



Group 2 Comparative Analysis

Differentiating Security Governance and Security Management

Case Study: Marriott Data Breach Incident



Introduction: Security Governance vs. Security Management



Security Governance

Strategic framework led by the board and executives

Ensures security matches with business goals

Manages risks, provides oversight and accountability

Answers: "Are we doing the right things?"



Security Management

Tactical execution by CISOs, managers, and security teams

Implements and operates security controls

Protects assets through daily operations

Answers: "Are we doing things right?"





Key Differences

Governance

- Sets strategy, direction, and risk appetite
- Responsible for "Why" decisions
- Determines acceptable risk levels
- Establishes compliance requirements

Management

- Handles implementation, monitoring, and daily operations
- Focuses on "How" actions
- Deploys firewalls and security tools
- Runs vulnerability scans and responds to incidents

Marriott Data Breach Incident



Marriott acquired Starwood in 2016, inheriting compromised IT infrastructure

Attackers had access to Starwood's database since 2014

In 2018, unusual activity was detected, revealing long-term access to sensitive guest data such as names, addresses, passports, and credit cards.

Marriott's Response

- Launched internal investigation
- Notified global regulators
- Informed impacted guests
- Offered free web monitoring and identity protection
- Improved data security measures

This incident highlights the hidden cybersecurity risks in mergers and acquisitions (M&A).



What Went Wrong

Security Governance Gaps

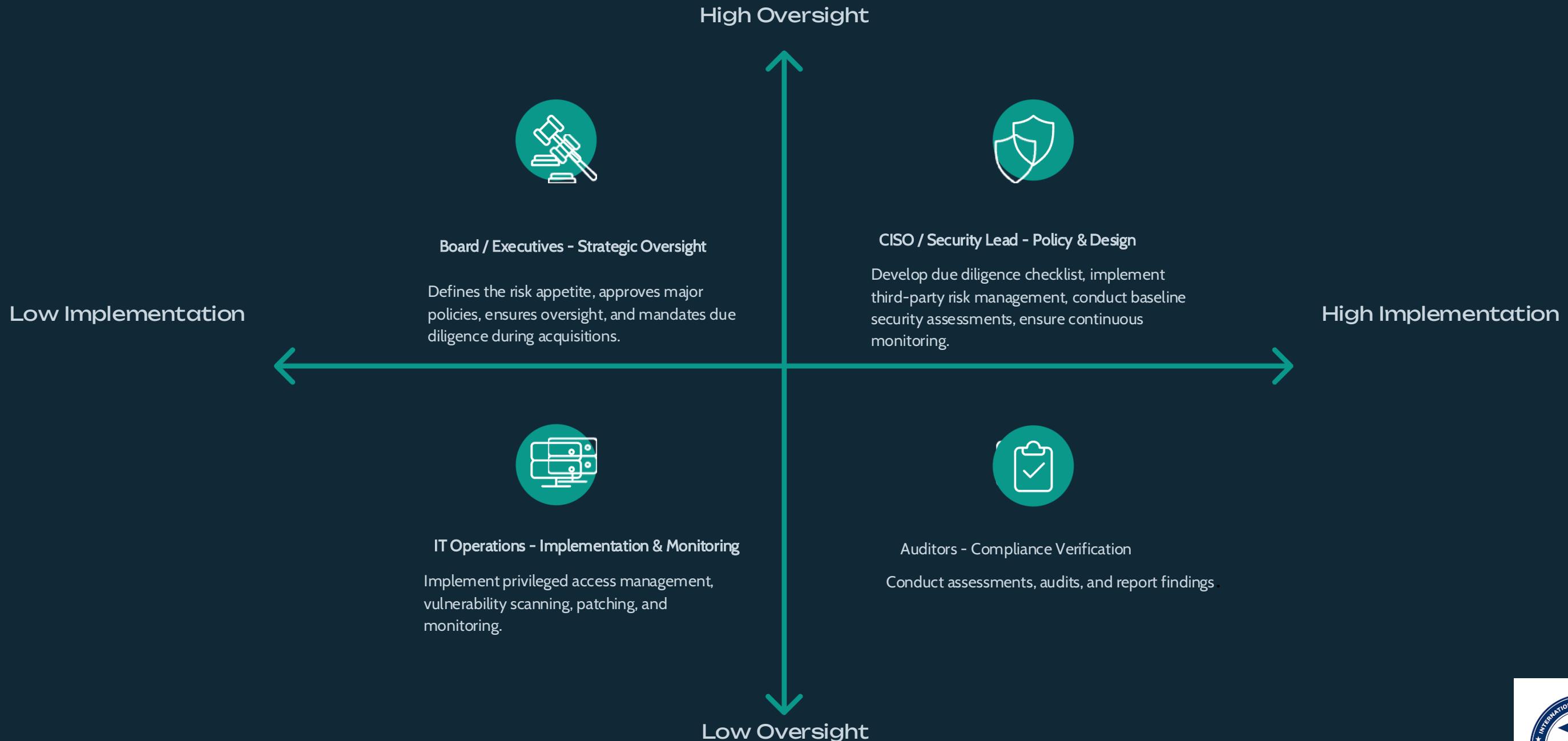
- Risk appetite not defined
- No due diligence or security assessment before M&A
- No policy in place for securing systems (e.g., PCI DSS)
- Lack of training and security awareness
- No continuous monitoring and audit from the Board level
- No clear roadmap or framework for privileged accounts

Security Management Gaps

- No periodic reports after acquisition
- Lack of access controls and privilege access management
- No vulnerability scans, patch management, or penetration testing
- Reactive rather than proactive threat detection
- No continuous monitoring by IT/Security teams
- Uncertain incident escalation paths



Roles and Responsibilities



Other roles not capture within the quadrant are:

- ❖ Compliance Officer
- ❖ Project Manager
- ❖ Risk Management Team
- ❖ Department Heads
- ❖ Employee etc.



RACI Matrix for Marriott-Starwood Breach Responsibilities

Key Activities	Board/ Executives	CISO/Security Lead	IT and Operation Teams	Internal Auditor	External Auditor
Define Risk Appetite	A	C	I	C	I
Cybersecurity Due Diligence	A	R	C	C	R
Approve Security Policies	A	R	C	C	I
M&A Security Integration	I	A/R	R	C	C
Privileged Access Management	I	A/R	R	C	C
Threat Detection	I	A/R	R	C	C

R - Responsible | A - Accountable | C - Consulted | I – Informed



RACI Matrix for Marriott-Starwood Breach Responsibilities Continued

Key Activities	Board/ Executives	CISO/Security Lead	IT and Operation Teams	Internal Auditor	External Auditor
Incident Response	A	R	R	C	I
Compliance and Regulatory alignment	A	R	C	R	C
Security Audits	I	C	C	C	R
Penetration Testing	I	C	C	C	R
Risk Reporting	A	R	I	R	C

R - Responsible | A - Accountable | C - Consulted | I – Informed



Conclusion

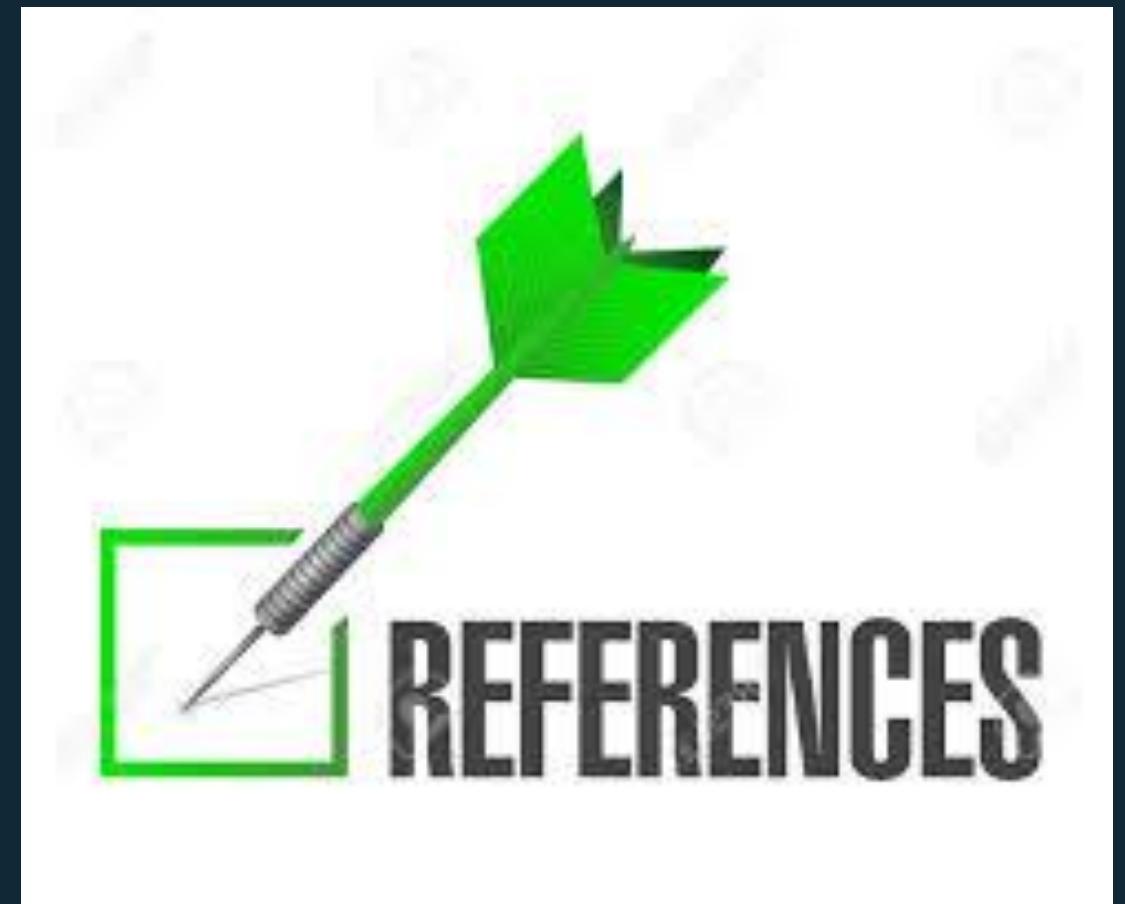
The Marriott case shows that failing to distinguish between **security governance** (strategic oversight, risk appetite, policies) and **security management** (operational controls, monitoring, response) leads to long-term breaches.

By clearly defining roles and responsibilities (as reflected in the RACI chart), organizations can align governance and management, ensuring inherited risks are addressed, operations are secured, and emerging threats are detected in time.



References

- ISACA COBIT 2019 – distinguishes governance (Evaluate, Direct, Monitor) from management (Plan, Build, Run, Monitor).
- NIST Cybersecurity Framework – emphasizes governance in establishing and monitoring risk strategy.
- ISO/IEC 27001:2022 outlines ISMS requirements (management) and leadership commitment (governance).
- <https://www.upguard.com/blog/what-is-a-ciso>
- <https://www.pmi.org/learning/library/project-governance-critical-success-9945>
- [board-overight-of-managements-risk-appetite](#)
- <https://www.grcmana.io/learn/grc/governance-roles>





Thank you
Questions?



Prepared by Group 2 members:

1. Gean Bernard
2. Khumo Tsoeu
3. Stella Oluwabukola Adejumo
4. Dolapo Ajibade
5. Vandana Mygapu
6. Magdalene Akpan
7. Tosin Oyewole
8. Nabirye Zahara
9. Muminat Lamidi
10. Odion Shalom Ebosetale
11. Hussein Kaosara Dolapo
12. Tinyang Stacey Enjeck
13. Linda Oluwadamilare Ogunsuyi
14. Comfort Tosin Olowookere
15. Nneamaka Edwin
16. Precious Ogwumike
17. Oluwatimilehin Oluwagbemi
18. Azeezat Animashaun
19. Ibrahim Zainab
20. Ojeah Laura
21. Rachael Gakanyi
22. Taiwo Owolebi
23. Akinleye Abidat Bolanle
24. Yusroh Titilayo Oduola
25. Halima Abubakar