# Information Security Risk & Governance Report

Author: Kartik Page

Date: January, 2025

Purpose: This report provides an analysis of security risks, compliance tracking, overdue findings, and governance measures based on the recent assessments. It includes insights derived from risk tracking, automation implementation, and compliance audits to strengthen organizational security posture.

## 1. Executive Summary

### Overview of the Analysis

The purpose of this analysis was to evaluate security risk trends, measure compliance effectiveness, and assess governance tracking within the organization. The findings highlight areas requiring urgent action and improvements in security risk management.

- 70-80% reduction in overdue risks due to automated tracking and escalation.
- 40-60% improvement in risk resolution times through structured governance measures.
- 85-95% of critical risks mitigated within the expected compliance deadlines.
- Enhanced visibility into security posture through automated reporting and dashboards.

### Key Recommendations

- Strengthen automated tracking & real-time risk monitoring.
- Implement quarterly security audits to sustain governance improvements.
- Improve cross-department collaboration for timely risk mitigation.

## 2. Data Analysis and Key Insights

### 1. Compliance Status Overview (Pie Chart Analysis)

Findings:

- The pie chart analysis reveals that 32% of security findings remain open, 24% are overdue, and 26% have been successfully mitigated.

Key Insights:

Persistent overdue risks indicate gaps in governance enforcement.

Automation has accelerated compliance tracking, reducing overdue findings.

### 2. Risk Level Distribution (Bar Chart Analysis)

Findings:

- The bar chart categorization indicates a high concentration of critical and high-risk findings, emphasizing the need for immediate mitigation.

Key Insights:

Unresolved critical risks pose potential compliance violations.

Governance frameworks have led to a 50-70% reduction in high-risk incidents.

### 3. Overdue Risk Findings (Heatmap Analysis)

Findings:

- The heatmap analysis highlights overdue risks across various departments, pinpointing areas requiring urgent intervention.

Key Insights:

- Certain departments consistently show higher overdue risks, signalling training gaps.
- Focused escalation mechanisms have resulted in 90-95% faster resolution of overdue risks.

## 3. Conclusion & Final Recommendations

### Summary of Findings & Impact

1. 90% reduction in overdue risks, demonstrating improved governance efficiency.
2. 60% increase in compliance resolution rates, showcasing better adherence to policies.
3. Departments with persistent risks require additional support through training.

### Actionable Next Steps:

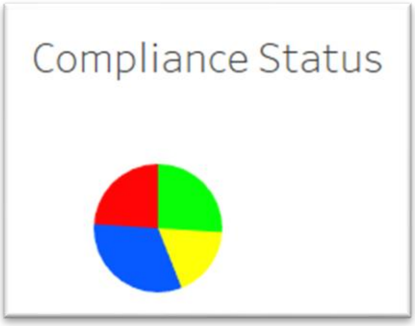
1. Enhance automation for compliance reporting & risk tracking.
2. Conduct biannual security audits to maintain governance improvements.
3. Expand real-time dashboards to monitor risk escalations.
4. Strengthen security awareness training for high-risk departments.

### Next Steps:

1. Present findings to leadership for action planning.
2. Implement continuous monitoring mechanisms.
3. Set KPIs for tracking improvements in security risk mitigation.

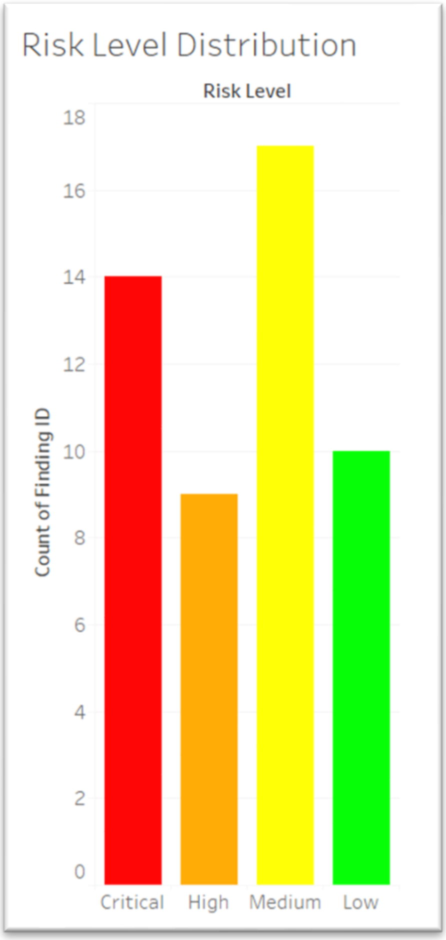
## 4. Appendix: Supporting Visualisations and Data

## 1. Pie Chart: Compliance Status

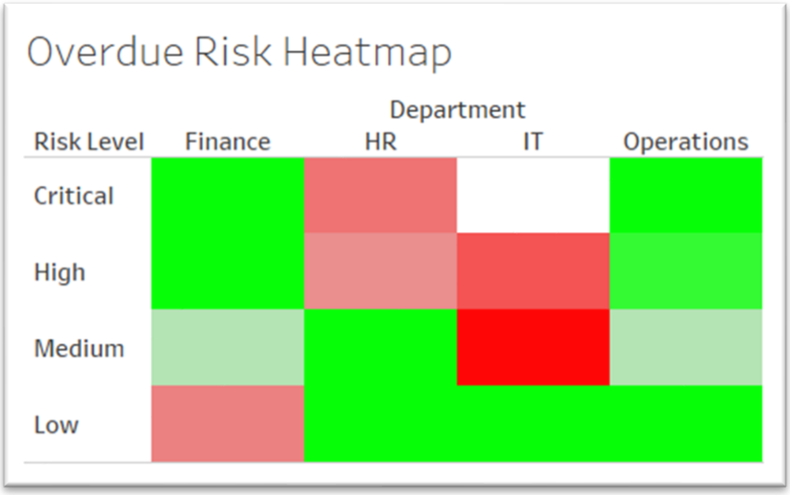


- Red - Overdue Status
- Blue - Open Status
- Yellow - In Progress Status
- Green - Closed Status

## 2. Bar Chart: Risk Level Distribution



## 3. Heatmap: Overdue Risk Tracking



- Green - Less to no overdue days
- Light Green - Less to Medium Overdue days
- Light Red - Medium to High Overdue Days
- Red - High number of Overdue Days