Luxgap

DATA PRIVACY PARTNER

LUXGAP

BUSINESS CONTINUITY

BCMS / BCP as-a-Service

A business continuity management system **ISO 22301 compliant**, aligned with **NIS2** and **DORA**, continuously maintained and accessible in all circumstances.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

CHAPTER 1 CHALLENGES & REGULATORY FRAMEWORK

Why an "always-on" BCMS/BCP?

Business continuity = regulatory requirement + operational resilience

A "static" BCP — a document filed in a shared folder and rarely updated — is rarely usable on the day a crisis occurs. Organizations experiencing a major outage often discover too late that their plans are obsolete, contacts have changed, IT dependencies have evolved, or procedures no longer match operational reality. The **Luxgap** offer addresses this by implementing and maintaining a **Business Continuity Management System (BCMS)** compliant with **ISO 22301**, tested at least once a year, and accessible even in the event of total unavailability of your infrastructure.

NIS2 (EU Dir. 2022/2555)

- Cyber risk management measures imposed on "essential" and "important" entities
- Explicitly includes business continuity: crisis management, backups, disaster recovery
- "State of the art" approach and alignment with recognized standards (ISO 22301 / ISO 27001)

DORA (EU Reg. 2022/2554)

- Direct obligation for the financial sector: ICT business continuity, response, and recovery plans
- BIA required + periodic testing of plans, including those involving third-party ICT providers
- Traceability and proof of effectiveness: audits, exercise reports, documented corrective actions

Expected Result

Rapid Decisions

Predefined roles, clear escalation criteria, priorities established in advance to act without hesitation in the critical first minutes of an incident.

Achievable RTO/RPO

Recovery objectives defined and validated for each critical process, IT system, and service provider, ensuring realistic and measurable recovery times.

Controlled Communication

Pre-validated communication plans for customers, supervisory authorities, partners, and media, reducing reputational risk and notification obligations.

Audit File Ready

Complete set of auditable evidence aligned with ISO 22301, NIS2, and DORA: policies, exercise reports, CAPA, management reviews, and change logs.

CHAPTER 2 CONTINUITY PORTAL

BCP accessible in all circumstances

Website independent of your infrastructure — 'break-glass' access option guaranteeing availability even in the event of total disaster

One of the main pitfalls of traditional continuity plans is their inaccessibility when they are most needed. If your plans are stored on an internal server, SharePoint, or intranet, a ransomware cyberattack or infrastructure failure makes them unavailable at the critical moment. The Luxgap portal solves this paradox by hosting your entire BCMS on a dedicated infrastructure, totally independent of your IS.

Structure of the continuity portal

- **"Total crash" page**: what to do in the first 0–60 minutes — immediate activation checklists, critical decisions to make, priority contacts
- **Escalation tree**: trigger thresholds, priority levels, formal BCMS activation criteria
- **Crisis Committee**: roles, responsibilities, designated replacements, multi-channel contact information
- **Operational plans**: ITDR/DRP, business continuity, crisis communications, vendor management
- **Practical appendices**: asset inventories, manual workaround procedures, pre-validated message templates
- **Offline exports**: downloadable PDFs + encrypted backup of all content

Operational Guarantees

24/7 Access

Permanent availability even if all your internal servers are unavailable. Independently hosted infrastructure with geographical redundancy.

Access Control & Logging

Secure authentication and timestamped access logs providing auditable evidence of use during audits or post-incident investigations.

Continuous Updates

Each organizational or IT change triggers a BCMS update. The portal continuously reflects the operational reality of your organization.

Full Traceability

Full versioning of all documents and a timestamped change log, ensuring a continuous audit trail and regulatory compliance.

CHAPTER 3 OUR OFFER

"BCMS as-a-Service" Offer (all-inclusive)

Implementation + maintenance + audit evidence + annual exercises (minimum) — all in a **monthly subscription** aligned with **ISO 22301 / NIS2 / DORA** with **continuous risk management**.

Our "all-inclusive" offer covers the entire BCMS lifecycle, from initial implementation to operational maintenance, including exercises and the production of auditable evidence. This "as-a-Service" approach eliminates the burden of internal management while ensuring a constant and demonstrable level of maturity.

Initial Implementation

- Framing: scope, stakeholders, applicable regulatory requirements
- BIA + Risk Assessment (disruption scenarios) + comprehensive dependency mapping
- RTO/RPO/MTPD definition by critical processes and services
- Strategies & solutions: people / premises / technology / suppliers / data
- Drafting of plans and procedures: crisis, communication, continuity, ITDR

Run & Continuous Maintenance

- PDCA Cycle: objectives, KPI/KRI, periodic reviews, corrective actions
- Change management (IT, providers, organization) with immediate update
- Continuous update of the BC portal + strict version control
- Awareness and training: managers, operational teams, on-call staff
- Regulatory watch: NIS2/DORA developments + "state of the art" standards

Exercises & Evidence

- Annual simulation exercise (tabletop + crisis communication)
- Targeted technical test(s) if ITDR included (restoration, failover)
- Exercise report + structured REX + action plan (CAPA)
- Internal ISO 22301 audit + annual management review
- Audit file ready for certification (if desired)

CHAPTER 4 ISO 22301 IN DETAIL

ISO 22301:2019 — Requirements (clauses 4 to 10)

The BCMS is a **management system** (Annex SL structure): **PDCA + evidence**. It is not a simple document, but a living system for continuous planning, execution, verification, and improvement.

PLAN

Clauses 4–7: Context, Leadership, Planning, Support

DO

Clause 8: BIA/Risks, Strategies, Plans, Exercises

ACT

Clause 10: CAPA, Continuous Improvement

CHECK

Clause 9: KPI/KRI, Internal Audit, Management Review

What « ISO 22301 compliant » entails (without compromise)

01

Scope, policies, formalized roles and responsibilities

The BCMS must be based on a documented framework, validated by management, with authorities clearly assigned at each level of the organization.

02

BIA process + disruption risk assessment

Impact analysis and identification of threat scenarios, periodically reviewed to reflect changes in the operational and technological environment.

03

Validated strategies and solutions

Complete coverage of critical resources: people, premises, IT, data and suppliers, with tested and documented solutions.

04

Executable plans and procedures + communication

Operational documents ready for use, including internal and external crisis communication with pre-validated templates.

05

Exercise/testing program + continuous improvement

Regular validation of the effectiveness of arrangements with structured feedback loop and tracked corrective actions.

06

Document control and auditable records

Rigorous document control: versioning, approvals, controlled distribution, and retention of evidence for each requirement.

Everything is maintained over time — a BCMS is not a static document but a living system that evolves with your organization, your technologies, and your regulatory environment.

ISO 22301 — Clauses 4 to 6 (Framing & Governance)

Foundations of the BCMS: organizational context, management commitment, objective and action planning.

Clauses 4 to 6 form the bedrock upon which the entire management system rests. They define the "why" and "how" of the BCMS even before the production of operational plans. Without these solid foundations, continuity plans lack strategic anchoring and organizational legitimacy.

1

Clause 4 — Context

- Analysis of internal and external context + identification of interested parties and their expectations
- Definition of the BCMS scope (services, sites, entities) with justification for any exclusions
- Mapping of critical processes and dependencies: people, IT, data, suppliers
- Register of applicable requirements: NIS2, DORA, contractual obligations, sectoral requirements

2

Clause 5 — Leadership

- Continuity policy validated by management + definition of measurable BC objectives
- Assignment of roles and authorities: steering sponsor, BC manager, business owners, ITDR, communications
- Establishment of the crisis committee: ensured succession, formalized decision rules, operational call-tree
- Integration of the BCMS into existing processes: risk management, compliance, purchasing, IT

3

Clause 6 — Planning

- Identification of risks and opportunities related to the BCMS + prioritized action plan
- Measurable objectives: target RTO/RPO, activation times, test success rates
- Planning for anticipated changes: cloud migration, M&A, service provider changes
- Trigger criteria, escalation levels, and return-to-normal conditions

ISO 22301 CLAUSE 7 — SUPPORT

ISO 22301 — Clause 7 (Support)

Competencies, awareness, communication, document control — the essential resources for BCMS operation

Clause 7 ensures that people have the necessary competencies, that communication channels are defined and tested, and that all documentation is controlled. These "support" elements are often underestimated but form the operational backbone of the system.

"Support" deliverables included in the subscription

Competencies & awareness

- Detailed competency plan: who needs to know what, and when
- Training matrix covering crisis leaders, ITDR teams, business units, reception, and communications
- Continuous awareness: periodic reminders, onboarding integration, participation in exercises
- Register of "break-glass" authorizations and formalized deputies

Controlled communication

- Crisis communication plan (internal and external) with pre-validated message templates
- Prioritized contact directory: key clients, supervisory authorities, critical service providers
- Defined alternative channels: phone/SMS, out-of-IT messaging, dedicated BC website
- Media management and message consistency to reduce reputational risk

Documents & evidence

- Complete document control: versioning, approval, controlled distribution
- Traceability: evidence of exercises, crisis reports, documented CAPA
- Register of changes and deviations (identified non-conformities)
- Structured retention of records (audit evidence pack)

ISO 22301 CLAUSE 8.2 — BIA & RISKS

ISO 22301 — Clause 8.2 (BIA + Risk Assessment)

Factual basis: impact, priorities, recovery objectives — the analytical foundation of any continuity strategy

BIA (Business Impact Analysis)

The business impact analysis forms the foundation of the BCMS. It objectively establishes which activities are critical, within what timeframe they must be restored, and which resources are essential for their operation.

1 Inventory of activities and processes

Classification by criticality level: "critical / important / support". Each process is evaluated based on its role in the value chain and its impact in case of interruption.

2 Analysis of impacts by time horizon

Multi-dimensional assessment: financial, legal/regulatory, clients, personal safety, reputation. Impacts are projected over different horizons (1h, 4h, 24h, 72h, 1 week…).

3 MTPD / MTPoD + RTO and RPO

Definition of the Maximum Tolerable Period of Disruption (MTPD) and the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical process and service.

4 Mapping of dependencies

Exhaustive identification of necessary resources: applications, databases, key personnel, physical sites, third-party suppliers and service providers.

Disruption risk assessment

- **Scenarios assessed**: cyberattack/ransomware, critical failure (IS, network, cloud), data loss or corruption, unavailability of a major ICT supplier, physical site disaster
- **Method**: probability × severity × detectability → risk prioritization and identification of control needs
- **Preventive & resilience measures**: backup, network segmentation, redundancy, manual bypass procedures
- **Planned reviews** + "hot" reviews after each significant incident or major environmental change

BCMS Outputs (governance)

- Consolidated RTO/RPO
- Recovery prioritization
- List of critical resources
- Supplier contractual requirements
- Prioritized improvement backlog

ISO 22301 CLAUSE 8.3 — STRATEGIES & SOLUTIONS

ISO 22301 — Clause 8.3 (Strategies & Solutions)

Choosing realistic solutions to meet RTO/RPO

Based on the requirements from the BIA and risk assessment, we design and validate end-to-end continuity strategies covering all critical resources: people, premises, technology, data, and supplier chain. The objective is to ensure that each strategy is not only documented but also realistic, tested, and maintained over time.

Solution Axes

People

Identified critical resources, formalized backup, defined on-call duties, 'break-glass' access to essential systems in case of unavailability of usual personnel.

Premises

Activatable remote work, pre-identified alternative sites, secure physical access, documented evacuation and fallback procedures.

Technology

Defined recovery architecture, documented restoration and failover procedures, tested and versioned technical runbooks.

Data

3-2-1 backup strategy, immutability of backups, regularly tested restoration, compliance with defined RPOs.

Suppliers

BC clauses integrated into contracts, communicated RTO/RPO requirements, documented replacement plans and exit strategies.

Design Decisions

- **Service levels by criticality** (bronze/silver/gold) and by process, allowing for proportionate sizing of solutions
- **Recovery by « wave »** : documented priorities, dependencies, and sequencing for an orderly recovery
- **Acceptance criteria** : tests, metrics, evidence, and controls defined to validate each solution
- **Cyber resilience measures** : network segmentation, MFA, administrator access control, logging
- ITDR ↔ business continuity alignment to avoid "siloed plans" that contradict each other on D-Day

Deliverables

- Consolidated BC strategy (by scenario and criticality)
- Solutions catalog + costs / efforts / dependencies
- Supplier requirements & contractual clauses
- ITDR runbooks and business checklists
- Prioritization matrix (re-activation)

ISO 22301 | CLAUSE 8.4 — PLANS & PROCEDURES

ISO 22301 — Clause 8.4 (plans & procedures)

Executable, available, and trained documents — plans your teams can actually use under pressure

Ready-to-run plan pack included

1

Crisis Management Plan

System activation, decision-making process, crisis log maintenance, crisis end criteria and return to normal mode.

2

Communication Plan

Coordinated internal and external communication with pre-validated "message map" for each audience: employees, customers, regulators, media.

3

Business Continuity Plan

Operational workarounds, recovery priorities, necessary resources, and delegation of authority to maintain critical activities.

4

ITDR / DRP

Restoration, failover, rebuild of critical systems with detailed and sequenced technical runbooks.

5

Critical Supplier Plan

Continuity SLAs, escalation procedures, pre-identified alternatives, and exit plan for each critical supplier.

6

Return to Normal Plan

Controlled return to normal operations, structured post-mortem, and corrective action plan (CAPA).

Ready-to-use scenarios

Each scenario includes: **immediate actions (0–60 min)**, **responsible parties & contacts**, **escalation decisions / criteria**, **pre-written communications**, and **return to normal procedure**.

- Cyberattack / Ransomware
- Critical Outage (IT system, network, cloud)
- Data loss / corruption
- ICT supplier unavailability
- Disaster / site incident
- HR unavailability (pandemic, strike)

ISO 22301 | CLAUSE 8.5 & 8.6 — EXERCISES & EVALUATION

ISO 22301 — Clauses 8.5 & 8.6 (exercises & evaluation)

Test, measure, correct: at least 1 exercise per year + after each major change

The exercise program validates the actual effectiveness of strategies and plans under simulated conditions. It produces documented and actionable evidence during certification audits, controls by supervisory authorities, or client due diligence. An untested plan is merely a hypothesis.

Types of Exercises

Tabletop

Crisis management simulation: decisions, escalation, prioritization, coordination of the crisis committee in a realistic scenario.

Call-tree / mobilization

Test of contact times and effective role assumption. Verification of team availability and responsiveness.

Communication Exercise

Notification simulation to clients, regulator, and press with the use of pre-validated messages.

Technical ITDR Test

Restoration, failover, and execution of runbooks in a test environment — if the ITDR scope is included.

Supplier Exercise

Coordination with critical providers: SLAs, tipping points, exit and replacement procedures.

Annual Test Governance

- **Scenario defined based on risks and BIA** with measurable objectives and clear success criteria
- **Observer roles** designated + success criteria: RTO/RPO achieved, time-to-decision, communication quality
- **Event log** maintained in real-time and collection of structured evidence during the exercise
- **Structured REX** (root cause analysis) + prioritized action plan (CAPA) with owners and deadlines
- **Plan updates** and formal revalidation after integrating identified corrections

Auditable Outputs

1. Exercise Plan
2. Exercise Report
3. CAPA & Follow-up
4. Formal Evaluation
5. Portal Update

ISO 22301 | CLAUSES 9 & 10 — AUDIT & IMPROVEMENT

ISO 22301 — Clauses 9 & 10 (measurement, audit, improvement)

Prove control and continuously improve — the BCMS does not just exist; it must demonstrate its effectiveness tangibly and continuously.

Clause 9 — Performance Evaluation

KPI / KRI

BIA coverage, plan update rate, exercise success, recovery times measured vs. objectives.

Internal Audit ISO 22301

Structured audit program, checklists by clause, documented findings, and collected evidence.

Management Review

Evaluation of BCMS adequacy, resource allocation, strategic decisions, and prioritization of actions.

Management / Risk Reporting

Monthly or quarterly dashboard summarizing the BCMS status, residual risks, and ongoing actions.

Clause 10 — Improvement

Non-conformity Management

Identification, documentation, and treatment of deviations with formalized corrective actions (CAPA) and follow-up until closure.

Post-incident & Post-exercise Improvement

Structured feedback (REX) after each significant incident or exercise, feeding the improvement cycle.

Treatment of Major Changes

New services, cloud migrations, outsourcings: each change triggers a BCMS re-evaluation.

Procedure Optimization

Simplification, automation, and reinforcement of the robustness of plans and procedures over time.

Evidence pack (audit-ready) continuously maintained

All evidence required by ISO 22301, NIS2, and DORA is collected, organized, and proactively kept up-to-date in the continuity portal. At any time, your organization has a complete and actionable audit file, without last-minute preparation efforts.

CHAPTER 5 REGULATORY ALIGNMENT

ISO 22301 ↔ NIS2 ↔ DORA Alignment

ISO 22301 provides the "system"; NIS2 and DORA set legal obligations.

Our approach: use ISO 22301 as a structuring backbone and simultaneously produce the evidence required by NIS2 (risk management measures for essential and important entities) and DORA (digital operational resilience for the financial sector). A single BCMS, three compliance frameworks covered.

ISO 22301 (deliverable)	NIS2 — Risk Management Measures	DORA — ICT BCP (response & recovery)	Concrete Benefit
8.2 BIA + risks	Business continuity, crisis management, risk assessment imposed by the directive	BIA + ICT disruption scenarios, basis for response and recovery plans	A single factual analysis serving all three frameworks
8.3 Strategies / solutions	Backups, recovery, resilience, "state-of-the-art" controls	ICT Plans, backup/restoration, solutions for critical functions	Validated and end-to-end dimensioned strategies
8.4 Plans / procedures	Crisis management and operational continuity (effective execution)	Response & recovery, communication, ICT supplier continuity	Executable and tested plans, not just documented
8.5–8.6 Exercises / evaluation	Demonstrable capability (tests/exercises) + continuous improvement	Periodic ICT plan tests + measurable proof of effectiveness	Proof of effectiveness usable by supervisors
9–10 Audit & improvement	Governance and proportionate measures, proof of execution	Traceability, internal control, reporting and remediation	Complete and always up-to-date audit file

→ **Result:** operational continuity that is **provable** and **auditable** — not just "documentation" stored in a shared folder. Your organization can demonstrate its compliance with all three regulatory frameworks at any time with a single management system.

CHAPTER 6 CERTIFICATION

ISO 22301 Certification (Possible)

Preparation included: documentation, evidence, internal audits, support — our subscription prepares and maintains a continuously certifiable BCMS.

ISO 22301 certification is a powerful lever of trust for your customers, partners, and supervisory authorities. It relies on an external audit conducted by an accredited certification body and demonstrates that your business continuity management system is not only documented but effectively operational and continuously improved.

Path to Certification

1. Framing & Scope
2. BIA & Risks
3. Solutions & Plans
4. Exercises & Evidence
5. Internal Audit
6. Management Review
7. Stage 1/2 Audit
8. Maintenance (Surveillance)

Responsibility Allocation

What Luxgap handles

- Drafting and maintaining all documented information required by the standard
- Providing the BC portal with version control and complete traceability
- Exercise and testing program + detailed report and CAPA
- Conducting the internal audit + support during the external certification audit
- Managing post-audit actions: addressing non-conformities and opportunities for improvement

Expected Client Role

- Appointing business and IT owners as well as a management level sponsor
- Validating objectives (RTO/RPO) and arbitrating choices for continuity solutions
- Actively participating in exercises with key decision-makers
- Providing visibility on changes: IT, suppliers, organization
- Approving external messages and policies (management validation)

CHAPTER 7 SERVICE GOVERNANCE

Service Governance (RACI) — all-inclusive monthly

A living BCMS: continuous updates + annual test + evidence — your business continuity managed as a service with clear responsibilities.

The RACI matrix below clarifies the distribution of responsibilities between Luxgap and your internal teams. This transparent governance ensures that each BCMS activity has an identified responsible party and a legitimate approver, while maintaining the appropriate involvement of your IT and business functions.

RACI (excerpt)

Activity	Luxgap	Management	IT	Business
BCMS Steering (PDCA)	**R**	**A**	C	C
BIA / RTO-RPO	**R**	**A**	C	C
ITDR / DRP (runbooks)	C	I	**R**	C
Crisis Committee & Communications	**R**	**A**	C	C
Annual Exercise + Report	**R**	**A**	C	C
Internal Audit & Management Review	**R**	**A**	C	C

R = Responsible (performs) | **A** = Accountable (approves) | **C** = Consulted (contributes) | **I** = Informed

24/7	1+/year	100%	3
Portal Access	Simulation Exercise	Evidence Maintained	Frameworks Covered
Permanent BCP availability	Full system test	Evidence pack always up-to-date	ISO 22301, NIS2, DORA

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116