GOVERNANCE DOCS

Enterprise Risk Assessment

Aldgate Engineering Group (sample)

The group's strategic plan, its three operating divisions and the major projects in the current three-year plan.

ASSESSED	25 September 2026
METHOD	ISO 31000:2018, clauses 6.4 (risk assessment) and 6.5 (risk treatment)
IN SCOPE	11 scope items, 12 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PROFILE	Manufacturing and industrial · 250 to 999 people
PREPARED BY	Governance Docs

CONTENTS

Where the organization's risks stand

PROCESS SCORE

90 / 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	4	0	1	4

WHAT THIS ASSESSMENT TELLS YOU

- 4 of 11 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, too much revenue depends on a few customers, at level 16 (High), owned by Commercial Director.
- 1 risk above the line has no treatment decision yet (R-04). Until it has one, the treatment plan is incomplete.
- Planned treatment brings the number of risks above the line from 4 to 1.
- 1 risk is not rated yet, so it is missing from the heat map and the priority order.

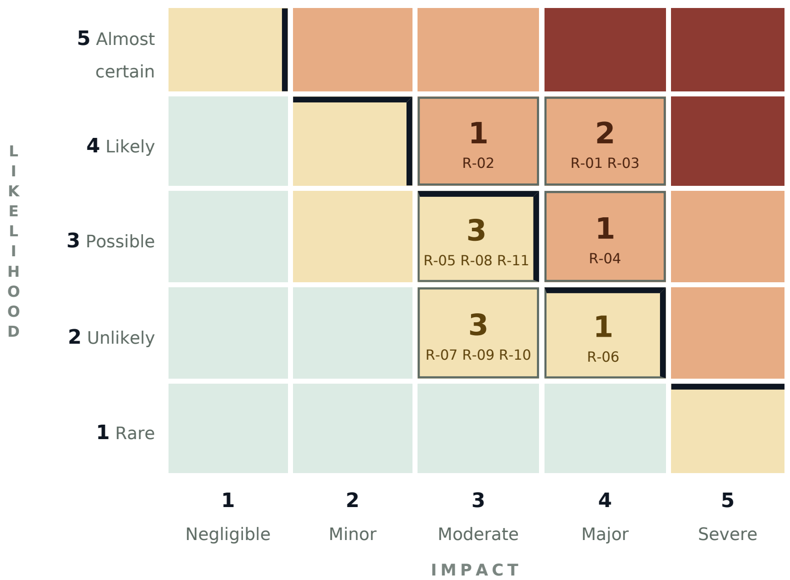
DO THESE FIRST

	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-04	Chief Executive	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	Chief Executive	Risk assessment and treatment methodology

Heat maps: today and after treatment

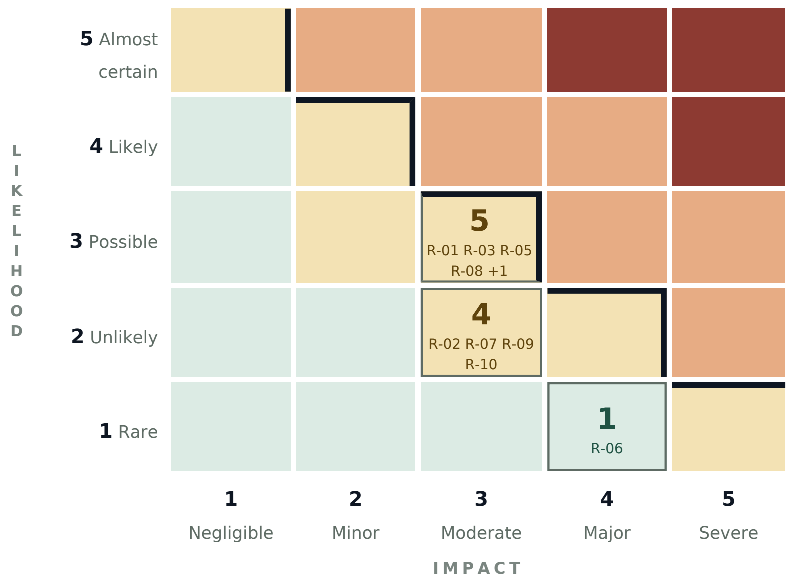
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

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

Analysis and priorities

IN ONE SENTENCE

Your enterprise risks are well mapped; decide how to treat the acquisition integration risk and confirm the margin plan's acceptance next.

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 enterprise risk assessment is largely complete: 12 risks identified, 4 above our appetite, and treatment planned that brings that number to 1. One decision is outstanding. We need a treatment decision on the acquisition integration, whose synergy targets depend on moving the acquired site onto group systems. With that decision recorded, the assessment is ready for board review.

WHERE YOU STAND

You have identified 12 enterprise risks across 11 scope items, and 11 are rated. Your process score is 90 out of 100, but the level is held at Developing because one risk above your appetite line, the acquisition failing to deliver value, has no treatment decision. Every objective, unit and project in scope has at least one risk, and every treated risk has a target, an owner and a due date.

WHAT IT MEANS FOR THE ORGANIZATION

4 risks sit above your appetite line, all of them High, and three of them bear directly on the operating margin: customer concentration, input cost inflation and an overrunning ERP project. Together they describe a plan that depends on a small number of customers paying prices that no longer cover costs, while a major investment runs over budget. Your planned treatment brings the number above the line from 4 to 1.

WHERE TO FOCUS FIRST

Decide how to treat the acquisition integration risk first, because it is what holds the level back and its synergy targets are part of the growth plan. Then close the gaps in the register: rate the reputational risk, give the IT failure risk an owner, and record the Chief Financial Officer's acceptance of the cost inflation treatment.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Decide how to treat the acquisition integration risk** R-04 An acquisition or partnership fails to deliver value · Above the appetite line with no treatment decision	This High risk sits above your appetite with no decision, which leaves the treatment plan incomplete and holds the level at Developing.	Agree a treatment with the Chief Executive, such as a tracked synergy plan with milestones, and record it.	Risk treatment plan	30 DAYS
2	**Rate the reputational risk** R-12 Reputational damage from media or social media · 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 your appetite.	Rate likelihood and impact against your criteria, with a sentence of rationale.	Risk assessment and treatment methodology	30 DAYS
3	**Name an owner for the IT failure risk** R-11 Major IT failure or cyber incident · Risk with no owner	ISO 31000 expects accountability for each risk to be assigned, and the legacy ERP is out of vendor support.	Assign the risk to the IT Director and review it with the ERP programme.	Risk assessment and treatment methodology	30 DAYS
4	**Record acceptance for the cost inflation plan** R-03 Input costs rise faster than prices · Residual risk not yet accepted by the owner	The indexation and hedging plan is in place but its owner has not accepted the risk that remains.	Ask the Chief Financial Officer to approve the plan and record the acceptance.	Risk treatment plan	60 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Record a treatment decision for the acquisition integration risk.
- Rate the reputational risk.
- Assign an owner to the IT failure risk.

DAYS 31 TO 60

- Collect residual-risk acceptance for input cost inflation.
- Commission the independent assurance review of the ERP project.
- Set new-account sales targets under the diversification plan.

DAYS 61 TO 90

- Update the risk treatment plan with the chosen control measures.
- Present the updated register and appetite to the board.

What was in scope

The objective, business unit or function, process, project or initiative, supplier or partner and key asset the assessment covered, with their owners.

Type	Scope item	Owner	Risks
Objective	**Revenue growth target**	Chief Executive	2
Objective	**Operating margin**	Chief Financial Officer	1
Objective	**New market entry**	Commercial Director	2
Business unit or function	**Operations**	Chief Operating Officer	3
Business unit or function	**Finance**	Chief Financial Officer	1
Process	**Order to cash**	Chief Financial Officer	2
Project or initiative	**ERP replacement**	Project Director	1
Project or initiative	**Acquisition integration**	Chief Executive	1
Supplier or partner	**Key raw material supplier**	Chief Operating Officer	1
Key asset	**Top ten customers**	Commercial Director	1
Key asset	**Key staff**	HR Director	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	Category	Owner	Existing controls	L	I	Level	Rationale
1	R-01	**Too much revenue depends on a few customers** Weakness: A handful of customers make up most of the revenue	Top ten customers, Revenue growth target	Financial, Strategic	Commercial Director	Account plans for the top five	4	4	16 · High	Two customers provide 41% of revenue; one is reviewing suppliers.
2	R-03	**Input costs rise faster than prices** Weakness: Fixed-price contracts with no indexation; no cost monitoring	Operating margin, Key raw material supplier	Financial	Chief Operating Officer	Annual price reviews	4	4	16 · High	Steel costs rose 22% in eighteen months; contracts have no price adjustment clause.
3	R-04	**An acquisition or partnership fails to deliver value** Weakness: Limited due diligence and no integration plan	Acquisition integration	Strategic, Financial	Chief Executive	Integration plan	3	4	12 · High	Synergy targets depend on moving the acquired site onto group systems.
4	R-02	**A major project runs over budget or late** Weakness: No stage gates, contingency or independent review	ERP replacement	Operational, Financial	Project Director	Monthly steering committee	4	3	12 · High	The ERP project is 18% over budget at the design stage.
5	R-05	**Loss of key people or skills** Weakness: No succession planning; knowledge held by a few	Key staff, Operations	Operational, Strategic	HR Director	Retention bonuses for four engineers	3	3	9 · Medium	Specialist welding skills held by a small, ageing team.
6	R-08	**Demand falls as the market or customer needs change** Weakness: Little market insight; the offer has not changed in years	Revenue growth target, New market entry	Strategic, Financial	Commercial Director	Annual strategy review	3	3	9 · Medium	Customers moving to lighter composite parts.

7	R-11	**Major IT failure or cyber incident** Weakness: Under-invested IT; no tested recovery plan	Operations	Operational, Reputational	**None**	Group IT security programme	3	3	**9 · Medium**	Legacy ERP out of vendor support until the replacement goes live.
8	R-06	**Workplace injury or ill health** Weakness: Risk assessments and safety training not kept up to date	Operations	Health and safety, Legal and compliance	Health and Safety Lead	ISO 45001 system; monthly inspections	2	4	**8 · Medium**	Two reportable incidents last year, both in the fabrication shop.
9	R-07	**Customers fail to pay what they owe** Weakness: No credit checks or limits; slow collection	Order to cash	Financial	Chief Financial Officer	Credit limits; credit insurance on export sales	2	3	**6 · Medium**	Debtor days stable at 52.
10	R-09	**New regulation raises costs or restricts activities** Weakness: Regulatory developments not tracked	New market entry	Legal and compliance, Strategic	Head of Compliance	Trade association briefings	2	3	**6 · Medium**	Carbon reporting rules will apply from 2027.
11	R-10	**Internal or external fraud** Weakness: Weak segregation of duties and approval limits; no reconciliations	Order to cash, Finance	Financial, Reputational	Chief Financial Officer	Two-person approval for payments	2	3	**6 · Medium**	One attempted supplier bank detail fraud last year, stopped.
12	R-12	**Reputational damage from media or social media** Weakness: No crisis communications plan or social media monitoring	**None linked**	Reputational	Chief Executive		–	–	**Not rated**	

What will be done, by whom and by when

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

Ref	Risk	Decision	Planned actions	Control measures	Owner and due date	Current to target	Accepted
R-06	**Workplace injury or ill health** Health and Safety Lead	**Modify**	Machine guarding upgrade in fabrication.	ER.17 Health and safety controls	Chief Operating Officer 30 Nov 2026	8 · Medium → 4 · Low	Chief Executive 22 Sep 2026
R-02	**A major project runs over budget or late** Project Director	**Modify**	Independent assurance review and stage-gated funding.	ER.15 Project governance and stage gates ER.14 Independent assurance or internal audit	Project Director 31 Dec 2026	12 · High → 6 · Medium	Chief Financial Officer 22 Sep 2026
R-03	**Input costs rise faster than prices** Chief Operating Officer	**Modify**	Add indexation clauses to new customer contracts and hedge part of the steel requirement.	ER.7 Contractual protection ER.9 Hedging or financial instruments	Chief Financial Officer 31 Jan 2027	16 · High → 9 · Medium	**Not recorded**
R-01	**Too much revenue depends on a few customers** Commercial Director	**Modify**	Diversification plan with sales targets for new accounts and multi-year agreements with the top two.	ER.10 Diversification ER.5 Monitoring, KPIs and key risk indicators	Commercial Director 31 Mar 2027	16 · High → 9 · Medium	Chief Executive 22 Sep 2026
R-05	**Loss of key people or skills** HR Director	**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-04	**An acquisition or partnership fails to deliver value**	Chief Executive	12 · High

5 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 31000 clauses 6.4 and 6.5 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-04	These risks are rated above Medium, the highest level you accept without treatment, but nobody has decided what to do about them. ISO 31000 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	ISO 31000 expects accountability and authority for managing each risk to be assigned: a named risk owner, by role.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MINOR	**Residual risk not yet accepted by the owner**	R-03	ISO 31000 clause 6.5.3 expects decision makers to be aware of the risk that remains after treatment. The owner's 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%	11 of 11	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.	92%	22 of 24	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.	75%	3 of 4	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.	100%	3 of 3	weight 10
Treatments scheduled Each treatment has an owner and a due date.	100%	3 of 3	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.	67%	2 of 3	weight 10

Findings by severity

1 | 2 | 1

Critical Major Minor

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 31000 clause 6.3.4 asks the organization to define its risk criteria, including the amount and type of risk it may or may not take, so that every risk is evaluated against the same yardstick. 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**	Under 10,000; absorbed within budgets; no stakeholder impact
2	**Minor**	10,000 to 50,000; minor delay to an objective; internal attention
3	**Moderate**	50,000 to 250,000; an objective at risk; limited external attention
4	**Major**	250,000 to 1 million; a strategic objective missed; board, regulator or media attention
5	**Severe**	Over 1 million; strategy or solvency threatened; sanctions or lasting reputational damage

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 control 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.