

# Senior Information Risk Officer

## Course Agenda

8:30 am to 9:00 am	Registration and Reception
9:00 am to 10:00 am	Security Climate Recent High Profile security events Security Principles and Definitions Data classification Government protective marking scheme Personnel clearance Security labelling issues Overview of Risk Management Risk management process Information Assurance What is Information Assurance? Information Governance Information Management Knowledge Management Intellectual Property
10:00 am to 10:15 am	Break
10:15 am to 12:30 pm	Strategic policy and legal initiatives Governments reports that shaped current policy Hanigan, Thomas Walport Review, Poynter review of Revenue & Customs Data Handling review and HMG Security Policy Framework SIRO IAS Duties and deliverables
12:30 pm to 1:30 pm	Lunch
1:30 pm to 3:00 pm	Key roles, Senior Information Risk Owner (SIRO), Information Asset Owners (IAO) their role, responsibilities and accountabilities Departmental Security Officer (DSO) role, responsibilities and relationship with SIRO
3:00 pm to 3:15 pm	Break
3:15 pm to 4:45 pm	Governance, Risk Management & Compliance Register Information Assets Information Assurance IA Maturity Model and Assessment Framework IA model self assessment 2010 Cabinet Office Information Risk Return Tool Annual Information Risk Report (IRR)
5:00 pm to 5:30 pm	IA Review Process Action Plan IAO responsibilities
	End of Day 1

Day 2	
9:00 am to 10:30 am	<ul style="list-style-type: none"> <li>Information Management</li> <li>Records Management</li> <li>RM standard ISO 15489</li> <li>The National Archives' Information Management Assessment (IMA) Strategy</li> <li>Data Sharing</li> <li>Quality of Information</li> <li>Staff use of Blogs and Wikis</li> <li>Freedom of Information</li> <li>Data Protection Act</li> <li>How data should be collected and stored</li> <li>Privacy impact Assessments</li> <li>New penalties</li> </ul>
10:30 am to 10:45 am	Break
10:30 am to 12:30 pm	<ul style="list-style-type: none"> <li>Risk Management</li> <li>Overview of ISO 3100</li> <li>Failure to exploit opportunities</li> <li>HMG Orange book</li> <li>Assessing Risks</li> <li>Risk Appetite</li> <li>Addressing risks</li> <li>Horizon Scanning</li> <li>Risk Assessment tools</li> <li>2010 Cabinet Office Information Risk Return Tool</li> <li>SIRO Checklist and issues of note</li> </ul>
12:30 pm to 1:30 pm	Lunch
1:30 pm to 3:30 pm	<ul style="list-style-type: none"> <li>Information Security</li> <li>Overview of ISO27001</li> <li>Security policies</li> <li>Security Awareness</li> <li>Access control</li> <li>IT risk management</li> <li>IS1 and IS2 Risk assessment</li> <li>Business Impact tables</li> <li>Example vulnerabilities</li> <li>Exploitation techniques and countermeasures</li> <li>Independent Testing</li> <li>Penetration tests</li> <li>CESG IT Health Check</li> </ul>

## Day 2 Continued

3.30 pm to 3.45 pm	Break
3:45 pm to 5:30 pm	Forensic Readiness Rowlinson: 10 Steps for Forensic Readiness Planning Key Forensic policies BS 10008:2008: Evidential weight and legal admissibility of electronic information. Specification Incident response IS Policy requirements for effective incident response Incident reporting Incident response guidelines Incident review lessons learned SIRO Checklist and issues of note Horizon scanning Sources of information on new threats SIRO Role and responsibility Final Checklist IAO Role and responsibility Final Checklist
5.30 pm	Close