsprozessen
- der Ableitung von ICT-RTO/RPO auf Basis der BIA
- technischer Lösungsoptionen inkl. Bewertung und Betrachtung der Restrisiken
- Festlegung des Final-MBCO bei Abweichungen
- Prüfdatum, Bewertung und Managementfreigabe

Bei internen Audits dient diese Dokumentation nun als Single Point of Truth zur Ableitungslogik zwischen Business-Anforderung und umgesetzter IRBC-Lösung.

Erweiterte Governance- und Managementanforderungen

Der neue Standard hebt die Bedeutung einer klaren und strukturierten Governance für IRBC hervor. Bisher waren viele Governance-Elemente (z. B. Policy, Handbuch, Jahresberichte usw.), Best Practices oder interpretationsbedingte Ableitungen. Die ISO/IEC 27031:2011 selbst blieb in ihrer Aussage zur Governance eher vage. In der 2025er-Version hingegen wird Governance explizit normativ gefordert, und das mit definierten Mindestanforderungen an Rollen, Steuerung und Managementeinbindung.

Was fordert die Norm konkret?

Während die ISO von 2011 Governance-Elemente lediglich erwähnte, fordert die neue Norm zwingend eine formale Einbindung von IRBC in die Führungs- und Steuerungsstrukturen des Unternehmens. IRBC wird zur Managementaufgabe mit Gremienbindung, Berichtspflichten und Schnittstellen zu BCMS, ISMS und (IT-)Risikomanagement.

In der Norm wird explizit betont, dass die oberste Leitung nicht nur die Verantwortung trägt, sondern auch Entscheidungen über Zuweisung von Ressourcen, Zielgrößen wie das Final-MBCO und Risikoakzeptanz auf Basis von IRBC-Berichten aktiv treffen muss.

Die Rolle des IRBC-Managers wird gestärkt – sowohl strategisch als auch operativ.

Zu den zentralen Anforderungen gehören unter anderem:

- formale Benennung eines IRBC-Managers mit klaren Aufgaben, Stellvertretung und Befugnissen
- regelmäßige Reviews durch die oberste Leitung inkl. KPI Reporting
- dokumentierte Richtlinien & Prozesse sowie Eskalations und Kommunikationswege
- Sicherstellung angemessener finanzieller und personeller Mittel für IRBC-Aktivitäten
- festgeschriebene Audit- und Review-Zyklen zur Wirksamkeit von Governance-Strukturen

Was bedeutet das für die Umsetzung?

IRBC ist nicht mehr als reines Instrument zur IT-Wiederanlaufplanung zu verstehen, sondern als integraler Steuerungsprozess, der aktiv zur Resilienzstrategie des Unternehmens beiträgt. Die Norm verlangt eine systematische Verankerung im Governance-Modell einschließlich klar dokumentierter Zuständigkeiten, abgestimmter Eskalationspfade und strukturierter Schnittstellen zum BCMS, ISMS und dem Krisenmanagement.

Erweiterte Governance- und Managementanforderungen

Ein besonderes Augenmerk liegt auch auf der Nachvollziehbarkeit und Auditfähigkeit der Rollenmodelle, Kommunikationsstrukturen und Entscheidungsprozesse. Sie müssen konsistent dokumentiert und im Rahmen interner wie externer Prüfungen nachvollziehbar darstellbar sein.

Die Norm nennt keine konkrete Form, verlangt aber ein Gremium mit entsprechender Steuerungsbefugnis und Interdisziplinarität. In der Praxis kann dies z. B. ein Resilience Board sein, in dem IRBC, BCM, ISM, Risk Management, IT-Betrieb und Unternehmensleitung regelmäßig IRBC-Themen abstimmen. IRBC-Entscheidungen dürfen nicht isoliert erfolgen, sondern müssen eingebettet in die Gesamtsteuerung der Unternehmensresilienz getroffen werden.

Unternehmen müssen sicherstellen, dass:

- IRBC-Rollen (Owner, Manager usw.) mit Aufgaben, Befugnissen und Vertretung schriftlich festgelegt sind
- ein interdisziplinäres Lenkungsgremium (z. B. Resilience Board) Management-Reviews regelmäßig, z. B. quartalsweise, durchführt
- Performance-Kriterien als KPIs im Management-Reporting integriert sind
- Ressourcenbedarf für IRBC in der Budget- und Investitionsplanung berücksichtigt wird
- die Governance-Strukturen, Kommunikations- und Eskalationswege regelmäßig überprüft und zentral gesteuert gepflegt werden
- IRBC in ein internes Audit- und Review-Programm aufgenommen ist und darüber die Wirksamkeit belegt werden kann

Erweiterte Governance- und Managementanforderungen

Praxisbeispiel: Beispiel GmbH – Etablierung einer IRBC-Governance-Struktur im regulierten Umfeld

Die Beispiel GmbH ist ein Finanzdienstleister und unterliegt den regulatorischen Vorgaben der NIS-2 und DORA. Eine interne Compliance-Prüfung hat ergeben, dass zwar ein grundlegendes ITSCM existierte, jedoch keine formale Governance-Struktur für IRBC. Rollen, Zuständigkeiten und Eskalationswege waren nur in einzelnen IT-Bereichen bekannt und nicht zentral dokumentiert.

Mögliche Maßnahmen zur Umsetzung der Normanforderungen:

1. **Einrichtung eines Resilience Board**
   - Aufgaben: vierteljährliche Reviews, Freigabe von IRBC-Zielen, Ressourcenentscheidungen, Risikoakzeptanzbeschlüsse
   - Zusammensetzung: IRBC-Manager, BC-Manager, CISO, IT-Betrieb, Risikomanagement, Geschäftsführung

2. **Formale Benennung eines IRBC-Managers**
   - schriftlich fixierte Aufgaben, Befugnisse und Vertretungsregelungen
   - Festlegung der Berichtslinie

3. **Integration von KPIs ins Management-Reporting**
   - quartalsweise Berichterstattung an das Resilience Board und jährliche Präsentation im Aufsichtsrat (wenn vorhanden)
   - Festlegung von KPIs: z.B. Zielerreichung ICT-RTO/ICT-RPO/Final-MBCO, Abweichungen bei Tests, Audit-Feststellungen, Fortschritt bei Maßnahmenumsetzung

4. **Auditfähigkeit**
   - Durchführung jährlicher Wirksamkeitsprüfungen
   - regelmäßige Auditierung (intern/extern)

Harmonisierung mit bestehenden Normen/Standards

Die neue Norm positioniert sich augenscheinlich als Ergänzungsnorm zu bestehenden Management-Standards und regulatorischen Rahmenwerken. Sie fordert eine enge Integration und Abstimmung mit angrenzenden Normen, um Inkonsistenzen zu vermeiden, Redundanzen zu minimieren und Synergien im Aufbau und Betrieb von Resilienzstrukturen zu schaffen.

Im Mittelpunkt stehen insbesondere die Schnittstellen zu:

- ISO/IEC 22301 (BCM): Business-Impact-Analyse, Strategieentwicklung, Risikosteuerung, Zielgrößendefinition
- ISO/IEC 27001 (ISMS): z. B. Controls 5.30 (ICT Readiness for Business Continuity) und 8.16 (Monitoring Activities) der ISO/IEC 27002:2022 bzw. A 5.30 und A 8.16 in ISO/IEC 27001:2022
- ISO/IEC 27005:2022 (Risikomanagement): IRBC-Strategieableitung sowie Szenarioanalysen (z. B. Annex B – CFIA/FMEA) basieren auf einer konsolidierten Risikolage gemäß ISO/IEC 27005
- ISO/IEC 27035 (Incident Management): Verzahnung von Vorfall- und Wiederherstellungsprozessen
- NIST SP 800-61 r3: Incident Handling Lifecycle, Lessons Learned
- NIST CSF 2.0: Funktionen Detect, Respond, Recover
- NIS-2, DORA, BSI-Standard 200-4: regulatorisch verpflichtende Resilienz- und Nachweisanforderungen

Was fordert die Norm konkret?

Im ISMS nach ISO 27002 schützt Control 5.30 die Verfügbarkeit kritischer ICT-Services. Die neue ISO 27031 liefert dafür den Umsetzungsleitfaden. Die Norm verweist auf Informationssicherheitsvorfälle und fordert ein abgestimmtes Vorgehen zwischen Incident Response, IRBC und BCM:

- eine harmonisierte Risiko- und Planungsbasis zwischen ISMS, BCMS und IRBC mit klarer Formulierung als Mussanforderung, wodurch die Umsetzung prüfpflichtig im Audit ist
- gemeinsame Zielgrößen ICT-RTO, ICT-RPO sowie Final-MBCO, durchgängig dokumentiert und gesteuert über eine einheitliche Dokumentenlenkung
- eine verbindliche Strategie für Tests, Übungen und Audits mit festgelegten Performance-Kriterien
- einheitliche revisionssichere Audit-Nachweise für interne und externe Prüfungen

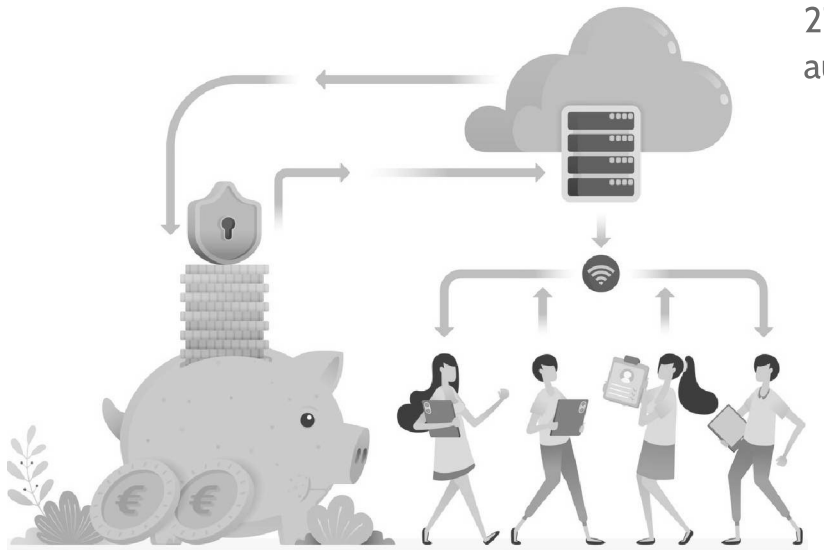
Harmonisierung mit bestehenden Normen/Standards

Was bedeutet das für die Umsetzung?

- **ISMS/BCMS-Harmonisierung:** Mapping von Controls und Prozessen
- **Synergie-Reporting:** Nutzung gemeinsamer Kennzahlen und Auditergebnisse
- **GRC-Modell:** Übergreifendes Governance-, Risk- & Compliance-Modell, das Resilienz als Querschnittsthema integriert

Praxisbeispiel: Beispiel GmbH – regulatorisch harmonisierte Steuerung

Als Betreiber von Cloud-Diensten für Finanz- und Verwaltungskunden ist die Beispiel GmbH sowohl durch DORA als auch durch NIS-2 reguliert. Bisher agierten ISMS, ITSCM und BCM ohne übergreifende (IT-)Risikosteuerung.



Im Rahmen der Einführung von ISO/IEC 27031:2025 wird ein integriertes Framework aufgebaut. Bestandteile sind:

- die Konsolidierung der (IT-)Risiko-bewertungen auf Basis ISO/IEC 27005
- ein Norm-Mapping zu DORA und NIS-2 (z. B. Control-Zuordnung zu ISO/IEC 27002 A 5.30)
- die Harmonisierung von ICT-RTO/RPO-Wiederanlaufziele zwischen BIA, BCM und IRBC
- die Definition einer einheitlichen Auditstruktur

Alle Maßnahmen werden in einem Gesamtdokument zusammengeführt und mit Gültig-keitsbereich, Ansprechpartnern, Kontrollterminen und Lessons-Learned-Zyklen ergänzt. Damit können interne und externe Prüfanforderungen nun vollständig belegt werden – mit konsistenter, revisionssicherer Dokumentation, Schnittstelle zu ITIL 4 und Abgren-zung zu IRBC.

Schnittstelle zu ITIL 4 und Abgrenzung zu IRBC

ITIL 4 führt die Praktik IT Service Continuity Management (ITSCM) fort, deren Ursprünge aus den 90er-Jahren stammen. In der Vergangenheit wurden die Begriffe ITSCM und IRBC häufig synonym verwendet, da sich beide auf den IT-Wiederanlauf konzentrierten.

Harmonisierung mit bestehenden Normen/Standards

Mit der neuen Norm verschiebt sich der Schwerpunkt deutlich von einem rein service-orientierten Wiederanlauf (ITIL) hin zu einer organisationsweiten Resilienzbetrachtung (IRBC). Damit ist es künftig wichtig, klar zu benennen, ob man von den operativen ITIL-Praktiken oder vom strategischen IRBC Framework spricht. Durch die Veränderungen der neuen Norm laufen die Disziplinen teilweise auseinander, erfordern aber weiterhin ein abgestimmtes Zusammenspiel.

Auswirkung bei regulatorischer Vorgabe

Für regulierte Unternehmen (z. B. Finanz- oder KRITIS-Sektoren), die Anforderungen entsprechend ISO/IEC 27031 erfüllen müssen, reicht eine reine ITSCM-Implementierung nach ITIL nicht mehr aus. ITIL deckt weiterhin die operativen IT-Continuity-Prozesse für zeitkritische IT-Services ab, erfüllt jedoch nicht die neuen strategischen Governance-, Risiko- und Resilienzanforderungen der überarbeiteten Norm.

Die Erweiterung eines vorhandenen ITSCM auf die Vorgaben der ISO/IEC 27031:2025 ist möglich. ITSCM bleibt für den IT-Wiederanlauf und erhält einen strategischen Überbau. Dieser Überbau verlangt eine formalisierte Governance, regelmäßige Management-Reviews und ein risikoorientiertes Test- und Auditprogramm. Damit verschieben sich Aufgaben teilweise vom technischen IT-Wiederanlauf hin zur Gremienarbeit, Kennzahlensteuerung und Risikobewertung.

Ein großer Nachteil ergibt sich aus der unterschiedlichen Prozesslogik beider Welten. ITIL folgt einem servicezentrierten Lebenszyklus, während ISO 27031 strategische, risikobasierte Steuerung betont. Werden ISO-Vorgaben nur oberflächlich an ITIL-Prozesse „angeflanscht“, entsteht ein Hybrid, der weder den ITIL-Effizienzvorgaben noch den ISO-Nachweispflichten voll entspricht. Zudem besteht die Gefahr einer dauerhaften Doppelpflege. Testergebnisse, Lessons Learned und KPI-Berichte fließen gleichzeitig in das ITIL-Continual-Improvement und in das IRBC-Reporting. Es drohen Medienbrüche und inkonsistente Informationen.

In der Konsequenz sollte ITSCM als Teilprozess unter dem IRBC betrieben werden. Das bedeutet, dass regulierte Unternehmen das bestehende ITSCM in die Governance und Teststruktur des IRBC aufnehmen müssen, so dass Audit- und Nachweisforderungen der Norm vollständig erfüllt werden. ITSCM bleibt grundsätzlich für den operativen IT-Wiederanlauf der zeitkritischen IT-Services durchaus relevant, während IRBC den strategischen Rahmen für organisationsweite IT-Resilienz bildet. Beide Managementdisziplinen sollten durch eine verbindliche übergreifende Governance synchronisiert werden.

Harmonisierung mit bestehenden Normen/Standards

Auch ohne ITSCM können sich Unternehmen ISO-27031-konform aufstellen, wenn IRBC selbst die Aufgaben aus ITIL übernimmt. Ein implementiertes ITSM oder ITIL erleichtert die operative Umsetzung, ist aber keine zwingende Voraussetzung. Die neue Norm erwartet jedoch, dass IRBC sämtliche fehlenden Prozesse dann funktional ersetzt.

	IRBC (ISO 27031:2025)	ITSCM-Praktik nach ITIL 4
Zweck	Sicherstellung der Resilienz zeitkritischer ICT-Services (inkl. Governance & Strategie)	Wiederanlauf von IT-Services gemäß vereinbarter Zeitziele
Scope	Organisation (BCMS) & IT-Infrastruktur, Governance, Risiko, IT-Dienstleister und Lieferanten, Daten	zeitkritische IT-Services
Planung	Strategien (Skills, Facilities, Technologie, ...)	Service-SLAs, IT-Infrastruktur, RZ
Fokus	Cyber, Lieferkette, Compliance, Daten- und (IT-)Dienstleisterresilienz	IT-Infrastruktur, IT-Service-SLAs
Governance	Rollenmatrix inkl. IRBC-Manager/Owner und Management-Review Best Practice: Resilience Board	Practice Owner, Practice Manager und Service Owner

Aus der neuen ISO/IEC 27031:2025 geht sehr klar hervor, dass IRBC und ITSCM nicht synonym sind. Während ITSCM als operative ITIL-Praktik für den Wiederanlauf von ICT-Services zuständig ist, definiert IRBC ein strategisches Rahmenwerk zur unternehmensweiten Steuerung der ICT-Resilienz. Regulatorische Anforderungen – insbesondere aus DORA und NIS-2 – können nur erfüllt werden, wenn IRBC implementiert ist. ITSCM kann dabei eingebettet, aber nicht alleinstehend genutzt werden.

Erweiterte Rolle des IRBC-Managers

Mit der überarbeiteten ISO/IEC 27031:2025 verändert sich die Rolle des IRBC-Managers grundlegend. Während dieser bislang hauptsächlich für die Planung und Umsetzung von IT-Wiederanlaufmaßnahmen entsprechend der Kontinuitätsanforderungen des BCM zuständig war, erweitert sich sein Aufgabengebiet nun erheblich. Er ist nicht mehr primär Planer für IT-Wiederanlaufmaßnahmen, sondern entwickelt aktiv resiliente IT-Strukturen, analysiert IT-Risiken, plant alternative IT-Betriebsmodelle und koordiniert mit BCM, ISM, Incident Response und Krisenmanagement entsprechende Maßnahmen und Prozesse.

Gefordert wird die Fähigkeit, vorausschauend resiliente IT-Strukturen zu gestalten, alternative IT-Betriebsmodelle bereitzustellen und auch im Falle komplexer Cyberangriffe die Funktionsfähigkeit zeitkritischer ICT-Services sicherzustellen. Er muss zukünftig nicht nur für den IT-Wiederanlauf bei einem kritischen IT-Vorfall planen, sondern auch die fortgesetzte IT-Betriebsfähigkeit in enger Abstimmung mit dem BCM, dem Incident Management, dem Cyber Response Planning und dem Krisenmanagement, z. B. bei einem Cyberangriff, sicherstellen.

Dabei agiert er als fachlicher Integrator zwischen technischen, organisatorischen und strategischen Anforderungen und muss über bereichsübergreifende Kompetenzen verfügen. Dazu zählen neben technologischer Expertise auch Kenntnisse in (IT-)Risikomanagement, Geschäftsprozessanalyse, Informationssicherheit, Testmanagement und Kommunikation.

Ein wesentlicher neuer Verantwortungsbereich ist die Definition und Pflege des Final-MBCO gemeinsam mit dem BCM, einschließlich technischer Machbarkeitsprüfung und Ableitung geeigneter (IT-)Recovery-Strategien. Ebenso gehört die Steuerung externer (IT-)Dienstleister zu seinen Aufgaben, einschließlich der vertraglichen Festlegung von Resilienzmaßnahmen, um Risiken aus Lieferketten zu minimieren.

Er trägt Verantwortung für die Auditierbarkeit, Steuerbarkeit und Rückverfolgbarkeit sämtlicher IRBC-Maßnahmen. Diese Aspekte werden als prüfpflichtige Anforderungen festgeschrieben und werden im Audit kontrolliert.

Erweiterte Rolle des IRBC-Managers

Was fordert die Norm konkret?

- strategische Verantwortung hinsichtlich Mitgestaltung von Resilienzzielen, Budgetplanung und Reporting ans Top-Management
- Architekturkompetenz zur Bewertung und dem Design resilienter IT-Landschaften (Redundanz, Zero Trust, Cloud Failover)
- Koordination mit dem BCM & Incident Management/Cyber Incident Response zur Sicherstellung, dass der IT-Wiederanlauf erst nach forensischer Freigabe erfolgt inkl. Abstimmung von Eskalationen
- Lifecycle Ownership hinsichtlich Aufbau, Pflege, Test und Audit aller IT-Continuity-Pläne
- Verantwortung für benötigte Kompetenzen (Skills), Schulungen und Ressourcen für Resilienzmaßnahmen
- Planung und Steuerung von Tests, KPI Tracking und des Lessons-Learned-Prozesses zur Messung und Verbesserung
- Steuerung externer (IT-)Dienstleister und Festlegung vertraglicher Resilienz-anforderungen

Was bedeutet das?

Der IRBC-Manager ist in der Umsetzungsverantwortung des gesamten IRBC-Lifecycle – von der Analyse über die Lösungsoptionen bis zur Steuerung von Übungen und Audits. Darüber hinaus wird er zukünftig zum zentralen Planer einer widerstandsfähigen IT-Landschaft, die Cyberresilienz integriert und auf eine robuste Aufrechterhaltung zeitkritischer IT-Services ausgelegt ist. Dies schließt die Fähigkeit ein, alternative IT-Betriebsumgebungen für den kritischen IT-Vorfall vorzuhalten und zu aktivieren.

Besonders im Kontext von Cyberbedrohungen (z. B. Ransomware, APT) übernimmt er zukünftig operative und strategische Verantwortung. Das umfasst:

- Entwicklung resilienter (IT-)Architekturen: Multi-Zone-Design, automatisiertes Failover, Immutable-Backup-Framework, Cloud-Exit-Strategien
- regelmäßige Resilience Architecture Reviews (RAR) für neue oder geänderte Systeme
- technische Bewertung der Einhaltung von ICT-RTO, ICT-RPO und Final-MBCO – insbesondere bei Cybervorfällen
- Integration und Koordination von Response- und IT-Wiederanlaufprozessen für zeitkritische IT-Services

Erweiterte Rolle des IRBC-Managers

Praxisbeispiel: Beispiel GmbH – regulatorisch harmonisierte Steuerung

Ursprünglich koordinierte der ITSC-Manager der Beispiel GmbH die Wiederanlaufplanung nach ITIL. Mit Einführung der ISO/IEC 27031:2025 wurde ein dedizierter IRBC-Manager mit umfassender Zuständigkeit für Analyse, Planung, IT-Architektur, Test und Dokumentation etabliert.

Der IRBC-Manager führt ein jährliches Resilience Architecture Review (RAR) ein, plant eine virtuelle Cloud-Failover-Zone und ließ Immutable Backups einführen. Für jedes kritische IT-System wurden

- die BIA-Vorgaben (z. B. RTO 2 Stunden),
- die technischen Optionen
- und organisatorischen Prozesse

methodisch aufeinander abgestimmt.

Die Ableitung der IRBC-Wiederanlaufziele aus der BIA ist jetzt dokumentiert in:

- dem IRBC-Lösungskonzept (mit RTO/RPO-Mapping)
- dem Maßnahmenregister mit Bewertung und Genehmigung
- dem Lessons-Learned-Protokoll aus Tests
- und dem Eskalationsprotokoll für Cyber Incidents

Die Rolle des IRBC-Managers ist im Resilience Board fest verankert, mit direkter Verantwortung für die Zielerreichung, Wirksamkeit und Nachvollziehbarkeit der resilienten IT-Architektur.

Fokussierung auf digitale Resilienz und Cyberresilienz

Mit der ISO/IEC 27031:2025 verschiebt sich der Schwerpunkt des IRBC durchaus deutlich. Während bisher vor allem der IT-Wiederanlauf zeitkritischer IT-Services nach einem kritischen IT-Vorfall im Fokus stand, rückt nun die Fähigkeit von IT-Systemen und -Strukturen, auch unter dynamischen, unsicheren und potenziell destruktiven Bedingungen wie Cyberangriffen funktionsfähig zu bleiben, adaptiv zu reagieren und gezielt zu lernen, in den Fokus. Sie stellt den Begriff der Resilienz in den Mittelpunkt des IRBC-Ansatzes. Resilienz wird dabei nicht nur als technisches Ziel verstanden, sondern als organisationsweites, strategisch verankertes Steuerungsprinzip.

Diese neue Ausrichtung schlägt sich insbesondere in den Anforderungen an proaktive Planung, kontinuierliche Verbesserung, lernfähige Organisationen und den Aufbau robuster, aber auch adaptiver Systeme nieder. Resilienz betrifft sowohl die IT-Systeme als auch Prozesse, Mitarbeitende, Lieferketten und organisatorische Steuerungsmechanismen. Damit wird IRBC zu einem wesentlichen Bestandteil des umfassenden Resilienz-Managements, in dem technische, organisatorische und auch kulturelle Aspekte gleichermaßen berücksichtigt werden sollen.

Ergänzend fordert die Norm explizit technische Maßnahmen wie Netzwerksegmentierung, redundante Datenhaltung, Zero-Trust-Architekturen, Datenintegritätsprüfungen und Wiederherstellungsmechanismen, die auch unter aktiven Angriffsbedingungen verlässlich funktionieren. Diese Vorgaben werden mit zeitlichen Steuerungsparametern verknüpft und auf ein definiertes Mindestleistungsniveau (Final-MBCO) gemappt.

Was bedeutet das konkret?
IRBC wird als Teil einer unternehmensweiten Resilienzstrategie etabliert. Der Fokus verschiebt sich von reiner IT-Continuity-Planung hin zur strategischen Sicherung der Geschäftsfähigkeit durch kontrollierte Reaktion, Adaption, Robustheit, Redundanz und Lernfähigkeit. Im Mittelpunkt steht nicht mehr der IT-Wiederanlauf, sondern die Aufrechterhaltung der Handlungsfähigkeit und der resiliente Umgang mit Unsicherheit nach folgenden Prinzipien:

- **Adaption:** Fähigkeit, sich veränderten Bedrohungslagen anzupassen
- **Robustheit:** Widerstandskraft gegen kritische IT-Vorfälle oder Angriffe
- **Redundanzfähigkeit:** Verfügbarkeit alternativer Ressourcen und IT-Systeme
- **Lernfähigkeit:** Etablierung von Feedbackschleifen aus Vorfällen und Übungen

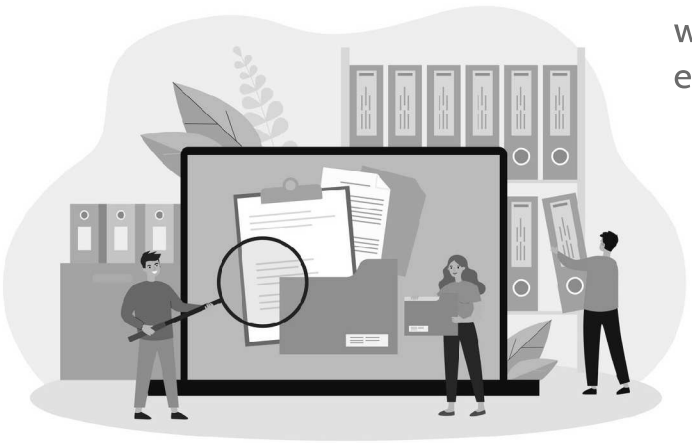
Fokussierung auf digitale Resilienz und Cyberresilienz

Digitale Resilienz wird als strategisches Ziel verstanden, das durch technische, organisatorische und strategische Maßnahmen, die über den klassischen IT-Wiederanlauf weit hinausgehen, sichergestellt werden muss.

Umsetzung:

- Ableitung von (IT-)Resilienz-Anforderungen aus strategischen Unternehmenszielen und (IT-)Risikoanalysen
- Integration resilienzfördernder Prinzipien in IT-Architektur, Prozessen und Unternehmenskultur
- Einrichtung von Feedback- und Lernschleifen aus Übungen, IT-Tests und kritischen IT-Vorfällen
- Entwicklung messbarer (IT-)Resilienz-KPIs und deren regelmäßige Bewertung im Rahmen von Management-Reviews

Praxisbeispiel
Die Beispiel GmbH betreibt eine Plattform für kommunale Verwaltungsprozesse. Ein Red-Team-Test simulierte einen Ransomware-Angriff auf das DMS. Zwar waren IT-Wiederanlaufpläne vorhanden, jedoch zeigte sich, dass keine forensisch abgesicherte Entscheidung zum Datenrestore vorgesehen war.



Im Zuge der Umsetzung von ISO/IEC 27031:2025 wurde daraufhin eine Cyberresilienzstrategie entwickelt:

- Die Datensicherung wurde auf Immutable Backups mit Geo-Redundanz erweitert.
- Ein segmentiertes Notfallnetzwerk wurde als gesonderte Wiederanlaufzone technisch implementiert.
- Die IT-Wiederanlauf- und Datenrestore-Prozesse wurden mit dem Cyber Incident Response Management, inkl. forensischer Freigabeschritte, abgestimmt.

Die Plattform kann jetzt auch bei aktiven Angriffen kontrolliert wiederhergestellt werden, mit dokumentierter Einhaltung der ICT-RTO und ICT-RPO und nachvollziehbarer Managemententscheidung.

Technologischer und datenbezogener Fokus

Der neue Standard legt einen starken Schwerpunkt auf den technologischen Unterbau sowie auf datenbezogene Anforderungen im Rahmen des IRBC. Resilienz wird nicht mehr nur auf Prozessebene betrachtet, sondern ausdrücklich auch auf der Ebene der benötigten IT-Ressourcen – also der IT-Infrastrukturen, Systeme und Anwendungen.

Die Norm fordert, technologische Abhängigkeiten systematisch zu identifizieren, alternative Versorgungs- und Bereitstellungswege zu definieren und die Datenintegrität auch bei kritischen IT-Vorfällen – etwa infolge von Cyberangriffen – sicherzustellen.

Im Zentrum steht dabei die Fähigkeit, zeitkritische IT-Services innerhalb akzeptabler Wiederanlaufzeiten verfügbar zu machen. Dazu zählen die Sicherung und Wiederherstellung von Systemkonfigurationen, Datenbanken, Kommunikationsinfrastrukturen sowie der Zugang zu cloudbasierten Anwendungen. Auch Aspekte wie geografische Redundanz, Segmentierung von Datenverbindungen, Absicherung von SaaS-Plattformen und die Resilienz von Schnittstellen werden ausdrücklich adressiert.

Was fordert die Norm konkret?

Die Resilienzfähigkeit von IT-Umgebungen und die Integrität geschäftskritischer Daten rücken in den Fokus der IRBC-Planung. Die Norm verlangt ein detailliertes Verständnis technischer Abhängigkeiten und dazu passender und geeigneter IT-Wiederanlaufplanung, insbesondere für physische sowie virtuelle IT-Infrastrukturen, Anwendungen, Daten und die Cloud-Nutzung.

Technisch bedeutet das, dass IT-Architekturen von Beginn an resilient geplant und betrieben werden müssen, durch den Einsatz von Redundanzen, von verteilten Systemen, automatisierten Failover-Mechanismen, Mikrosegmentierung oder cloudbasierten Hochverfügbarkeitsstrategien. Organisatorisch verlangt die Norm den Aufbau klarer Verantwortlichkeiten, kontinuierlicher Überwachungs- und Eskalationsprozesse sowie die Einbindung von Personal mit spezifischem Know-how zur Aufrechterhaltung zeitkritischer ICT-Services unter erschwerten Bedingungen.

Technologischer und datenbezogener Fokus

Die ISO/IEC 27031:2025 hebt in mehreren Abschnitten folgende Anforderungen besonders hervor:

- Dokumentation aller zeitkritischen ICT-Services inkl. zugeordneter Wiederanlaufzeitwerte (ICT-RTO, ICT-RPO, Final-MBCO) und ihrer Rolle im Geschäftsprozess
- IT-Komponenten (z. B. IT-Infrastruktur, IT-Systeme, Anwendungen und Schnittstellen) müssen sowohl für den Normalbetrieb als auch für alternative IT-Betriebsumgebungen, inkl. ihrer Konfiguration, dokumentiert sein.
- Die Norm fordert den Einsatz geeigneter IT-Technologien zur Absicherung der Resilienz, z. B. Redundanzdesign, automatisierte Failover, Cloud-Cluster sowie RPO-konforme Backupverfahren mit festgelegten Speicherorten und Zugriffspfaden.
- Für jeden zeitkritischen ICT-Service muss nachvollziehbar dargestellt werden, welchen geschäftskritischen Prozess er unterstützt und wie die zugehörige Technologie- und IT-Architekturstruktur ausgestaltet ist.
- Abweichungen zwischen technischer IT-Leistungsfähigkeit (z. B. realisierbare ICT-RTO) und den durch das BCM definierten Zielwerten müssen identifiziert, risikobewertet und im Managementreport adressiert und freigegeben werden.

Umsetzung (empfohlene Maßnahmen)

Resilience by Design:

- Planung resilienter IT-Systemarchitekturen mit Redundanz, Segmentierung, automatisierten Failover-Mechanismen, cloudbasierten Hochverfügbarkeitsstrategien

Resilient Data Management:

- Absicherung, Isolierung und Verfügbarkeit von Daten trotz Kompromittierung

Detektion und Kontrolle:

- Integration von forensischen, detektiven und präventiven Komponenten zur Früherkennung und Isolierung

Technologischer und datenbezogener Fokus

Darüber hinaus adressiert die ISO/IEC 27031:2025 IRBC auch im Kontext digitaler und cyberbezogener Bedrohungslagen. Damit unterstützt die Norm die Entwicklung hin zu einem umfassenden Resilienzverständnis, wie es auch in

- **DORA**
  - Art. 10: ICT Risk Management Framework
  - Art. 11: ICT Business Continuity Policy und Response & Recovery Plans
- **NIST Cybersecurity Framework**
  - Function „Recover“ (RC.IM-1 bis RC.IM-3)
  - Functions „Respond“ (RS) und „Identify“ (ID)

verankert ist. IRBC wird dadurch zu einem integralen Bestandteil der IT-Risikosteuerung sowie der strukturellen und operativen IT-Widerstandsfähigkeit gegenüber komplexen, auch cyberinduzierten, Bedrohungsszenarien.

Die Tabelle zeigt die zentralen Themenfelder in der Übersicht:

Themenfeld	Kerninhalte
Resiliente IT-Architektur	Multi-Zonen- und Multi-Regionen-Design, automatische Failover-Mechanismen, "Defence-in-Depth"
Resilient Data Management	Air-Gap-/Immutable-Backups, Crypto-Shredding-Schutz, regelmäßige Restore-Übungen
Detection & Control	Forensische Tools, Anomalieerkennung, Frühwarnmechanismen
Zero-Trust & Mikrosegmentierung	Durchsetzung von Least-Privilege, kontinuierliche Authentifizierung, Isolation kompromittierter Segmente
Cloud- & SaaS-Abhängigkeiten	Exit-Strategien, Multicloud-Clustering, vertraglich bindende RTO/RPO-Garantien
Observability & Telemetrie	Einheitliche Log-Pipeline, KI-gestützte Anomalie-Erkennung, Frühwarnindikatoren für Datenkorruption
Compliance, Verschlüsselung & Schlüsselmanagement	DSGVO/DORA-konforme-Policies, Lifecycle-Kontrolle von Schlüsseln, HSM-Nutzung

Technologischer und datenbezogener Fokus

Für Unternehmen bedeutet es, dass sie nicht nur über eine IT-Notfallplanung zum IT-Wiederanlauf verfügen müssen, sondern dass sie den kontinuierlichen Betrieb ihrer zeitkritischen ICT-Services und IT-Infrastrukturen auch unter Belastung sicherstellen und diese Fähigkeit durch geeignete Maßnahmen und Dokumentationen dauerhaft nachweisen müssen. Resilienz wird damit zum strategischen Ziel und IRBC zu einem zentralen Baustein der digitalen Unternehmensresilienz.

Was bedeutet das für die Umsetzung?

- Erhebung kritischer IT-Technologie- und Datenabhängigkeiten im Rahmen der (IT-)Risikoanalyse
- Definition redundanter Datenpfade und IT-Wiederanlaufkonzepte für hybride IT-Umgebungen
- Planung von Szenarien für Daten- und Anwendungswiederherstellung inkl. IT-Teststrategie
- Absicherung der Integrität und Verfügbarkeit von Daten auch bei Angriffsszenarien

Eine bloße IT-Wiederanlaufplanung und/oder Backup Skript genügt nicht mehr. Unternehmen müssen ihre IT-Technologien konsequent an den Resilienzzielen ausrichten.

Typische Schritte sind dabei:

- Resilience Architecture Review (RAR) für jedes größere IT-/OT-Projekt, u. a. Geo-Redundanz-Check, Segmentierungslayout und Dependency-Mapping
- Immutable-Backup-Framework und getrennte Credentials, Write-Once-Policy, regelmäßige automatisierte Restore-Tests in isolierter Sandbox
- Continuous Hardening & Patch Pipeline, Infrastructure-as-Code
- Cloud Exit Drills zu alternativem Provider/On Prem Cluster inkl. dokumentierter RTO-Messung
- Telemetriebasierte Frühwarnung – Data Lag, Snapshot Health Score, Mean Failover Success Rate; Bericht direkt ans Resilience Board

Technologischer und datenbezogener Fokus

Praxisbeispiel: Beispiel GmbH – Resilienztechnologie als IT-Architekturprinzip

Die Beispiel GmbH betreibt ein hybrides Rechenzentrum mit SaaS- und Plattformdiensten. Ein Audit ergab, dass Wiederanlaufziele für das Datenarchiv nicht mit der BIA abgestimmt waren. Geforderter RPO laut BCM zwei Stunden, technisch realisierbar: acht Stunden

In Folge wurde ein Resilience Architecture Review (RAR) etabliert:

- Segmentierung der Datenbankverbindung zur Isolierung bei Angriff
- Einführung von Immutable Backup, getrenntem Credential Storage, automatisiertem Restore-Test
- Cloud Exit Drill inkl. RTO-Messung und Dokumentation
- Gap-Analyse in einer IRBC-Technologie-Matrix; Bericht ans Resilience Board

Die Maßnahmen wurden als technologisches Resilienz-Framework im IRBC-Dokumentationssystem, inkl. Gap-Status zu BIA-RTO /BIA-RPO sowie Lessons Learned aus Übungsszenarien, erfasst.

Business-Anforderungen und BIA-basierte Steuerung

In der Praxis nicht neu aber eine zentrale Forderung der ISO/IEC 27031:2025 ist die konsequente Ableitung aller IRBC-Maßnahmen aus den Business-Anforderungen. Statt nur IT-technische Wiederanlaufzeiten festzulegen, verlangt die Norm, dass Business-Impact-Analyse (BIA), Risiko-Assessment und ICT-Wiederanlaufziele eng verzahnt sind.

Neu ist die klare Trennung zwischen fachlichen Continuity-Zielen (BIA-RTO/RPO) und technischen IT-Zielen (ICT-RTO/RPO). Dabei gilt: ICT RTO/RPO ≤ BIA RTO/RPO. Abweichungen sind durch Investitionen zu schließen oder als Risiko im Final-MBCO-Prozess zu dokumentieren.

Die neue Norm fordert eine lückenlose Nachvollziehbarkeit (Proof Chain) vom Geschäftsprozess bis zum IT-Testnachweis. Jede Zuordnung muss dokumentiert und jährlich oder bei signifikanten Änderungen überprüft werden.

Dadurch entsteht eine geschlossene Kette von:

Geschäftsprozess → Kritikalität/BIA-Bewertung → BIA RTO/RPO → MBCO → ICT RTO/RPO → Final-MBCO → Strategie & Plan

Was fordert die Norm konkret?

ICT-Services sind nach Prozessabhängigkeit, Kritikalität und Wiederanlaufpriorität zu analysieren. Daraus werden Zielgrößen (RTO, RPO, MBCO), Wiederanlaufstrategien und Ressourcen abgeleitet, unter Berücksichtigung externer Anforderungen.

Organisationen müssen sicherstellen, dass jedes IT-Asset nachweislich so aufgestellt ist, dass der vom Fachbereich definierte BIA RTO/RPO eingehalten wird. Die wichtigsten Passagen des Normtextes lassen sich wie folgt clustern:

Kapitel	Kernanforderung
Business Expectations for IRBC	• Ermittlung kritischer Geschäftsprozesse und deren ICT-Abhängigkeiten • Festlegung Initial MBCO & Prioritäten • Dokumentation externer/regulatorischer Anforderungen
Defining Prerequisites for IRBC	• Ableitung von ICT-RTO/RPO aus BIA-Ergebnissen • Festlegung der Final-MBCO nach Risiko- und Machbarkeitscheck • Validierung der Ziele durch das Management
IT-Continuity-Plan	• Pläne müssen RTO/RPO, Workarounds und Übergang vom IT-Not- zum IT-Normalbetrieb (Final-MBCO à Full Recovery) widerspiegeln

Business-Anforderungen und BIA-basierte Steuerung

Zusätzlich fordert die Norm:

- Jede Zuordnung Prozess → IT Asset → RTO/RPO muss in einer nachvollziehbaren Traceability-Matrix hinterlegt sein.
- Mindestens jährlich – oder bei signifikanten Änderungen – sind BIA RTO/RPO, MBCO und ICT RTO/RPO gemeinsam zu verifizieren.
- Wenn Gaps bestehen, sind entweder technische Maßnahmen, Alternativstrategien oder eine formelle Risikoakzeptanz (Final-MBCO) zu dokumentieren und vom Top-Management zu genehmigen.
- Jeder ICT RTO muss durch planmäßige Übungen oder Failover-Tests belegt werden; Ergebnisse fließen in Lessons Learned.

Was bedeutet das für die Umsetzung?

Die konsequente Trennung von BIA RTO/RPO und ICT RTO/RPO verschiebt den Fokus von einer rein technischen IT-Wiederanlaufplanung hin zu einem geschäftsgetriebenen Resilienzmanagement. Vor allem verlangt die Norm ein durchgängiges Proof-Chain-Prinzip. Das bedeutet, jede fachliche Forderung muss sich bis zur letzten IT-Systemkonfiguration und bis zum letzten Testnachweis zurückverfolgen lassen.

Unternehmen müssen deshalb ihre Continuity Governance so ausrichten, dass

- die Fachbereiche verbindlich die Prozesstoleranzzeiten vorgeben,
- das IRBC-Team diese Werte unmittelbar in umsetzbare IT-Ziele übersetzt,
- alle Zwischenschritte (MBCO → CT RTO/RPO → Final-MBCO) transparent, versioniert und auditierbar dokumentiert sind.

Das erfordert nicht nur eine enge Abstimmung zwischen BCM, IRBC und (IT-)Risikomanagement, sondern auch eine Investitionsplanung, um technische Gaps zu schließen oder Risiken formell zu akzeptieren. Erst wenn diese Traceability-Kette lückenlos dokumentiert ist, gilt die Normforderung als erfüllt.

Es sind strukturierte Methoden zur Kritikalitätsbewertung, Abhängigkeitsanalyse und Zielableitung zu etablieren. IRBC wird dadurch integraler Bestandteil der betrieblichen (IT-)Risiko- und Resilienzbewertung.

Business-Anforderungen und BIA-basierte Steuerung

Praxisbeispiel: Beispiel GmbH

Die Beispiel GmbH betreibt Cloud-Dienste für kommunale Steuerportale. Über die BIA wurde festgestellt, dass die Fachbereiche für das Steuerprüfportal eine maximale Unterbrechung von vier Stunden (BIA-RTO) akzeptieren. Die Gap-Analyse ergab jedoch, dass bei einem Komplettausfall der Restore in der Cloud-Infrastruktur rund sechs Stunden dauert (ICT-RTO).

In Folge wurden folgenden Maßnahmen beschlossen:

- technische Aufrüstung des Storage-Layers mit Snapshot-Replikation
- Anpassung der IRBC-Losungsoption (z. B. Failover)
- formelle Risikoakzeptanz durch das Top-Management bis zur Umsetzung

Alle Schritte wurden in einer Traceability-Matrix dokumentiert:

- Geschäftsprozess → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → Final-MBCO → Strategie & Recovery-Plan
- Zusätzlich wurde der neue Wert im IT-Funktionstest überprüft und in den IRBC-Testbericht integriert.

Damit ist die BIA-Verknüpfung technisch, organisatorisch und dokumentarisch belegt.

Risikobasierte Planung und Final-MBCO

Der MBCO (Minimum Business Continuity Objective) ist keine neue Erfindung im aktuellen Standard. Neu ist jedoch die erweiterte Betrachtungsweise in der ISO/IEC 27031:2025, in der der sogenannte Final-MBCO eingeführt wird. Der MBCO beschreibt das minimal erforderliche Leistungsniveau eines zeitkritischen Geschäftsprozesses bzw. des unterstützenden ICT-Services, das in einem kritischen (IT-)Vorfall noch aufrechterhalten werden muss bzw. innerhalb RTO erreicht werden muss, um schwerwiegende Folgen zu vermeiden. Der MBCO ergibt sich aus der BIA.

Der Final-MBCO ist das validierte Ergebnis einer Planung, in der nicht nur das reine BIA-Ergebnis, sondern zusätzlich zu den BIA-Ergebnissen risikobasiert hergeleitet wird, unter Berücksichtigung von:

- technischer und organisatorischer Machbarkeit
- technischen und organisatorischen Abhängigkeiten (z. B. Lieferketten, (IT-)Dienstleister)
- Bedrohungsszenarien und Schwachstellen
- Erkenntnissen aus Tests, Übungen und Audits

Der Final-MBCO dient dabei als Planungs- und Steuerungsgröße für alle (IT-) und organisatorischen Maßnahmen, die über den unmittelbaren IT-Notbetrieb hinausgehen und einen stabilen Geschäftsbetrieb sicherstellen sollen. Zudem wird eine risikobasierte Herleitung und Validierung der Kontinuitätsziele gefordert.

Das bedeutet, dass RTO-, RPO- und MBCO-Werte nicht statisch festgelegt werden sollen, sondern im Kontext möglicher Bedrohungsszenarien, Eintrittswahrscheinlichkeiten und Schadensauswirkungen regelmäßig überprüft und angepasst werden müssen.

Der Final-MBCO soll formal dokumentiert, risikobasiert validiert und vom Management genehmigt werden. Er ist damit verbindlich für die Planung kritischer IT-Vorfälle und die IT-Wiederanlaufstrategie. Der Final-MBCO ist somit nicht nur ein Analyseergebnis, sondern ein vorgegebenes und dokumentiertes Ziel.

Risikobasierte Planung und Final-MBCO

Was fordert die Norm konkret?

Die Norm verlangt eine explizite Unterscheidung zwischen dem temporären IT-Notbetrieb (MBCO) und dem finalen (IT-)Betriebsziel (Final-MBCO). Diese Zielgröße ist entscheidend für die (IT-)Wiederanlaufplanung, Priorisierung von Ressourcen und Gestaltung der (IT-)Recovery-Strategien. Final-MBCO dient dabei als Planungs- und Steuerungsgröße für alle Maßnahmen, die über die unmittelbare Notversorgung hinausgehen und einen stabilen Geschäftsbetrieb wiederherstellen sollen, wie zum Beispiel:

- explizite Trennung zwischen MBCO und Final-MBCO
- risikobasierte Validierung: technische Machbarkeit, Abhängigkeiten, Lieferanten, Personal
- Management-Genehmigung des Final-MBCO inklusive dokumentierter Risikoakzeptanz
- Plan- und Strategie-Ableitung: Recovery-Schritte müssen zeigen, wie der Übergang vom Not- in den Final-MBCO erfolgt.
- Überprüfung mindestens jährlich oder bei wesentlichen Änderungen; Nachweis im Management-Review

Die Wiederanlaufziele werden nicht isoliert definiert, sondern im Kontext eines realistischen, risikobasierten Gesamtszenarios analysiert und validiert. Das soll die strategische Verbindlichkeit der IT-Wiederanlaufziele erhöhen und soll Inkonsistenzen zwischen Geschäfts- und IT-Perspektive minimieren. Die Validierung des Final-MBCO soll absichern, dass alle IT-Wiederanlaufpläne organisatorisch, technisch und vertraglich umsetzbar sind.

Was bedeutet das für die Umsetzung?

Die Umsetzung der risikobasierten Planung beginnt mit einer erweiterten Analyse auf Basis der durchgeführten BIA. Dabei sind auch Eintrittswahrscheinlichkeiten, Lieferantenabhängigkeiten und Bedrohungsszenarien zu betrachten. Diese Detailtiefe soll transparent machen, wo rein technische IT-Wiederanlaufkapazitäten allein nicht ausreichen.

- Risikobasierte Planung = BIA + (IT-)Risiko- und Abhängigkeitsfaktoren (Bedrohungsszenarien, IT-Dienstleister, Machbarkeit)

Die Norm beschreibt dies unter „Inputs from business impact analysis“ und verlangt, dass das Top-Management die so ermittelten Ergebnisse und Anforderungen formell bestätigt.

Risikobasierte Planung und Final-MBCO

Die Umsetzungsschritte im Detail:

1. **Erweiterte Analyse**
Auf Basis der BIA werden Bedrohungen, Eintrittswahrscheinlichkeiten und Abhängigkeiten erfasst.

2. **Machbarkeitsanalyse**
Lücken zwischen Soll- (BIA-RTO/-RPO) und technischer/organisatorischer Ist-Fähigkeit (ICT-RTO/-RPO) werden identifiziert.

3. **Risikobasierte Entscheidung**
Investition oder formelle Risikoakzeptanz durch Genehmigung höherer Final-MBCO durch Resilience Board.

4. **Dokumentation und Versionierung**
Final-MBCO in Traceability-Matrix, IT-Wiederanlaufplanung, Risikoregister und Auditunterlagen aktualisieren.

5. **Tests & Review**
Szenariotests durchführen und Übergang vom MBCO zum Final-MBCO validieren. Ergebnisse ins KPI-Dashboard und Lessons Learned einfließen lassen.

Praxisbeispiel: Beispiel GmbH – MBCO vs. Final-MBCO

Die Beispiel GmbH betreibt ein zentrales Schadensbearbeitungssystem für Kunden im Versicherungsbereich. Die BIA legt als MBCO fest: Notbetrieb durch manuelle Bearbeitung, begrenzte Datenrecherche max. 48 Stunden.

Gap-Analyse zeigt: Ein vollständiger Recovery des ICT-Service (mit Kundenportal, Datenbank-Replikation und CRM-Integration) ist erst nach 72 Stunden möglich.

Daraus wird ein Final-MBCO abgeleitet: Systembetrieb mit 80 Prozent Funktion nach 72 Stunden, inkl. aktueller Datenlage

Das Resilience Board akzeptiert das Gap durch formellen Beschluss. Der Final-MBCO wird dokumentiert, getestet und in der IT-Wiederanlaufplanung berücksichtigt.

Recovery-Planung und Dokumentationsanforderungen

Die IRBC-Pläne sollen nicht nur technische IT-Wiederanlaufprozesse, sondern auch organisatorische Abläufe, Workarounds und Kommunikationswege umfassen. In der Ausgabe von 2011 wurden Continuity-Pläne zwar empfohlen, galten aber überwiegend als anhängende Technik-Artefakte von DR-Projekten. Die Revision 2025 hebt sie zu einem zentralen "Wirksamkeits-Control". Ein Plan ist erst normkonform, wenn er

- die Trennung zwischen Business-RTO/RPO und ICT-RTO/RPO nachvollziehbar abbildet,
- das Final-MBCO als verbindliche Zielgröße referenziert,
- über einen gesteuerten Lebenszyklus mit Versionskontrolle, Tests und Reviews nachweislich aktuell gehalten wird.

Statische Handbücher sind in eine versionierte, auditierbare Dokumentenlenkung zu überführen, unabhängig vom Medium. Entscheidend ist die prüfbare Verknüpfung von Inhalt, Freigabe, Test und Lessons Learned.
Pläne müssen rollenbasiert, szenariobezogen, vollständig dokumentiert, regelmäßig getestet, aktualisiert und in die BCM-Dokumentation integriert werden. Kommunikation, Eskalation und Entscheidungswege sind verbindlich zu regeln. Die Norm definiert sieben verpflichtende Inhaltsblöcke.

Abschnitt	Inhalt
Zweck & Geltungsbereich	Verknüpfung zur BIA, kritische Services, Auslösekriterien
Recovery-Organisation	Rollen, Eskalationswege, Kontaktdaten, Stellvertreter
Zielmatrix	Nachweis, dass ICT-RTO/RPO ≤ BIA-RTO/RPO, inkl. Final-MBCO-Bezug
Schritt-für-Schritt-Runbooks	Technische Prozeduren, Workarounds, Übergang in Notbetrieb
Kommunikationswege	Freigabe-Flow, Abstimmung mit Incident Response & BCM
Lieferanten & Abhängigkeiten	Kontakte, SLAs, Testbelege, Exit-Klauseln
Lebenszyklus-Nachweis	Versionierung, Tests, Reviews, Lessons Learned

Entscheidend ist, dass alle Informationen revisionssicher abgelegt sind und auch bei einem Ausfall des IT-Betriebs schnell zur Verfügung stehen.

Recovery-Planung und Dokumentationsanforderungen

Was bedeutet das für die Umsetzung?

Praktisch übersetzt sich diese Vorgabe in einen eigenen, auditierbaren **Dokumentenlenkungsprozess** innerhalb des IRBC. Unternehmen müssen ein einheitliches Plan-Template definieren, eine Versionierungs- und Freigabelogik etablieren und einen verbindlichen Test-Kalender verankern. Ob sie dafür ein DMS, ein revisionssicheres Git Repository oder einen physisch geführten Notfallordner nutzen, ist zweitrangig. Wichtig ist, dass Änderungen, Tests und Reviews nachvollziehbar protokolliert werden und dass stets eine **Kopie offline verfügbar** ist. Ergänzend ist es sehr sinnvoll eine automatische Verknüpfung mit dem Change und Incident Management zu etablieren, sodass jede relevante Änderung an IT-Systemen oder Prozessen automatisch einen Plan-Review auslöst und Testergebnisse in ein Resilience-KPI-Dashboard fließen.

Umsetzungsschritte

1. Plan-Template definieren – einheitliche Struktur für Audit-Nachweise.
2. Dokumentenlenkung aufsetzen inkl. Freigabe-Workflow
3. Change-Trigger verknüpfen – relevante Änderungen lösen automatisch Plan-Review aus
4. Offline-Verfügbarkeit sicherstellen – Kopien in IT-Notfall- und/oder Krisenräumen, Notfall-Laptops oder gesicherter Cloud-Umgebung

Plan-Lifecycle

Erstellung → Versionierung → Test → Review → Lessons Learned → Aktualisierung

- Versionierung: jede Änderung mit Freigabevermerk (Owner + Datum)
- Durchführung regelmäßiger Tests nach zeitlicher Frequenz oder bei Systemänderung
- Review-Ergebnisse in den Management-Report einfließen lassen.
- Lessons Learned: Verbesserungen und KPI-Abgleich dokumentieren

IRBC-Strategien und Wiederherstellungsdesign

In der ISO 27031:2025 wird die Auswahl von IRBC-Strategien entlang von sechs Wirkungskategorien strukturiert. Ziel ist ein ganzheitliches Resilienz-Design, das technische, organisatorische und lieferantenbezogene Aspekte integriert. Strategien sollen nicht isoliert, sondern in ihrer Wechselwirkung betrachtet werden, um konsistente und wirtschaftlich tragfähige Lösungen zu schaffen.

Strategien bzw. Lösungen müssen abgeleitet werden für die Kategorien Skills, Facilities, Technology, Data, Processes und Suppliers. Die Auswahl soll risikobasiert, wirtschaftlich tragfähig und aufeinander abgestimmt sein. Wechselwirkungen sind zu analysieren, Strategien nachvollziehbar zu dokumentieren.

Was fordert die Norm konkret?

Für jede der sechs Kategorien sind Strategien bzw. Lösungskonzepte zu entwickeln, zu bewerten und zu dokumentieren:

Kategorie	Typische Optionen	Auswahlkriterien
Skills & Knowledge	Cross-Training, Skill-Redundanz, Zertifizierungen	Kritische Kompetenzen, Verfügbarkeit von Experten
Facilities	Zweitstandort, Carrier-neutrales Rechenzentrum, Mobile Datacenter	Geo- und Klimarisiken, Anbindung
Technology	Active-Active-Cluster, automatisiertes Failover, Zero-Trust-Segmente	RTO/RPO, Komplexität, Lizenzmodelle
Data	Immutable Backups, Air-Gap, Echtzeit-Replikation	RPO-Anforderungen, Datenvolumen, Latenz
Processes	Automatisierte Runbooks, SOAR-Playbooks, Escalation Matrix	Prozesskritikalität, Automationsreife
Suppliers	Multi-Cloud-Strategien, Provider-Failover, Exit-Klauseln	Abhängigkeitsrisiken, SLA-Qualität, Vertragsstrafen

IRBC-Strategien und Wiederherstellungsdesign

Was bedeutet das für die Umsetzung?

- Strategien müssen risikobasiert und wirtschaftlich tragfähig ausgewählt werden.
- Wechselwirkungen und Abhängigkeiten sind zu analysieren und zu dokumentieren.
- Jede Strategie muss auf die definierten RTO-/RPO-/MBCO-Ziele ausgerichtet sein.
- Die Umsetzung ist regelmäßig zu überprüfen und anzupassen.

Unternehmen müssen dafür ein strukturiertes Verfahren zur Strategieentwicklung etablieren. Das umfasst mindestens:

- Bewertungsschema für Risiken, Kosten, Komplexität und Umsetzbarkeit
- Szenarienvergleiche (z. B. technisches vs. organisatorisches Recovery-Design)
- Wirtschaftlichkeitsanalysen (CAPEX, OPEX, Lebenszykluskosten)
- zentrales Resilienzstrategiedokument, das als Referenz für Planung, Tests und Audits dient

Praxisbeispiel

Für eine kritische Kundenservice-Plattform wird eine Kombination aus Cloud-Failover, dezentralem IT-Notbetrieb und Workarounds auf manueller Basis entwickelt. Die Strategie wird regelmäßig mit Stakeholdern validiert und dokumentiert.

Umsetzungsempfehlungen für Unternehmen

Übergang von ISO 27031:2011 auf die Version 2025

Für Unternehmen, die bisher nach ISO/IEC 27031:2011 oder einem klassischen IT-Disaster-Recovery-Framework arbeiten, empfiehlt sich ein dreistufiges Migrationsmodell. Ziel ist es, die neuen Governance-Vorgaben, erweiterten Dokumentationspflichten und das Konzept des Final-MBCO schrittweise zu integrieren, ohne den laufenden IT-Betrieb zu überlasten.

Schritt 1 – Gap-Analyse

Ziel: Erfassung des Ist-Zustands und Identifikation von Lücken gegenüber der ISO/IEC 27031:2025

Vorgehen:

- Sammlung aller relevanten Dokumente: ICT-Continuity-Pläne, Notfallhandbücher, Testberichte, BIA-Ergebnisse, Auditberichte
- Abgleich der Dokumente mit den dreizehn Kapiteln der Norm
- Häufige Lücken:
  - _ fehlende IRBC-Policy
  - _ unvollständige Traceability von BIA-Zielen zu ICT-RTO/RPO
  - _ kein Resilience Board
  - _ fehlende KPIs für RTO-/RPO-Messung
- Erstellung einer Reifegradübersicht (0–5) und Ableitung schneller Quick-Wins:
  - _ Benennung eines IRBC-Managers
  - _ einfaches KPI-Dashboard
  - _ erste Version der Traceability-Matrix

Umsetzungsempfehlungen für Unternehmen

Schritt 2 - Schließung prioritärer Lücken

Governance:

- Veröffentlichung der IRBC-Policy mit Managementfreigabe
- Einrichtung des Resilience Board (BCM, IRBC, ISMS, Risikomanagement, ICT-Betrieb)
- Budgetrahmen für IRBC-Maßnahmen freigeben

Dokumentation:

- vollständige Traceability-Matrix: Geschäftsprozess → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → Final-MBCO → Testnachweis
- Integration in die Dokumentenlenkung

Technische Maßnahmen:

- Versionierung aller ICT-Continuity-Pläne
- Offline-Bereitstellung (Krisenraum, Notfall-Laptops, gesicherte Cloud)
- Testkalender (mind. ein Mal jährlich Live-Failover oder Restore Drill)
- erste Immutable-Backup- und Air-Gap-Strategien

Schritt 3 - Optimierung und Audit-Readiness

Optimierung:

- KPI-Dashboards im Regelbetrieb
- systematischer Lessons-Learned-Prozess
- Szenarioübungen (z. B. Ransomware, Lieferantenausfall, Ausfall der Haupt-Cloudregion)
- Nachweis der Fähigkeit zum Übergang MBCO → Final-MBCO

Audit-Readiness:

- vollständige Proof-Chain
- Audit-Repository mit IRBC-Policy, Traceability-Matrix, Plänen, Testberichten, Management-Review-Protokollen

Umsetzungsempfehlungen für Unternehmen

Umsetzungstabelle

Maßnahme	Verantwortlich
IRBC-Policy erstellen und freigeben	IRBC-Manager, Geschäftsführung
Resilience Board einrichten	Geschäftsführung
Traceability-Matrix implementieren	IRBC-Manager, BCM
Testkalender festlegen	IRBC-Manager, ICT-Betrieb
Immutable Backup umsetzen	ICT-Betrieb
Szenarioübung „Ransomware“	IRBC-Manager, ISMS
Final-MBCO dokumentieren und freigeben	IRBC-Manager, Management
Audit-Readiness-Check durchführen	IRBC-Manager, internes Audit

Umsetzungsempfehlungen für Unternehmen

Übergang vom klassischen ITSCM zu ISO/IEC 27031:2025

Unternehmen, die bisher ein klassisches IT Service Continuity Management (ITSCM) nach ITIL-Prinzipien betreiben, müssen ihr Vorgehen strategisch erweitern. Während ITSCM den technischen IT-Wiederanlauf einzelner ICT-Services fokussiert, integriert ISO 27031 IRBC als strategischen Resilienzbaustein in das BCMS.

1. **Governance**
   - Einrichtung eines Resilience Board
   - Anpassung der ITSCM-Manager-Rolle zum IRBC-Manager
   - Einführung quartalsweiser Management-Reviews
2. **Dokumentation**
   - Umwandlung von DR-Plänen in vollständige ICT-Continuity-Pläne
   - Einführung einer Traceability-Matrix
   - Versionierung und revisionssichere Ablage
3. **Integration**
   - Verzahnung von ITSCM mit BCM, ISMS und Incident Response
   - Abgleich mit ISO 27002 A.5.30 und A.8.16
   - einheitliche Eskalations- und Freigabewege
4. **Anpassung Teststrategie**
   - technische Failover-Tests beibehalten
   - Ergänzung um szenariobasierte Übungen (Cyberangriff, Cloud-Ausfall, Lieferantenausfall)
   - Lessons Learned in Pläne und KPIs integrieren

Ausblick

Die ISO/IEC 27031:2025 stellt den Übergang von technischer Notfallplanung zu einem strategischen, organisationsweiten Resilienzmanagement dar. Unternehmen müssen ihre Strukturen, Prozesse und Rollen entsprechend anpassen, um die erweiterten Anforderungen zu erfüllen.

Sie haben Fragen zum Thema? Melden Sie sich gern bei uns!

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

Stand: September 2025

Die Controllit AG ist Ihr Partner für Business Continuity Management (BCM). Seit unserer Gründung entwickeln wir integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management, Information Security Management und Krisenmanagement. Wir helfen Ihnen mit strategischen, organisatorischen und technischen Konzepten, Ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Foto-/Grafiknachweise: Titel: 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