The NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) has become a reference for executives and upper management in many critical infrastructure sectors, creating a lexicon to frame the discussion of risk management. However, even with this reference, many organisations struggle to close the gap among risk tolerance, business objectives and cybersecurity efforts.

This new course on Implementing NIST Cybersecurity Framework Using COBIT® 5 course will equip managers with the skills to frame real-world, technical cybersecurity projects in risk management terms that executives can understand and use to make and justify business decisions. Based on a guidance developed by ISACA, the course is focused on the Cybersecurity Framework (CSF), its goals, the implementation steps and the ability to apply this information. The course and exam are for individuals who have a basic understanding of both COBIT® 5 and security concepts, and who are involved in improving the cybersecurity program for outside organisations or their own organisation.

Background
In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary risk-based cybersecurity framework that is “prioritized, flexible, repeatable, performance-based, and cost-effective.”

The Cybersecurity Framework (CSF) was developed through an international partnership of small and large organisations, including owners and operators of the nation’s critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST).

Who Should Attend
Individuals who have a basic understanding of both COBIT® 5 and security concepts, and who are involved in improving the cybersecurity program for outside organisations or their own organisation.

Learning Outcomes
- Understand the goals of the Cybersecurity Framework (CSF)
- Understand the content of the CSF and what it means to align to it
- Understand each of the seven CSF implementation steps
- Be able to apply and evaluate the implementation steps using COBIT® 5

Course Contents
- **COBIT® 5 Review**
  - Overview to CSF; CSF Structure
- **Phase 1**
  - Step 1: Prioritise and Scope; Scenario Activity
- **Phase 2**
  - Step 2: Orient & Step 3: Create a Current Profile; Scenario Activity
- **Phase 3**
  - Step 4: Conduct a Risk Assessment & Step 5: Create a Target Profile
  - Scenario Activity
- **Phase 4**
  - Step 6: Determine, Analyse, and Prioritise Gaps
  - Scenario Activity
- **Phase 5**
  - Step 7: Implement Action Plan
- **Phases 6**
  - CSF Action Plan Review
- **Phase 7**
  - CSF Life Cycle Management
- **Exam Preparation:**
  - Implementing NIST CSF Exam

Duration: 2 Days