FQA Certified Risk Management – Global best practices
"IT & Information Security Risk Management"

Workshop facilitated by leading global risk 'guru' including ISO 27001:2022 aspects and practical case studies

Course description:

Re-vamp your IT DR and InfoSec processes with the latest best practice regarding threats such as:

• Cyber (including Ransomware) attacks
• Data centre downtime (e.g. due to flooding or fire)
• Assessing IT Risk and conducting a Business Impact Analysis (BIA)

During this highly interactive workshop, you will come away knowing you've validated your existing processes against the latest lessons learned or started to build a practical IT Risk, IT DR and InfoSec process from scratch. Various real-life examples will include 'the good, the bad and the ugly' which we will review and from which we will learn useful tactics.

The case studies we use will come from a range of different sectors such as banking, technology, telecommunications, logistics, manufacturing, energy, government, insurance and other industries.

Apart from the facilitator highlighting various examples, video materials can be used followed by discussion and analysis.
Discussions, case study analyses (e.g. of recent cyber-attacks) and other practical exercises to play with the learned material will be part of this interactive workshop.

.**This workshop entitles you to 08 CPE credits.**

Learning outcomes, benefits and tools/techniques

This course gives you all the tools to develop a practical, compliant IT continuity and Information Security Management process.

- Gain practical experience during **interactive exercises, discussions** and **case studies** – including topics such as Governance, IT Risk assessment, Business Impact Analysis, RTOs/RPOs, IT DR testing, the CIA concept and the changes in ISO 27001 related to the 2022 version.
- Learn to utilise a practical **Information Security Assessment template** and understand the link with other Management Systems such as Business Continuity and Enterprise Risk Management.
- Acquire the necessary expertise to contribute to **implementing** an IT continuity and/or Information (including Cyber) Security Management process in accordance with ISO 27001, COBIT and/or ITIL.
- Learn how to **reduce efforts** to maintain IT DR and InfoSec **documentation**
- Gain practical ideas for achieving **commitment to IT Risk and InfoSec** at Executive level as well as all other levels of your organisation
- Know the concepts, approaches, standards, methods and techniques allowing to **effectively manage** IT Risk and Information Security Management process
- Key Performance indicators (**KPIs**) and Key Risk Indicators (**KRIs**)

- Other **'hot topics'** relevant to your industry/location (based on the results of your pre-workshop delegate questionnaire).
- **Who should attend:**

No prerequisites or prior knowledge are required. This course suits those either **directly or indirectly involved in IT Risk, IT Management, IT Continuity/DR, Enterprise Risk Management, Business Continuity, Information Security and/or Cyber Security**, or interfacing/related processes or projects - in any industry, and in any size organisation:

- CISOs
- Information/Cyber Security professionals
- IT Professionals
- IT DR Managers
- Business Process Owners and Risk Owners
- Business Risk Managers
- Business Continuity Managers/Co-ordinators
- Governance, Risk and Compliance Managers/Specialists
- InfoSec and Risk Consultants
- Operational Risk Managers/Analysts
- Auditors
- Project Managers
- Business Analysts
- Business Strategy Managers and Strategic Planners
- Senior and Operational Managers/Executives.
  .

For further information please email us at **info@continuityandresilience.com**