GOVERNANCE DOCS

Business Continuity Risk Assessment

Kestrel Foods (sample)

The chilled ready-meal production site, the distribution centre and the systems that take and fulfil retailer orders.

ASSESSED	25 September 2026
METHOD	ISO 22301:2019, clause 8.2.3, with continuity measures from clause 8.3
IN SCOPE	12 scope items, 12 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PROFILE	Manufacturing and industrial
PREPARED BY	Governance Docs

CONTENTS

Where the organization's risks stand

PROCESS SCORE

91 / 100

Level 2 · Developing

The risks are identified, but gaps in rating or treatment would not survive an audit.

Held at Developing while 1 critical finding is open; the score alone would place it higher.

Initial | **Developing** | Defined | Managed

The score measures how complete and defensible the assessment is, not how risky the organization is.

RISKS	ABOVE APPETITE	CRITICAL	ABOVE AFTER TREATMENT	FINDINGS
12	5	0	1	4

WHAT THIS ASSESSMENT TELLS YOU

- 5 of 11 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-05, recovery arrangements never tested, at level 16 (High), owned by Business Continuity Manager.
- 1 risk above the line has no treatment decision yet (R-05). Until it has one, the treatment plan is incomplete.
- Planned treatment brings the number of risks above the line from 5 to 1.
- 1 risk is not rated yet, so it is missing from the heat map and the priority order.

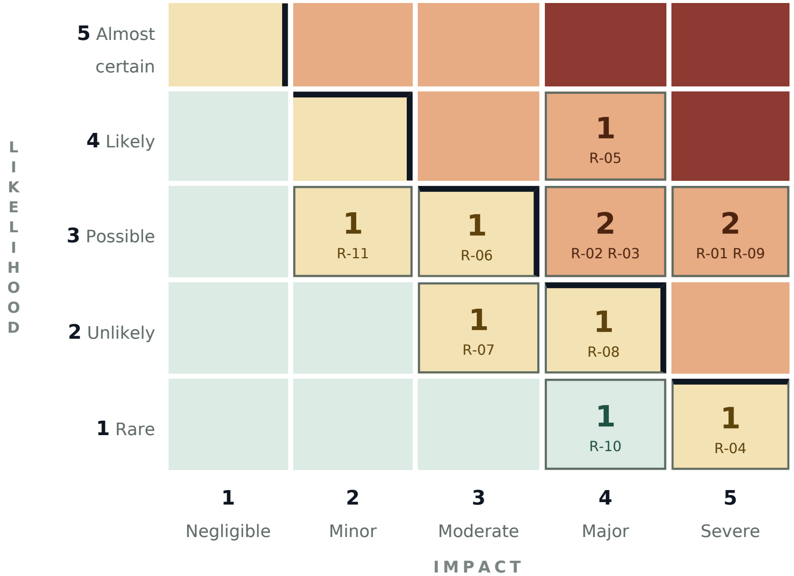
DO THESE FIRST

	SEVERITY	ACTION	RISKS	OWNER	DOCUMENT THAT CLOSES IT
1	CRITICAL	**Above the appetite line with no treatment decision** Choose modify, avoid, share or retain for each one, with the risk owner.	R-05	Business Continuity Manager	Risk treatment plan
2	MAJOR	**Not yet rated for likelihood and impact** Rate each one against the likelihood and impact scales in your criteria.	R-12	Head of Finance	Risk assessment and treatment methodology

Heat maps: today and after treatment

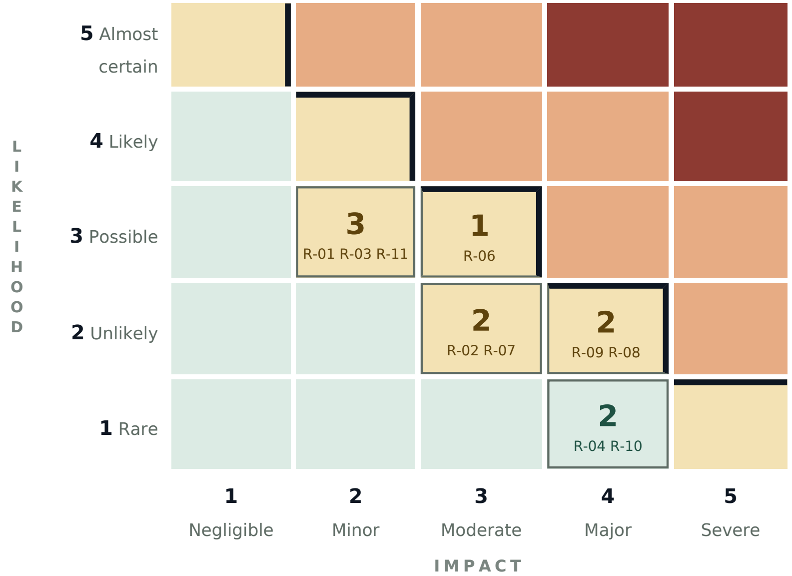
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

Current risk levels



11 of 12 risks rated.

Target levels after treatment



10 risks plotted; 0 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

RISKS BY LEVEL

1 Low	5 Medium	5 High	1 Not rated

Analysis and priorities

IN ONE SENTENCE

Your continuity risks are well understood; decide how to treat untested recovery arrangements, the highest risk in the register, first.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our business continuity risk assessment is largely complete: 12 risks of disruption identified, 5 above our appetite line, and treatment planned that brings that number to 1. One decision is outstanding. Our recovery arrangements have never been tested, and that risk has no treatment decision. We need agreement to exercise the plan this quarter; with that recorded, the assessment is ready for management review.

WHERE YOU STAND

You have identified 12 risks of disruption across 12 scope items, and 11 are rated. Your process score is 91 out of 100, but the level is held at Developing because the highest risk, recovery arrangements never tested, sits above your appetite line with no treatment decision. Every scope item has at least one risk, and every treated risk has a target, an owner and a due date.

WHAT IT MEANS FOR THE ORGANIZATION

5 risks sit above your appetite line, all of them High, and they cluster around the few things production cannot run without: power for refrigeration, the order system, a single supplier of chilled chicken and backups that would not survive ransomware. Because chilled stock is lost within hours, any of these would quickly become missed retailer deliveries. Your planned treatment brings the number above the line from 5 to 1.

WHERE TO FOCUS FIRST

Decide how to treat untested recovery arrangements first: an exercise is the cheapest way to find out whether the other treatments will work when they are needed. Then close the gaps in the register: rate the cash risk, give the emergency contacts risk an owner, and collect the owner's acceptance for the ransomware treatment.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Decide how to test the recovery arrangements** R-05 Recovery arrangements never tested · Above the appetite line with no treatment decision	This is the highest risk in the register and has no decision, which leaves the treatment plan incomplete and holds the level at Developing.	Agree a tabletop exercise date with the Business Continuity Manager and record modify as the decision.	Risk treatment plan	30 DAYS
2	**Rate the cash risk during a long disruption** R-12 Cash runs short during a prolonged disruption · Not yet rated for likelihood and impact	An unrated risk has no level, so it is missing from the heat map and cannot be compared with the appetite line.	Rate likelihood and impact with the Head of Finance, using the outage lengths from your impact analysis.	Risk assessment and treatment methodology	30 DAYS
3	**Name an owner for emergency contacts** R-11 Staff cannot be contacted in an emergency · Risk with no owner	Every risk of disruption needs an owner, or nobody will build the out-of-hours call tree it depends on.	Assign the risk to the HR Manager and set a date for the call tree.	Risk assessment and treatment methodology	30 DAYS
4	**Record acceptance for the ransomware treatment** R-09 Ransomware halts IT systems · Residual risk not yet accepted by the owner	The treatment is planned but its owner has not accepted the risk that remains; a name and a date is enough.	Ask the IT Manager to approve the backup plan and record the acceptance.	Risk treatment plan	60 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Record a treatment decision for untested recovery arrangements.
- Rate the cash risk during a prolonged disruption.
- Assign an owner to emergency contacts.

DAYS 31 TO 60

- Run a tabletop exercise of the continuity plan.
- Collect residual-risk acceptance for the ransomware treatment.
- Complete the manual order process for an ERP outage.

DAYS 61 TO 90

- Update the business continuity strategy with the chosen measures.
- Present the updated register and treatment plan at management review.

What was in scope

The prioritized activity, premises, IT system or service, supplier or partner, key people or teams and vital records the assessment covered, with their owners. How critical this item is to your prioritized activities. Import it from your business impact analysis to set it for you. H high, M medium, L low.

Type	Scope item	Owner	Criticality	Risks
Prioritized activity	**Production**	Operations Manager	H	4
Prioritized activity	**Customer order intake**	Commercial Manager	H	1
Prioritized activity	**Dispatch and delivery**	Logistics Manager	H	2
Prioritized activity	**Payroll**	Head of Finance	M	1
Premises	**Production site**	Facilities Manager	H	2
Premises	**Distribution centre**	Logistics Manager	H	1
IT system or service	**ERP and order management system**	IT Manager	H	2
IT system or service	**Refrigeration control system**	Engineering Manager	H	2
Supplier or partner	**Key raw material supplier**	Procurement Manager	H	1
Supplier or partner	**Courier network**	Logistics Manager	M	1
Key people or teams	**Operations team**	Operations Manager	H	3
Vital records	**Customer and order records**	IT Manager	M	1

Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

#	Ref	Risk scenario	Scope items	Resources lost	Owner	Existing controls	L	I	Level	Rationale
1	R-05	**Recovery arrangements never tested** Weakness: No exercise programme; backups and standby systems not restored in a test	Production, Dispatch and delivery	Technology, Information	Business Continuity Manager	Plan written in 2024	4	4	16 · High	The plan has never been exercised; contact details are out of date.
2	R-01	**Prolonged power or utility failure** Weakness: No backup power, or backup that has never been tested under load	Production site, Refrigeration control system, Production	Premises, Technology	Facilities Manager	Single grid supply; no generator	3	5	15 · High	Chilled stock is lost after four hours without power; two outages last winter.
3	R-09	**Ransomware halts IT systems** Weakness: No offline backup and no rehearsed recovery; no manual fallback	ERP and order management system, Customer and order records	Technology, Information	IT Manager	Endpoint protection; backups on the same network	3	5	15 · High	Backups are reachable from the office network.
4	R-02	**A single-source dependency with no alternative** Weakness: Nobody has looked for alternatives or held extra stock	Key raw material supplier, Production	Suppliers	Procurement Manager	Two weeks of packaging stock	3	4	12 · High	One supplier provides all chilled chicken; no approved alternative.
5	R-03	**Critical IT system outage** Weakness: No standby environment and no workaround for the activities that use it	ERP and order management system, Customer order intake	Technology	IT Manager	Nightly backup of the ERP	3	4	12 · High	Orders arrive by EDI; a day without the ERP means missed retailer slots.
6	R-06	**Loss of a key person with unique knowledge** Weakness: Knowledge not written down; no trained deputy	Operations team, Refrigeration control system	People	Operations Manager		3	3	9 · Medium	Only the engineering lead can reset the refrigeration controls.

7	R-08	**Widespread staff illness or a pandemic** Weakness: No remote working, cover or minimum staffing plan for critical activities	Operations team, Production	People	HR Manager	Pandemic plan from 2020	2	4	**8 · Medium**	Production cannot run below 70% staffing.
8	R-07	**Logistics or courier partner cannot deliver** Weakness: One carrier for all deliveries	Courier network, Dispatch and delivery	Suppliers	Logistics Manager	Two couriers on contract	2	3	**6 · Medium**	Second courier can take about 60% of volume.
9	R-11	**Staff cannot be contacted in an emergency** Weakness: Contact lists out of date and held only on company systems	Operations team	People	**None**	Staff list in the HR system	3	2	**6 · Medium**	No out-of-hours call tree.
10	R-04	**Fire destroys or closes a site** Weakness: No alternate location; vital records and equipment only on that site	Production site	Premises, Technology, Information	Facilities Manager	Sprinklers; annual fire risk assessment	1	5	**5 · Medium**	Sprinklered site; but no alternative production capacity.
11	R-10	**Flooding or water damage at a site** Weakness: Equipment and stock at floor level; no water detection	Distribution centre	Premises, Technology	Facilities Manager	Site outside the flood zone	1	4	**4 · Low**	Low-lying loading bay flooded once in 2019.
12	R-12	**Cash runs short during a prolonged disruption** Weakness: No business interruption cover and no emergency funding line	Payroll	Finance	Head of Finance		–	–	**Not rated**	

What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The continuity measures listed are the ones the treatment relies on; they carry into the business continuity strategy. Acceptance is the risk owner's approval of the plan and of the risk that remains.

Ref	Risk	Decision	Planned actions	Continuity measures	Owner and due date	Current to target	Accepted
R-03	**Critical IT system outage** IT Manager	**Modify**	A documented manual order process and a tested ERP restore within eight hours.	BC.6 IT disaster recovery plan and standby environment BC.10 Manual workarounds for critical activities	IT Manager 15 Dec 2026	12 · High → 6 · Medium	Managing Director 22 Sep 2026
R-09	**Ransomware halts IT systems** IT Manager	**Modify**	Offline, immutable backups and a tested restore of the ERP.	BC.7 Backups with regularly tested restores BC.6 IT disaster recovery plan and standby environment	IT Manager 31 Dec 2026	15 · High → 8 · Medium	**Not recorded**
R-02	**A single-source dependency with no alternative** Procurement Manager	**Modify**	Qualify a second supplier and agree a call-off contract.	BC.11 Alternative or dual-sourced suppliers BC.13 Buffer stock of critical materials	Procurement Manager 31 Jan 2027	12 · High → 6 · Medium	Managing Director 22 Sep 2026
R-01	**Prolonged power or utility failure** Facilities Manager	**Modify**	Install a standby generator for refrigeration and a fuel supply contract.	BC.9 Uninterruptible power supply and generator BC.25 Environmental monitoring and fire, flood and temperature detection	Facilities Manager 28 Feb 2027	15 · High → 6 · Medium	Managing Director 22 Sep 2026
R-04	**Fire destroys or closes a site** Facilities Manager	**Share**	Review business interruption cover and agree co-packing capacity with a partner.	BC.14 Business interruption insurance BC.1 Alternate site or work location	Head of Finance 31 Mar 2027	5 · Medium → 4 · Low	Managing Director 22 Sep 2026

R-06	**Loss of a key person with unique knowledge** Operations Manager	**Retain**	Risk retained at its current level.	–	9 · Medium → 9 · Medium	**Not recorded**

ABOVE THE LINE WITH NO DECISION YET

Ref	Risk	Owner	Level
R-05	**Recovery arrangements never tested**	Business Continuity Manager	16 · High

4 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

Where the assessment falls short

Each finding is a gap between the assessment as recorded and what ISO 22301 clause 8.2.3 ask for, with the risks it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
CRITICAL	**Above the appetite line with no treatment decision**	R-05	These risks are rated above Medium, the highest level you accept without treatment, but nobody has decided what to do about them. ISO 22301 expects a treatment option to be chosen for every risk that fails the acceptance criteria.	Choose modify, avoid, share or retain for each one, with the risk owner.	Risk treatment plan
MAJOR	**Not yet rated for likelihood and impact**	R-12	Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order.	Rate each one against the likelihood and impact scales in your criteria.	Risk assessment and treatment methodology
MAJOR	**Risk with no owner**	R-11	Every risk of disruption needs an owner with the accountability and authority to manage it, or the continuity strategy chosen for it has nobody to deliver it.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MINOR	**Residual risk not yet accepted by the owner**	R-09	The risk owner should approve the continuity measures and accept the risk of disruption that remains. A name and a date is enough to show it happened.	Record the owner's acceptance once they have approved the plan.	Risk treatment plan

PROCESS SCORE IN DETAIL

Criteria defined Every likelihood and impact level has a definition, and the appetite line is set.	**100%**	11 of 11	weight 10
Scope covered Every scope item has at least one risk linked to it.	**100%**	12 of 12	weight 10
Risk owners named Every risk has an owner accountable for it.	**92%**	11 of 12	weight 15
Risks rated Every risk has a likelihood and an impact, so it has a level.	**92%**	11 of 12	weight 15
Ratings explained Existing controls and a rationale are recorded for each risk.	**88%**	21 of 24	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.	**80%**	4 of 5	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.	**100%**	4 of 4	weight 10
Treatments scheduled Each treatment has an owner and a due date.	**100%**	4 of 4	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.	**75%**	3 of 4	weight 10

Findings by severity

1 · Initial (0+)
A start on a register, not yet an assessment that decisions can rest on.

2 · Developing (40+)
The risks are identified, but gaps in rating or treatment would not survive an audit.

3 · Defined (60+)
A complete, repeatable assessment with a treatment plan behind it.

4 · Managed (80+)
Owned, justified and accepted: ready for management review and audit.

Criteria used and basis of this report

ISO 22301 clause 8.2.3 asks the organization to identify, analyse and evaluate the risks of disruption to its prioritized activities, against criteria it has set, and to decide which need treatment. This is the record of the criteria every rating in this report was made against.

LIKELIHOOD SCALE

Value	Label	Definition
1	**Rare**	Not expected in the next 5 years; no known case here or in the sector
2	**Unlikely**	Could happen once in 2 to 5 years; has happened in the sector
3	**Possible**	Could happen about once a year
4	**Likely**	Expected several times a year
5	**Almost certain**	Expected monthly or more often, or already happening

IMPACT SCALE

Value	Label	Definition
1	**Negligible**	Disruption within recovery objectives; nobody outside notices
2	**Minor**	A critical activity down close to its recovery time objective; 10,000 to 50,000
3	**Moderate**	Recovery objectives missed; customers affected; 50,000 to 250,000
4	**Major**	Maximum tolerable disruption approached; contracts and regulator affected; 250,000 to 1 million
5	**Severe**	Maximum tolerable disruption exceeded; lasting loss of customers or licence; over 1 million

RISK LEVELS AND ACCEPTANCE

Band	Levels	Treatment
Low	1–4	Accepted without treatment
Medium	5–9	Accepted without treatment
High	10–16	Needs a treatment decision
Critical	17–25	Needs a treatment decision

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

Process score. Nine dimensions, each the share of risks (or of risks above the line) that meet it, multiplied by its weight; the weights add up to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

Your workbook. The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a list of the continuity measures your treatments rely on.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.