Hands-On Data Protection Workshop Topics

Hands-on Focus & Projects

The course heavily focuses on hands-on activities (aided by the bundled data protection management system; DPMS) and assignments given. It trains and shows participants how to be compliant, emphasizes on information security, and comes with Compliance Manual, Audit & bundles all the Tools needed. Participants may go on to take the CIPM International Certification.

Core Modules & Outcomes

1. Introduction to PDPA & Compliance – 1.0 Day
2. Information Security: Policy, Templates & Tools - 1.0 Day
3. Implementing Data Protection Policies & Initiatives - 1.0 Day

DAY 1 : Introduction to PDPA & Compliance

Section 1: The Personal Data Protection Act

1.1 Review the requirements & principles of the PDPA & clearing confusion
1.2 Apply the knowledge in the context of your organization - policies, practices, products and services
1.3 Consequences of non-compliance & what are needed to comply

Section 2: Roles & Responsibilities of the Compliance/Data Protection Officer

2.1 Understand what the organization must do in order to comply with the PDPA
2.2 Define the responsibilities of the DPO & Preparation for Enforcement

Section 3: Programme Management & the Privacy Operational Life Cycle

3.1 Identify various exposures within the organization
3.2 Interview executives confidently to gather and evaluate the current practices against PDPA regulations and compliance standards
3.3 Conduct an Assessment, Gap Analysis & Personal Data Inventory Map on procedures and practices of business / services that could contravene the PDPA and security policies

Hands-On Data Protection Workshop Topics

Day 2 - Information Security: Policy, Templates & Tools

Section 4: Information Security Basics & Plan
4.1 Define Information Security & Difference Between Privacy & Security
4.2 Create Action Plan to Close Gaps and Identify Steps to Achieve Info. Security
4.3 Be Aware of the Information Security Controls & Competency Areas
4.4 Track the Identified Gaps to Closure

Section 5: Controlling, Securing & Implementing an Information Security Management System for PDPA
5.1 Know the SPECIFIC Steps Needed for Controlling & Securing Personal Data
5.2 Create & Implement a Information Security Policy using ISO27001 Methodology & P-D-C-A Model

Day 3 - Implementing Data Protection Policies & Initiatives

Section 6: Data Protection Policy
6.1 Define Data Protection Policy & Difference Between Privacy Policy & Notice
6.2 Draft own Personal Data Protection Policy amid various considerations

Section 7: Closing the Gaps Identified & Next Steps
7.1 Follow a methodology to help close the gaps identified
7.2 Get buy in & Follow-up with management & Committee

Section 8: Staying Compliant & Performance Management
8.1 Understand the need to continue to PDPA Audit on an on-going basis
8.2 Monitor Compliance & Communicate the Compliance Framework

Section 9: Incident / Response Management & Demonstrating Accountability
9.1 Understand information requests & importance of Data Breach Notification
9.2 Demonstrate Accountability while handling & Responding to any Incidents

Section 10 : Mock Investigation, Observations, FAQs & Close Up