

Overview

This workshop is aimed at assisting company executives, senior leadership and middle-management understand the full context, scope and impact of privacy and data protection.

Whilst addressing key aspects of regulation and standards, it focuses on the strategic imperatives associated with good governance, and effective and sustainable privacy and data protection management.

By considering primary risks, benefits, and operational impacts, it is designed to help leaders appreciate their need to be involved, understand their specific responsibilities and what is needed in their teams to ensure that a sustainable culture of privacy and data protection is embedded into the organisation.

After considering current capabilities, clearly defined next steps are considered along with associated tools, frameworks, and deliverables.

Privacy & Data Protection Workshop

Key Outcomes:

After this workshop, leaders will:

1. Have a clear understanding of privacy and data protection and the regulatory requirements.
2. Have gained insights into the strategic and tactical drivers for sustainable privacy management.
3. Understand the benefits of establishing a defined programme for privacy management and governance.
4. Be informed on where current gaps and potential risks lie.

Be provided with a high-level, step-by-step guide on establishing a data privacy programme.

5. Be aware of the options available to them for more detailed planning and implementation of an operational programme for privacy compliance.
6. Understand what further training is needed.

Profile of Facilitator



Alan Raubenheimer

CIPP/E, CIPM, CIPT, FIP (IAPP)
CDMP (DAMA)

Alan has over 35 years' experience in Data Management, Analytics, and IT Leadership. He is a former CIO in the Financial Services arena and has a wealth of experience in assisting organisations design and implement technology, governance privacy architectures, strategies, operating models, and programmes.

He specializes in Information and Technology Governance and Data Privacy and has acted as lead consultant in helping many organisations implement programs for **data governance and privacy**, including some of the largest insurers and banks in Africa and worldwide.

Alan is a certified international trainer for the IAPP (International Association of Privacy Professionals) and holds the CIPP/E, CIPM, CIPT certifications and holds the elite Fellow of International Privacy FIP certification. His company is an official training partner for the IAPP, and he personally provides instruction in all the certifications he is qualified in. He also provides training on other areas of data management, governance, and information risk management.

In the past two years he has assisted organisations in South Africa and Bermuda to implement governance frameworks and programs for Information & Technology Governance Privacy Management, Cybersecurity Risk Management and Data Governance.

Content

Note: Content can be adjusted to the size of the audience, nature of the organisation and will address both global and specific local requirements.

- ❖ Introduction and discussion of key drivers in the organisational context.
- ❖ Review of key concepts and how privacy and data protection fit into corporate governance and strategy.
- ❖ Consider regulatory requirements and impact
 - Key elements of the data protection regulation and other influencers
 - Understand roles and responsibilities
 - Understand the intersect and distinction between security and privacy.
 - Consider impact on the organisation, timelines
 - Discuss high-level risks – include security and operations
- ❖ Consider rationale, benefits and liabilities, challenges of readiness and program establishment
- ❖ High-level analysis of organisational readiness
 - Executive sponsorship, buy-in, budget, accountability
 - Capability Assessment done
 - Framework and strategy defined
 - Organisational roles aligned
 - Policy & procedure alignment
 - Must include incident & breach response
 - Training and Communication plan created
 - Initial training conducted (for existing staff and established for new joiners)
 - Risk Analysis completed
 - Vendor and supplier analysis
 - Privacy Program established
 - Operational plan of activities
 - Key milestones established
 - Stakeholder engagement
 - RACI
 - Measurement
 - Monitoring
- ❖ Consider next steps, including:
 - Conduct Maturity/Gap Assessment
 - Consider standards and frameworks – align with Information & Technology, Data/Data Management and Security Frameworks and Governance. If needed:
 - Create Information & Technology Governance Framework
 - Create Security/Cybersecurity Framework
 - Create Data Governance Framework
 - Create Privacy/Data Protection Framework
 - Review/establish Policies and Procedures
 - Roadmap, implementation plan
 - Establish roles, appoint key individuals
 - Create operational plan(s) - include training, awareness and communication, risk analysis and vendor management
 - Create Measurement and Monitoring plan – include KPI's for key stakeholders
 - Discuss enabling technologies for Data Governance, Privacy Management
 - Procurement
 - Implementation

To book your seat, please contact us : info@velisafrica.co.za (0861716150)