GEMSERV SERVICES: DATA GOVERNANCE FRAMEWORK

Gemserv

Gemserv

INTRODUCTION

In today's data driven world, organisations are faced with increasing compliance, legal and regulatory requirements as well as a greater responsibility to protect their client's data. This, in turn, has raised the importance of organisations having robust Data Governance Frameworks. The key challenges that arise in establishing a Data Governance Framework are:

- Defining the Data Governance metrics to create a robust Data Governance Framework
- Streamlining and aligning the multitude of compliance, legal and regulatory requirements into a single effective and efficient governance model that will reduce the burden on the organisations to remain compliant, while ensuring that all the requirements are met

DATA GOVERNANCE FRAMEWORK

DATA GOVERNANCE FRAMEWORK

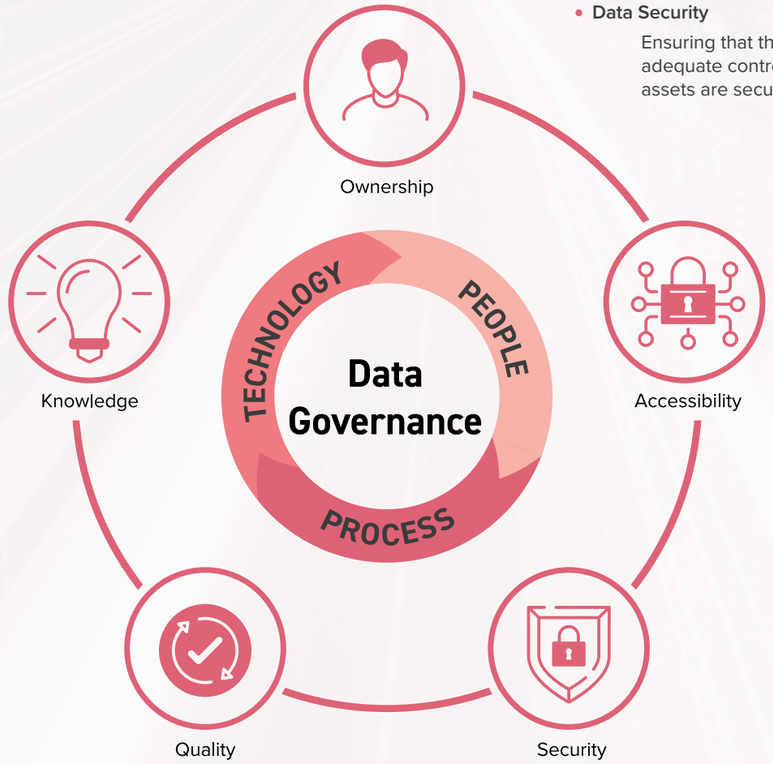
A Data Governance Framework is a cross-functional infrastructure that is used to manage the creation, maintenance and deletion of data across People, Processes and Technology within an organisation.

To be effective, the Data Governance Framework should ensure the following aspects are considered with respect to the organisation's data:

- Confidentiality: Ensuring that the data is available to only those who are authorised to access it
- Integrity: Ensuring that the data is accurate and consistent
- Availability: Ensuring that the data is available when it is required
- Quality: Ensuring that the data is fit enough to serve its purpose in a given context

In order to ensure these aspects are met, the Data Governance Framework should adopt the following principles:

- **Data Ownership & Accountability:**
  Identifying and assigning ownership of data assets within the organisation to ensure that there are identified individuals accountable for the governance and management of the data assets
- **Standardised Rules & Regulations**
  Creating policies and guidelines that will govern how the data is managed within the organisation
- **Data Quality Standards & Data Standardisation**
  Ensuring that data quality standards are defined to ensure that the data within the organisation is fit for purpose and conforms to defined data standards
- **Transparency & Auditability in Data Governance Processes**
  Ensuring that there are clear records of all Data Governance activities and processes providing a transparent view to any external regulatory body on how data has been managed within the organisation
- **Data Security**
  Ensuring that the organisation has implemented adequate controls to ensure the critical data assets are secured



DATA GOVERNANCE FRAMEWORK

There are a whole host of international standards, legislations and regulations that help organisations to formulate a Data Governance Framework that addresses the principles mentioned previously. The challenge is doing so in a way that is cost and resource effective, but efficient in meeting the needs of the organisation.

Most organisations adopt the iterative Plan-Do-Check-Act management method for control and continuous improvement of processes. Gemserv's clients requiring Data Services are in various stages of maturity in the below cycle. The cycle can be outlined as below:

- **Plan:** Establish objectives/plan required to deliver the desired results
- **Do:** Implement the plan established in the "Plan" phase
- **Check:** The output from the "Do" phase is checked to ensure it meets the objectives
- **Act:** The established processes are continually improved. Any actions identified to implement continuous improvement would feed into the "Plan" Stage

There are various use cases of how Gemserv's approach has helped organisations achieve various facets of data governance in an efficient and effective manner.

PLAN

- Gap Analysis Services
- Impact Assessment Services

DO

- Consultancy Services
- Implementation Service

CHECK

- Audit Services

ACT

- BAU Services

CASE STUDY 1 – DO – ISO 27001 & PCI DSS PROJECT IMPLEMENTATION

Typically, the second stage of our data services involves the 'Do' section, which is essentially developing the policies, procedures and processes necessary to embed lasting compliance within an organisation.

As one example of such a project, we provided specialist advice to NRS, a provider of disability aids and mobility equipment with over 1.4 million products delivered into homes every year, and a risk profile that included a high volume of personal data being processed. Gemserv's support included providing security assurance services through implementing a system for ISO 27001 compliance across the organisation.

With bespoke compliance at the heart of our service approach, Gemserv embarked on improving NRS' existing security controls in augmenting an Information Security Management System for their multi-site estate, rather than adding unnecessary cost through developing a generic set of policies from scratch. In particular, NRS highly appreciated the competitive edge that Gemserv was able to add, through allowing the organisation to quickly complete the NHS Toolkit's requirements, with a score of 100%. Additionally, as NRS is a company that depends largely on electronic transactions, Gemserv worked on aligning them with Payment Card Industry Data Security Standards (PCI DSS), to further differentiate the company from other device manufacturers and service providers on the market.

CASE STUDY 2 – CHECK – PCI THIRD PARTY ASSESSMENTS

The 'Check' stage of the Plan-Do-Check-Act cycle includes ensuring that implementation of compliance activities meets the relevant standards – either as established by the organisation, business or regulatory requirements, or best practice. To this end, Gemserv worked with JP Boden, a leading UK retailer, to ensure that their complex and multi-payment channel environment covering a range of different locations, systems, services and a few key service providers, were aligned and certified to the requirements of the PCI DSS. PCI DSS awareness is a critical factor to the success of any PCI assessment. Gemserv consultants provided advice, guidance and practical implementation support. This, coupled with a pragmatic approach towards the formal assessment, proved invaluable to the JP Boden compliance programme.

CASE STUDY 3 – CHECK – CYBERSECURITY AND DEVICE ASSURANCE

The 'Check' stage ensures that implementation of compliance activities meets the relevant standards. As part of this, Gemserv recently provided assurance services to Verv, a company developing 'Smart Homes' technologies that deploy machine-learning and data analytics to monitor the usage and cost of domestic appliances. Drawing on the expertise of Consultants with backgrounds working in network security and device engineering, Gemserv conducted an evidence-based assessment of Verv's device architecture, focusing on reviewing key documentation relevant to the security characteristics of the systems, and also underwent penetration testing on the devices to identify any vulnerabilities or weaknesses. Following this, Gemserv was able to provide a report with risk rankings of each identified weakness and advise on how to secure the Verv device in line with security best practices, to meet the requisite standards under existing and upcoming regulations.

CASE STUDY 4 – ACT – DATA PROTECTION OFFICER SERVICES

In the 'Act' stage of the Plan-Do-Check-Act cycle, Gemserv aims to provide ongoing advice to organisations so that they retain high standards of compliance in their day-to-day operations. As part of this, we provide outsourced Data Protection Officer or Cybersecurity Officer services, which allow clients to retain an established line of support to a team of professionals. This allows them to draw on the necessary expertise when requested, such as with respect to data breaches, data subject requests, legislative changes or supervisory authority investigations.

An example of this approach is the Virtual Data Protection Officer support we provided to JAC Computer Services. The organisation, a key supplier of health systems to the NHS, processed and had access to large amounts of sensitive personal data. Using our experience in data protection consulting for both technology companies and the NHS, Gemserv provided a risk-based approach to implement GDPR compliance, including ensuring Privacy by Design in policies and procedures, providing training to staff, risk-assessing suppliers, liaising with supervisory authorities and advice and guidance on a free-flowing basis.

DATA GOVERNANCE FRAMEWORK

ADVANTAGES OF GEMSERV'S APPROACH

- Reduced effort for compliance teams as Governance, Risk & Compliance (GRC) efforts are streamlined,
- Reduced cost of compliance/Increased ROI
- Increased efficiencies as existing controls are leveraged
- Better centralised metrics for GRC

In conclusion, there is an increasing onus on organisations to meet various legal and regulatory standards to protect the data they hold. In order to do this, organisations need to implement a good data governance model in an effective and efficient manner that minimises the resources required, while maximising the organisation's GRC posture and maturity. Gemserv's proven approach will help ensure that organisations can leverage existing controls and processes to efficiently implement an effective Data Governance Framework.

Gemserv

LONDON

+44 (0)20 7090 1022

bd@gemserv.com

IRELAND

+353 (0)1 669 4630

ireland@gemserv.com

CONTACT US TODAY, TO DISCOVER HOW WE CAN HELP YOU