BUSINESS CONTINUITY MATURITY ASSESSMENT

A 10-minute self-assessment benchmarked against ISO 22301.
Identify your gaps before a crisis does.

commercial@sicurogroup.com • www.sicurogroup.com

SICURO GROUP

How to use this assessment. For each of the 10 dimensions below, read the four descriptions and circle or tick the one that most accurately reflects your organisation's current state. Score each dimension 0–3. Transfer your scores to the summary sheet on page 2, total them, and locate your maturity band. There are no right or wrong answers — an honest assessment produces the most useful result.

SCORING GUIDE

0	1	2	3
Not in place	**Informal / Ad hoc**	**Documented**	**Tested & embedded**
Nothing exists — no policy, procedure, or ownership	Understood informally but not documented or tested	Written procedures exist with named owners, not yet tested	Exercised, reviewed, and embedded in operational practice

DIMENSIONS 1–5

01 Governance & Crisis Authority — 5.3

Does a named individual have documented authority to declare a crisis and activate emergency procedures, with at least one named successor?

0 ☐	1 ☐	2 ☐	3 ☐
No designated person or process	Understood informally, not written down	Documented with named successor	Documented, tested, communicated to all relevant staff

02 Business Impact Analysis — 8.2.2

Have RTOs and MTPDs been defined, validated by business owners, and linked to recovery strategies for all critical functions?

0 ☐	1 ☐	2 ☐	3 ☐
No formal BIA completed	Rough estimates, not documented	RTOs/MTPDs documented for most critical functions	Full BIA validated by leadership, linked to strategies

03 Crisis Response Structure — 8.4.2

Could your team execute a structured response — with clear ownership and escalation — without improvising? Are procedures accessible if IT is unavailable?

0 ☐	1 ☐	2 ☐	3 ☐
No crisis response procedure exists	Some guidance exists, never tested	Documented procedures, offline-accessible, owned by named roles	Tested in exercises with after-action reports

04 IT & Cyber Resilience — 8.4.4

If ransomware encrypted all operational systems tonight, is there a tested IT disaster recovery plan and manual fallback for critical operations?

0	1	2	3
No plan — would be managed reactively	IT team has rough approach, no documented ITDR	ITDR plan with defined RTOs and manual fallbacks	ITDR tested, backups verified, cyber incident response active

05 Supply Chain & Third-Party Dependencies — 8.1

Do you know whether critical suppliers have BCM plans that cover the failure modes that affect you, and are continuity obligations in your contracts?

0	1	2	3
No review of supplier BCM conducted	We assume suppliers have plans, unconfirmed	Critical suppliers asked to confirm BCM capability	BCM reviewed, obligations contractual, alternatives identified

DIMENSIONS 6–10

06 Mass Notification & Communication — 8.4.3

Could your team execute a structured response — with clear ownership and escalation — without improvising? Are procedures accessible if IT is unavailable?

0	1	2	3
No crisis response procedure exists	Some guidance exists, never tested	Documented procedures, offline-accessible, owned by named roles	Tested in exercises with after-action reports

07 Vital Records & Offline Access — 7.5.3

Could your team execute a structured response — with clear ownership and escalation — without improvising? Are procedures accessible if IT is unavailable?

0	1	2	3
No crisis response procedure exists	Some guidance exists, never tested	Documented procedures, offline-accessible, owned by named roles	Tested in exercises with after-action reports

08 Regulatory & Compliance Continuity — 4.2.2

Could your team execute a structured response — with clear ownership and escalation — without improvising? Are procedures accessible if IT is unavailable?

0	1	2	3
No crisis response procedure exists	Some guidance exists, never tested	Documented procedures, offline-accessible, owned by named roles	Tested in exercises with after-action reports

09 Exercise Programme — 8.5

Has your organisation run a structured tabletop exercise or simulation within the past 12 months, with a documented after-action report and tracked remediation?

0	1	2	3
☐	☐	☐	☐
No exercise of any kind conducted	Informal discussion only, or exercise 3+ years ago	Exercise within past 2 years with some documented findings	Annual programme, after-action reports, tracked remediation

10 Financial Resilience — 8.3.4

If all revenue-generating activity stopped completely, how long could the organisation meet fixed obligations from liquidity and credit facilities? Has this been stress-tested?

0	1	2	3
☐	☐	☐	☐
Less than 4 weeks — or never assessed	4–8 weeks from current liquidity	2–3 months with access to credit facilities	3+ months, stress-tested, documented financial continuity strategy

Summary & Gap Report

Transfer your scores below, total them, and identify your maturity band.

SCORE TALLY

#	DIMENSION	ISO 22301 CLAUSE	SCORE
01	Governance & Crisis Authority	5.3	_____
02	Business Impact Analysis	8.2.2	_____
03	Crisis Response Structure	8.4.2	_____
04	IT & Cyber Resilience	8.4.4	_____
05	Supply Chain & Third-Party Dependencies	8.1	_____
06	Mass Notification & Communication	8.4.3	_____
07	Vital Records & Offline Access	7.5.3	_____
08	Regulatory & Compliance Continuity	4.2.2	_____
09	Exercise Programme	8.5	_____
10	Financial Resilience	8.3.4	_____
TOTAL SCORE			_____ / 30

MATURITY BANDS — CIRCLE YOUR RESULT

0-7 — **Foundational — significant exposure**

Your BCM programme is at an early stage. The gaps identified represent material operational, regulatory, and reputational risk. The immediate priority is not certification — it is establishing the basic structures that allow your organisation to function during a disruption. A gap analysis will identify the fastest path to meaningful resilience.

8-14 — **Developing — key gaps present**

Some foundations exist, but critical gaps in testing, documentation, or ownership create significant vulnerabilities. A structured gap analysis will identify which gaps carry the highest near-term risk and the most efficient route to closing them before they are exposed by a real event.

15-21 — **Established — validation required**

Your programme has meaningful substance. The next stage is validation — ensuring plans are exercised, successors are briefed, and third-party dependencies are mapped. An independent review will surface the gaps that internal assessment reliably misses.

22-30 — **Advanced — optimisation focus**

You have a mature BCM programme. Focus should shift to continual improvement: stress-testing against emerging threat scenarios, integrating BCM into operational decision-making, and ensuring the programme remains current as the business and regulatory environment evolve.

PRIORITY GAPS — NOTE DIMENSIONS SCORING 0 OR 1

1.
2.
3.
4.
5.

What comes next

This assessment identifies where gaps exist. A Sicuro Group consultant session maps exactly what it would take to close them — with a prioritised programme, realistic timelines, and cost-effective solutions tailored to your sector and risk profile. We have delivered BCM gap analyses and ISO 22301 implementation programmes for clients across energy, financial services, and critical infrastructure in EMEA.

To arrange a free 45-minute gap analysis session: commercial@sicurogroup.com
sicurogroup.com · Sicuro Group LLC