THE CHAMPION/PROTECTOR/PROMOTER PROGRAM FOR

DATA PRIVACY AND CYBERSECURITY

TRAINING AND AWARENESS

Virtual Online | Duration 15 H

INSTRUCTOR PROFILES

Kersi F. Porbunderwala

Data Protection, Data Privacy, GDPR, IT Security and GRC Profile

My corporate tenure started in 1972 as Night Manager (during studies) at Sheraton Hotel Copenhagen. After graduation in Accounting and Finance from Copenhagen Business School in 1976, I began my career as Credit Manager, later as Chief Accountant, Business Controller, Finance Director and Managing Director, starting with Westin Hotels (1984-1976) and then for SAS Radisson Hotels (1988-1984). During my tenure at Westin Hotels, I was a member of the Group Financial Services Committee. In 1988 I was the President and CEO for a stock-listed real estate company and from 1996 as Nordic/European Financial Operations as Business Controller for ExxonMobil. From 2018-2005, I was the director of RGP; a US stock listed consultant company. I have further completed Westin Hotels Executive Management Certification Program in 1980 and The SAS Executive Development Certification Program in 1984.

GRC/GDPR/IT AND CYBERSECURITY PROTECTOR, PROMOTER AND CHAMPION TRAINING AND AWARENESS OBJECTIVES:

From the directors to all employees GRC/GDPR/IT and Cybersecurity Training and Awareness have become an essential part of the business. The focus now is on developing appropriate response plans that minimise the damage in the event of a GRC/GDPR/IT and Cybersecurity breach. The organisation, the board, management, and all managers can develop a proper response plan only if everybody in the organisation has a firm grip on GRC/GDPR/IT and Cybersecurity fundamentals.

We have developed a -5-3 and -8hour online training and awareness program on GDPR, IT and Cybersecurity issues as GRC components. Organisations that handle personal or private data or information face complex data privacy and IT and cybersecurity challenge to effectively manage GRC risks. The impact of these challenges covers the entire information lifecycle of the data privacy and protection processes. That is why in each of the three online seminars will ensure that all participants get training on compliance that goes beyond the general requirements and address the critical steps and stages of GRC, data privacy and IT and Cybersecurity compliance highlighting the essential success factors and everybody in the organisation has a common understanding of the values of GRC/GDPR/IT and Cybersecurity Training and Awareness:

1. Training the board, directors, senior management, and employees to identify potential issues and develop reporting systems to encourage good behaviour and improve performance.
2. Everybody in the organisation understands the importance of Data Privacy, Data Protection IT and Cybersecurity and its significance on every business equation side.
3. Cyber-attacks are costly for businesses and reputation. In addition to financial damage, the breaches are progressively destructive to systems and networks, and there is a need for improving frameworks to determine a purpose and consistent processes.
4. Reducing the costs and evaluating performance as cybercrime costs are more than 400$ billion. Data Privacy fines amount to 250$ billion, and Compliance costs are now up to %7 of the organisation's expenses.
5. Supervising the corporate guiding principles and policies to analyse performance and take a critical eye to the performance.

GOVERNANCE, RISK AND COMPLIANCE (GRC)

- Concepts, objectives, principles, and best practices for GRC.
- How to ensure effective GRC processes across the organisation:
a clear understanding of the respective roles and their relationships with each other.
- The People, Purpose, Process, and Performance components of Good Governance.
- How to develop a corporate governance and risk management frameworks for setting responsibilities and accountabilities for the board and delegated committees .
- How to manage the corporate governance and risk management frameworks for setting responsibilities and accountabilities for the senior management.
- Developing, executing, and monitoring a corporate code of ethics outline and define a company's business practices.
- How to focus on ethical and moral codes to shape the company's corporate culture.
- Introduction to the Nordic Corporate Governance Model .
- Aligning corporate goals with Governance objectives and framing the company's plans to the corporate governance program.
- How to develop a solid Governance structure to monitor dealings, interactions, and transactions effectively.
- How to develop more transparent business practices, structure, and framework to trace all activities efficiently.
- Monitoring fraud risk management to prevent unlawful or illicit activity. If well-designed and applied, reporting systems should allow companies to monitor success and detect fraudulent activity by using their employees for their eyes and ears.
- How to supervise the corporate governance and risk management frameworks for setting responsibilities and accountabilities for the CxO and Compliance and Risk Officers.
- Tips and roadmap to design a useful model for corporate governance.
- How to implement a compliance register for regulatory, legal, and contractual regulations.
- How to facilitate data-driven risk assessments with quantified risk.
- How to design and use a risk and control matrix.
- Strategies to design, formalise, implement, and train on internal controls and write good policies with who-is-doing-what Responsible, Accountable, Consulted, Informed (RACI) matrices.
- Tips for wisely invest in internal activities, consultants, and software.
- Discussions about real-world business cases.

GDPR AND PRIVACY

- Essential requirements, standard provisions, concepts, and principles for GDPR compliance and other key privacy regulations.
- How to create synergies between data security and privacy compliance.
- How to design and operate a privacy program.
- Tips and model of a security policy and other supporting policies.
- How to identify and record the uses of personal data.
- How can GDPR force the organisations into taking better care of the personal data they hold.
- Tips and models for standard policies: access policy, document retention schedules, policy on the acceptable use of information technology.
- Tips for implementing and auditing efficient security and compliance controls for privacy.
- Tips for managing consents, information requests, and breaches to compliance with GDPR.
- How to monitor and test internal and external compliance with security controls on personal data.
- Contractual requirements for suppliers processing personal data.
- Discussions about real-world business cases.

IT- AND INFORMATION SECURITY

- The Cybersecurity technologies, processes, and practices designed to protect networks, computers, programs, and data from IT and cyberattack, damage or unauthorised access.
- The objectives of the CIA Triad; Confidentiality, Integrity, and Availability.
- Concepts, objectives, principles, and best practices for information security.
- Strategies for selecting the data security framework: ISO, NIST, ISF, COBIT, SANS, and Octave.
- How to develop and conduct a scenario planning exercise for Data breach.
- How to identify/quantify cyber risks based on threats and vulnerabilities.
- Tipis to identify and implement key IT controls.
- How to protect against email scan, phishing, malware, attacks, and other common threats.
- How to monitor security with vulnerability assessments, penetration tests, log reviews, and other activities.
- Roadmap to respond to security breaches and incidents.
- How to design an awareness training program.
- Discussions about real-world business cases.

Date
22 - 24 February, 2021

Course Fee
450 JOD

Questions and Local Registration
For More Information And Registration From Jordan Please Contact
Eng. Amer Al Najjar Training Center Manager Mobile :
00962777399728