KASEWARE

Security Impact Summary

Use this format to brief executive leadership on security value, not just activity.

Reporting Period:
Month, quarter, or event period

Top Risk Areas:
List the highest-priority risks affecting assets, operations, compliance, or public safety.

Actions Taken:
Summarize the key actions the team took to assess, reduce, contain, or escalate risk.

Current Gaps or Constraints:
Note any resource, technology, staffing, data, or process limits that still affect risk.

Recommended Next Step:
State the decision or investment needed, tied to risk and business impact.

Business Outcomes:
Connect each action to a measurable result.

Risk Reduction:
What exposure decreased? What threat, asset, or compliance risk improved?

Faster Response:
How did response time, containment time, or escalation time improve?

Operational Efficiency:
What manual work, tool switching, or duplicate effort decreased?

Decision Confidence:
What clearer data, reporting, or leadership visibility improved?

Metrics to Highlight:
Insert only metrics the team can support with internal data.

High-risk incidents reduced by:	X%
Average response time changed from:	X to Y
Open risks reduced from:	X to Y
Manual reporting time reduced by:	X hours
Tools or workflows consolidated:	X
Leadership briefings completed within target time:	X%

Executive Takeaway:
One or two sentences that explain what changed, why it matters, and what leadership should do next.