Northbridge Logistics

Executive summary

Scope: All applications (3)
Period: All recorded dates
Generated 2026-10-23 06:22 UTC by Elena Marsh
The risk score, exposure and unresolved counts are as of the time generated. The period applies to findings recorded, tasks completed and decisions made.

Risk

As of the time generated

Figure	Value	How it is worked out
Company risk score	81 (Critical)	The company score is its highest application score: Fleet Tracking Service, 81. Worst unresolved finding: “Exposed administrator credentials in source code” (critical). 4 unresolved findings. The worst is critical, so the score starts at 75; +4 for each of 1 further critical finding (4), +2 for each of 0 one level lower (0), +1 for each of 2 lower still (2). Score 81.
Unresolved findings	10 (4 critical, 2 high, 2 medium, 2 low)	Open or in progress. Resolved, accepted-risk and won't-fix findings are not counted here.
Resolved findings	0	Of 10 recorded.
Findings recorded in the period	10	All recorded dates

Financial exposure

As of the time generated

Figure	Value	How it is worked out
Estimated exposure (one incident per application)	$9.6M	Fleet Tracking Service: $2,232,000. Worst unresolved finding: “Exposed administrator credentials in source code” (critical). Outage assumed for a critical finding: 72 hours (planning assumption: Critical 72, High 24, Medium 8, Low 2). Cost of an hour of downtime: $3,500, the figure entered for this application. Business interruption = 72 × $3,500 = $252,000. Data breach response = 12,000 data records × US$165 per record = $1,980,000. Source for the per-record figure: IBM Cost of a Data Breach Report 2023: US$165 per record, global average. Total $2,232,000. Customer Billing Portal: $3,618,000. Worst unresolved finding: “SQL injection in billing API” (critical). Outage assumed for a critical finding: 72 hours (planning assumption: Critical 72, High 24, Medium 8, Low 2). Cost of an hour of downtime: $9,000, the figure entered for this application. Business interruption = 72 × $9,000 = $648,000. Data breach response = 18,000 data records × US$165 per record = $2,970,000. Source for the per-record figure: IBM Cost of a Data Breach Report 2023: US$165 per record, global average. Total $3,618,000. Invoice Document Storage: $3,738,000. Worst unresolved finding: “Public storage bucket with customer files” (critical). Outage assumed for a critical finding: 72 hours (planning assumption: Critical 72, High 24, Medium 8, Low 2). Cost of an hour of downtime: $1,500, the figure entered for this application. Business interruption = 72 × $1,500 = $108,000. Data breach response = 22,000 data records × US$165 per record = $3,630,000. Source for the per-record figure: IBM Cost of a Data Breach Report 2023: US$165 per record, global average. Total $3,738,000. Company total $9,588,000: each application counted once.
Covered by recorded insurance	$4M	Cover recorded across 3 applications: $4,000,000. Fleet Tracking Service: exposure $2,232,000, cover $1,000,000, deductible $25,000 -> covered $1,000,000, uncovered $1,232,000. Customer Billing Portal: exposure $3,618,000, cover $2,000,000, deductible $50,000 -> covered $2,000,000, uncovered $1,618,000. Invoice Document Storage: exposure $3,738,000, cover $1,000,000, deductible $25,000 -> covered $1,000,000, uncovered $2,738,000. Per application: covered = the smaller of its cover and (its exposure - its deductible). Uncovered = exposure - covered. The company figures are the sums.
Not covered	$5.6M	Exposure minus what recorded cover would pay, per application.
Not included	Likelihood, reputation damage, customer churn, regulatory fines, cost to fix	The product holds no data to base them on.

Risks carried by decision

As of the time generated

Figure	Value	How it is worked out
Findings closed as accepted risk or won't fix	0	Not fixed, and not counted as unresolved or as resolved.

Remediation progress

Now, and in the period where a line says so

Figure	Value	How it is worked out
Tasks open / in progress / in review	8 / 2 / 0	As of the time generated.
Overdue tasks	1	Open work past its due date.
Unresolved findings without a task	0	Overdue is shown as two numbers: tasks past their due date, and unresolved findings past their SLA date that have no task. A finding with an open task is counted through its task only. Deadline targets: critical 7 days, high 30, medium 60, low 90, counted from the date a finding was recorded.
Tasks completed in the	0	All recorded dates. A task counts as completed, and as meeting or missing its deadline, only when a

Figure	Value	How it is worked out
period		person started it (moved the task to in progress or in review) and then completed it. A task closed because its finding was resolved directly is shown as "closed without recorded work" and is not credited as a completion.
Deadlines met / missed	No worked task with a deadline was completed in this period	Worked tasks with a due date: completed on or before it, or after it.
Mean time to remediate	Not enough completed fixes yet (0 of 5)	Counts remediation tasks that a person started (moved to in progress or in review) and then completed, from task creation to completion. Findings resolved directly without a worked task, and accepted-risk or won't-fix closures, are not counted. Shown once five fixes qualify.

Top risks

As of the time generated. The ten most severe unresolved findings, by severity then CVSS.

Finding	Application	Severity	CVSS	Status	Recorded
SQL injection in billing API	Customer Billing Portal	Critical	9.8	In progress	2026-10-23
Exposed administrator credentials in source code	Fleet Tracking Service	Critical	9.1	In progress	2026-10-23
Public storage bucket with customer files	Invoice Document Storage	Critical	9.1	Open	2026-10-23
Privilege escalation via host misconfiguration	Fleet Tracking Service	Critical	9	Open	2026-10-23
Stored cross-site scripting in customer profile	Customer Billing Portal	High	7.6	Open	2026-10-23
Weak TLS configuration	Customer Billing Portal	High	7.5	Open	2026-10-23
Insecure direct object reference on invoice documents	Customer Billing Portal	Medium	6.5	Open	2026-10-23
Sensitive data written to application logs	Fleet Tracking Service	Medium	5.5	Open	2026-10-23
Software version disclosure	Customer Billing Portal	Low	3.7	Open	2026-10-23
Outdated JavaScript library with a known vulnerability	Fleet Tracking Service	Low	3.1	Open	2026-10-23

Applications

As of the time generated

Application	Risk score	Band	Unresolved	Critical	High	Exposure	Insurance
Fleet Tracking Service	81	Critical	4	2	0	$2.2M	Exceeds what the $1M cover would pay by $1.2M (55% uncovered, including the $25K deductible).
Customer Billing Portal	81	Critical	5	1	2	$3.6M	Exceeds what the $2M cover would pay by $1.6M (45% uncovered, including the $50K deductible).
Invoice Document Storage	75	Critical	1	1	0	$3.7M	Exceeds what the $1M cover would pay by $2.7M (73% uncovered, including the $25K deductible).

Exposure figures are estimates from your own recorded figures and stated assumptions, not measured loss data. Likelihood, reputation, churn and fines are not modelled.