TORRENS UNIVERSITY AUSTRALIA

Cybersecurity Governance in Sustainable Enterprises

A Framework Analysis of the Qantas Data Breach
Examining Compliance Deficiencies in Third-Party Risk Management

Student: Jose Antonio Escalante Lopez
Student ID: A00154979
Course: CSE641 Cybersecurity for Sustainable Enterprises
Date: 2026-04-19
Assessment Type: Report

https://orcid.org/0009-0000-5896-6797
openpgp4fpr:bb5b08bd40c6bd27cf4e68a4b24525ef85e6a3ba

Table of Contents

1 Abstract

This report examines the 2025 Qantas cyber incident, in which a threat actor gained unauthorized access to a third-party customer servicing platform, exposing the personal information of approximately 6 million customers. The incident is analyzed through three cybersecurity compliance frameworks; the Essential Eight Maturity Model, the NIST Cybersecurity Framework and the ISO/IEC 27001 standard alongside applicable Australian legislation including the Privacy Act 1988 (Cth) and the SOCI Act 2018. The analysis identifies deficiencies in patch management, multi-factor authentication and third-party access governance as the primary contributing factors. The report further argues that cybersecurity integrity is a foundational requirement for sustainable enterprise operations within a Bio-Circular Green Economy context.

2 Cybersecurity role within Green Economies

The society awareness regarding the global challenges has been evolving in recent years. Some organizations had accepted the global issues contributing to solve them through their processes practices in a Bio-Circular Green Economy (*BCG*).

> A BCG economy can be described as a system that tackles global challenges through a model of economic, social and environment production and consumption that aims to build a sustainable society based on developing bioproducts and using waste in a closed loop system through approaches such as reduction, reuse, recycle etc. (Edyvean et al., 2023, p. 52)

Defining sustainable organizations within a BCG is important. However, the functioning of these systems could be easily broken if the technology used to that purpose is compromised. Sulich et al. (2021) stated the importance of maintaining the integrity of the systems, availability and confidentiality to allow sustainable processes to operate effectively and achieve the goal of sustainability. This report examines Qantas data breach to analyze how governance frameworks and cybersecurity regulations support sustainable enterprise operations.

3 Qantas Cyber Incident

The interconnection among devices, networks, and third-party service providers is growing exponentially, expanding the attack surface for organisations globally. This is exemplified by the 2025 Qantas cyber incident, where a threat actor gained unauthorised access to a third-party customer servicing platform, exposing personal information of approximately 6 million customers (Qantas Airways Limited, 2026). While confidentiality was compromised, data integrity and operational availability were maintained flights and services remained fully unaffected (Qantas Airways Limited, 2026). Reputational consequences were significant, with a public CEO apology issued, while financial exposure remains subject to regulatory determination. Qantas Airways Limited (2026) documented proactive notifications to the ACSC, OAIC, and AFP as minimum regulatory obligations met. Further details of the incident are available at Qantas Newsroom. Further examination of applicable governance frameworks and compliance strategies follows.

4 Governance strategies and standards

As digital interconnection between organizations and third-party service providers expanded, legislative frameworks became necessary to define accountability for personal data protection.The **Privacy Act 1988(Cth)** serves as an example of that need. Qantas remained legally responsible for protecting customer personal information under the *Australian Privacy Principle 11-security of personal information subsection 11.1* (Office of the Australian Information Commissioner, 2024), regardless of whether that data was handled by a third-party operator. The Privacy Act 1988 (Cth) is one of several laws governing Qantas's obligations in this incident. Under Part IIIC of the *Privacy Act 1988 (Cth)* (Australian Government, 1988) requires APP entities to notify affected individuals and the OAIC when a data breach is likely to cause serious harm highlighting the essential compliance required by Qantas. Moreover, under the SOCI Act 2018 (Cyber and Infrastructure Security Centre, 2018), Qantas was required to maintain a written risk management program

covering its critical infrastructure assets, including risks arising from third-party service providers. The breach suggests this program did not adequately govern third-party platform access. The Qantas data breach demonstrates how laws protect users, organisations and the data exchanged between entities. Personal information held by organisations must preserve its confidential, integral and available nature (Sulich et al., 2021). In this incident, confidentiality was compromised through inadequate governance of third-party platform access, exposing the personal information of approximately 6 million customers. However, data integrity and availability were maintained demonstrating that the breach, while significant, was contained in scope.

5 Cybersecurity Compliance Frameworks

This paper will examine the *Essential Eight Maturity Model*, *NIST Cybersecurity Framework* and the *ISO/IEC 27001* standard that were utilized to analyse deficient processes regarding personal information custody by third-party actors.

Knowing that laws and regulations protect and define how organizations, customers and the world relate to each other, there are tools that serve as guides to preserve the nature of the regulatory governance; these are frameworks. The Essential Eight Maturity Model is an example of how an enterprise addresses a technological problem such as a data breach. The Figure 1 illustrates that the main issue was gaining access through a patch that was not updated in the 48 hrs window stated in the Essential Eight Maturity Model. Therefore, the hackers moved through the network possibly due to the absence of multifactor-authentication of users' credentials and finally extracted 6 million records from the database because of the insufficient restriction of privileges of the third-party users' accounts. This incident highlights the necessity for Qantas to audit and test third-party operators' procedures.

Figure 1: (Australian Signals Directorate, 2017)

Standards are needed as well to determine particularly how procedures must be implemented or at least the minimum requirements to meet. The ISO/IEC 27001 standard aims to set the responsibilities of the entities among their whole working process and establish preventive and containment procedures against technological threats (International Organization for Standardization & International Electrotechnical Commission, 2022, p. 1). The Qantas cyber incident exhibits a possible fragile supervision of third-party risk management processes as well as their non-compliance with section A.5.20 of the ISO/IEC 27001 standard (International Organization for Standardization & International Electrotechnical Commission, 2022, p. 12). Additionally, section A.8.8, A.8.19, A.8.5 and A.5.17 are strongly related throughout the incident, underscoring the absence of these implementations stated in the Essential Eight Maturity Model and the ISO/IEC 27001 where Qantas was responsible for maintaining data confidentiality. The convergence of these deficiencies across the ISO/IEC 27001 standard and the Essential Eight Maturity Model is further examined in the conclusion.

Another framework that assists cybersecurity professionals to assess the organizations' performance is the NIST Cybersecurity Framework. This tool provides an overall taxonomy of high-level cybersecurity outcomes that serve as understanding, assessment and prioritization of cybersecurity efforts to be communicated within the company (National Institute of Standards and Technology, 2024). The Qantas incident demonstrates how a business can sustain operations even with a threat developing internally. As shown in the Figure 2, the third-party operator of Qantas failed to identify and detect a threat, resulting in a data breach that implicated the failure to protect the personal information of customers. The absence of the NIST

CSF Identify and Detect functions within the third-party platform governance reflects a significant compliance gap that enabled the incident to escalate.

The implications of this incident extend beyond reputational damage and the possible harm to customers through the exposure of their personal information. If Qantas was following a path of sustainability, the incident disrupted it by forcing the organization to assign time, efforts and resources to an external situation that compromised the company at every level. The convergence of these deficiencies across the ISO/IEC 27001 standard, the Essential Eight Maturity Model and the NIST Cybersecurity Framework is further examined in the conclusion.

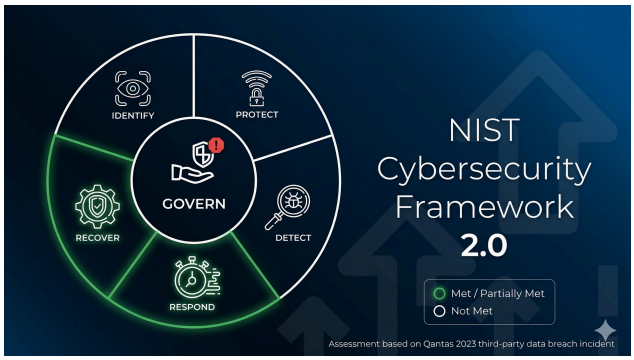

Figure 2: (National Institute of Standards and Technology, 2024)

6 Conclusion

To conclude, the external implications of the Qantas incident are significant, however the internal consequences the company faces across different levels are considerably greater. Frameworks such as the NIST CSF provide a broader vision to channel organizational efforts regarding cybersecurity culture. Standards such as ISO/IEC 27001 define the scope and methodology to achieve that vision. Furthermore, frameworks such as the Essential Eight Maturity Model assist in identifying the gaps in processes to adhere to standards and the cybersecurity landscape. Finally, laws benefit society by regulating the economic interaction between actors and promoting compliance within organizations. The Qantas incident ultimately demonstrates that sustainable enterprise operations depend not only on environmental and social commitments, but on the integrity of the digital systems that support them.

7 References

Bibliography

Australian Government. (1988,). *Privacy Act 1988*. https://www.legislation.gov.au/C2004A03712/latest/text

Australian Signals Directorate. (2017,). *Essential Eight maturity model*. https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model

Cyber and Infrastructure Security Centre. (2018,). *Security of Critical Infrastructure Act 2018*. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

Edyvean, R. G., Apiwatanapiwat, W., Vaithanomsat, P., Boondaeng, A., Janchai, P., & Sophonthammaphat, S. (2023). The Bio-Circular Green Economy model in Thailand – A comparative review. *Agriculture and Natural Resources*, *57*(1), 51–64. https://li01.tci-thaijo.org/index.php/anres/article/view/258253

International Organization for Standardization, & International Electrotechnical Commission. (2022,). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. ISO. https://www.iso.org/standard/27001

National Institute of Standards and Technology. (2024,). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

Office of the Australian Information Commissioner. (2024,). *Read the Australian Privacy Principles*. https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles

Qantas Airways Limited. (2026,). *Qantas cyber incident*. https://www.qantasnewsroom.com.au/media-releases/qantas-cyber-incident

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and Sustainable Development. *Procedia Computer Science*, *192*, 20–28. https://doi.org/10.1016/j.procs.2021.08.003

8 Technical Appendix

8.1 Appendix A — Framework Controls Mapped to the Qantas Incident

The following table summarises the specific controls from each framework that were identified as deficient in the Qantas cyber incident.

Framework	Control	Deficiency
Essential Eight	Patch Applications — Level 1	Critical patch not applied within 48-hour window
Essential Eight	Multi-Factor Authentication — Level 1	MFA absent for third-party platform access
Essential Eight	Restrict Admin Privileges — Level 1	Over-privileged third-party accounts
ISO/IEC 27001	A.5.19 — Supplier relationships	Inadequate security controls over third-party access
ISO/IEC 27001	A.5.20 — Supplier agreements	Missing security requirements in third-party agreements
ISO/IEC 27001	A.8.5 — Secure authentication	MFA not enforced for platform access
ISO/IEC 27001	A.8.8 — Vulnerability management	Unpatched software in third-party environment
NIST CSF	Identify — Asset Management	Third-party platform not adequately assessed
NIST CSF	Detect — Anomalies and Events	Threat not identified or detected in time
NIST CSF	Protect — Access Control	Insufficient access restrictions on customer data

8.2 Appendix B — Visual Documentation Reference

- **Essential8.png:** ACSC Essential Eight Maturity Model diagram illustrating the eight mitigation strategies across three maturity levels, used to assess Qantas compliance gaps in patch management, MFA and privilege restriction.
- **NIST.png:** NIST Cybersecurity Framework diagram illustrating the five core functions — Identify, Protect, Detect, Respond and Recover — used to assess Qantas third-party governance and threat detection deficiencies.