Creating an Insider Threat Detection Programme

TICDS-109

The purpose of an Insider Threat Detection Programme is to equip business leaders with the insight and tools needed to identify, counter, and mitigate risks posed by insider threats. These threats, whether malicious, negligent, or accidental, can bypass traditional security measures due to the insider's legitimate access to systems and data.

The programme helps leaders understand behavioural indicators, implement proactive controls, and foster a culture of vigilance across the organisation. By doing so, it reduces the likelihood of data breaches, financial loss, reputational damage, and regulatory non-compliance.

Module 1: Insider Threat Awareness

A Threat Detection Programme helps organisations identify and respond to insider risks early, protecting sensitive data, ensuring compliance, and maintaining business continuity.

- The key governance elements of the programme
- How to target communications effectively
- Leadership responsibilities
- The five steps to establishing a threat detection programme

Suitable for:

An Insider Threat Detection Programme course is essential for individuals and teams responsible for safeguarding sensitive data, systems, and organisational integrity.

Benefits:

The Delegate will receive a Total Quality Assured (TQA) certificate of achievement upon successful completion.

Skills achieved:

- Data Security (Advanced)
- IT Threat Detection (Intermediate)

Estimated Time:

20 Minutes

Related Resources:

- Information Security Breach Assessment
- ISO 27001 Gap Analysis
- Planning Gap Analysis
- Support Gap Analysis
- Operational Gap Analysis
- Data Policy Agreement Checklist
- Information, data and Cyber Security Incident

Related Courses:

- Are you the Target?
- Insider Threat Awareness
- Essentials of Cyber Security