Information Security

Governance, Controls and Operational Resilience at 1datapipe

Table of Contents

Introduction

Enterprise organisations are under increasing pressure to demonstrate that the suppliers they engage maintain effective information security, operational resilience and risk management practices. Regulators, auditors and customers expect organisations to understand not only how data is used, but also how it is protected.

At 1datapipe, information security is a fundamental component of our operating model. Security controls are designed to protect the confidentiality, integrity and availability of information whilst supporting the operational resilience expectations of enterprise and regulated organisations. This is supported by our ISO27001 certification, held since 2022.

This guide provides an overview of the principles, governance structures and controls that underpin our approach to information security and operational resilience.

Security by Design

Information security is most effective when it is integrated into business processes rather than applied retrospectively.

1datapipe adopts a security-by-design approach, ensuring security considerations are incorporated throughout operational processes, supplier onboarding, technology implementation and service delivery activities.

This approach helps reduce risk, improve consistency and support regulatory expectations relating to governance and accountability.

Security considerations are embedded within:

- System design and implementation
- Supplier management processes
- Access management procedures
- Operational change activities
- Incident management processes
- Business continuity planning

Information Security Governance

Effective security requires clear ownership and accountability.

Information security oversight is supported through governance structures that define responsibilities, escalation routes and reporting mechanisms.

Governance activities include:

- Risk assessments
- Security reviews
- Control monitoring
- Policy management
- Incident oversight
- Continuous improvement initiatives

Security governance is designed to ensure that information security remains aligned with business objectives, customer requirements and emerging threats.

Security Controls

Information security controls are implemented to support the protection of systems, data and operational processes.

These controls may include:

Access Management

Access to systems and information is controlled according to business need and the principle of least privilege.

Access rights are reviewed periodically to ensure permissions remain appropriate.

Encryption

Encryption is used to protect information both during transmission and whilst stored.

Encryption helps reduce the risk of unauthorised disclosure and supports the protection of sensitive business information.

Monitoring and Detection

Monitoring capabilities assist in identifying unusual activity, potential threats and operational issues.

Monitoring supports both preventative and detective security controls.

Vulnerability Management

Security vulnerabilities can emerge as technology evolves.

Processes are therefore implemented to identify, assess and remediate vulnerabilities in a timely manner.

Security Awareness

Technology alone cannot eliminate risk.

Employees play an important role in maintaining security, and awareness programmes help ensure staff understand their responsibilities and recognise potential threats.

Risk Management

Security risks are assessed through structured risk management processes.

Risk management activities consider:

- Threat landscape
- Business impact
- Likelihood of occurrence
- Existing controls
- Residual risk

> *The objective is not to eliminate all risk, which is impossible, but to ensure risks are understood, managed and monitored appropriately.*

Incident Management

Even the strongest security environments must be prepared for potential incidents.

1datapipe maintains incident response procedures designed to support:

- Identification
- Investigation
- Containment
- Eradication
- Recovery
- Post-incident review

Where required, regulatory notification obligations are considered as part of incident management activities.

Lessons learned are used to strengthen controls and improve resilience.

Operational Resilience

Operational resilience extends beyond traditional information security.

Enterprise customers increasingly expect suppliers to demonstrate their ability to continue operating during disruptive events.

Operational resilience focuses on maintaining important services despite challenges such as:

- Cyber incidents
- Technology failures
- Supplier disruption
- Human error
- External events

Resilience planning supports continuity of critical business operations and helps minimise disruption.

Business Continuity

Business continuity planning helps organisations prepare for events that could affect normal operations.

Plans are designed to support:

- Service continuity
- Recovery activities
- Communication processes
- Escalation procedures

- Customer support activities

Business continuity arrangements are reviewed periodically to ensure continued effectiveness.

Third-Party Security Oversight

Enterprise organisations increasingly recognise that security risks can originate from third parties.

Supplier governance activities therefore include consideration of:

- Security maturity
- Compliance obligations
- Contractual commitments
- Operational dependencies
- Ongoing assurance activities

This helps ensure that third-party relationships align with organisational security expectations.

Security Assurance

Customers frequently require evidence that security controls are operating effectively.

Security assurance may include:

- Independent assessments
- Security reviews
- Policy documentation
- Governance evidence
- Risk management information

Providing assurance supports customer due diligence activities and strengthens trust.

Supporting Regulated Organisations

Regulated organisations face increasing scrutiny regarding operational resilience, cyber security and supplier risk management.

The expectations of financial regulators, data protection authorities and operational resilience frameworks continue to evolve.

Our approach is designed to support customers in meeting these expectations through strong governance, documented controls and ongoing oversight.

Conclusion

> *Information security and operational resilience are essential components of organisational trust.*

Through governance, risk management, security controls and resilience planning, 1datapipe seeks to maintain a secure and dependable operating environment that supports customers operating in highly regulated and risk-sensitive sectors.

As threats and regulatory expectations continue to evolve, we remain committed to continuous improvement and the ongoing protection of customer confidence.