

About Us



We are Educom International in partnership with UK Executive Consulting & Training, knowledge solutions providers. We offer consulting and professional training with well-established track record in the UK, Europe, Middle East and Africa.

We are committed to training professionals to become smart decision-makers and creative problem-solvers. We have helped countless clients reach sustainable positive change.



We offer to the forward looking, discerning corporate organizations, the benefit of deep content, relevant up-to-date, and accurate skills-oriented-training programs.

Our clients include startups, corporate executives, Banks, Financial Services, Government Organizations, and Oil and Gas companies of all sizes.

Information Security General

ITIS01	Information Security Governance: Guidance for Information Security
111301	Managers
ITIS02	Security Considerations for Cloud Computing
ITIS02	Cybersecurity Audit
ITIS04	Fundamental of IT Risk
ITIS05	Responding to Targeted Cyberattacks
ITIS06	fundamental of Payment Card Industry Data Security Standard
ITIS07	General Data Protection Regulation (GDPR)
	Reduce the Attack Surface
ITIS08	
ITIS09	Protect your digital Assets
ITIS10	Introduction to NIST Security and Privacy Controls for Information
ITIC11	Systems and Organizations
ITIS11	5G – Privacy Threats, Mitigating Mechanisms & Regulatory
ITIS12	Information Technology Controls
ITIS13	Change and Patch Management Controls
ITIS14	Continuous Auditing (IT): Implications for Assurance, Monitoring, and
171015	Risk Assessment
ITIS15	Management of IT Auditing
ITIS16	Managing and Auditing Privacy Risks
ITIS17	Managing and Auditing IT Vulnerabilities
ITIS18	Information Technology Outsourcing
ITIS19	Auditing IT Application Controls
ITIS20	Identity and Access Management
ITIS21	Business Continuity Management (BCM)
ITIS22	Developing the IT Audit Plan
ITIS23	Auditing IT Projects
ITIS24	Fraud Prevention and Detection in an Automated World
ITIS25	Auditing User-developed Applications
ITIS26	Information Security Governance
ITIS27	Auditing IT Governance
ITIS28	Auditing Smart Devices (Understanding and Auditing Smart Devices)
ITIS29	Assessing Cybersecurity Risk: Roles of the Three Lines of Defense
ITIS30	Understanding and Auditing Big Data
ITIS31	Auditing Insider Threat Programs

IT Security in Oil and Gas

ITOG01	IT security in Oil and Gas Pipelines
ITOG02	IT security in Oil and Gas Tank Farms
ITOG03	IT security in Oil and Gas Terminals
ITOG04	IT security in Oil and Gas Exploration & Production
ITOC05	IT socurity in Oil and Cas SCADA

Information Security - NIST Standards

Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio ITIS95 SP 800-221 Enterprise Impacts of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio ITIS96 SP 800-218 Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS95 SP 800-221 Enterprise Impacts of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio ITIS96 SP 800-218 Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio ITIS96 SP 800-218 Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Programs Within an Enterprise Risk Portfolio ITIS96 SP 800-218 Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS96 SP 800-218 Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Recommendations for Mitigating the Risk of Software Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Vulnerabilities ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems Security Guidelines for Storage Infrastructure
ITIS97 SP 800-215 Guide to a Secure Enterprise Network Landscape ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS98 SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Government: IoT Device Cybersecurity Requirement Catalog ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS99 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Government: Establishing IoT Device Cybersecurity Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
Requirements ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS100 SP 800-210 General Access Control Guidance for Cloud Systems ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS101 SP 800-209 Security Guidelines for Storage Infrastructure
ITIS102 SP 800-207 Zero Trust Architecture
ITIS103 SP 800-205 Attribute Considerations for Access Control Systems
ITIS104 SP 800-193 Platform Firmware Resiliency Guidelines
ITIS105 SP 800-192 Verification and Test Methods for Access Control Policies
/Models
ITIS106 SP 800-190 Application Container Security Guide
ITIS107 SP 800-184 Guide for Cybersecurity Event Recovery
ITIS108 SP 800-183 Networks of 'Things'
ITIS109 SP 800-181 Rev. 1 Workforce Framework for Cybersecurity (NICE Framework)
ITIS110 SP 800-177 Rev. 1 Trustworthy Email
ITIS111 SP 800-172A Assessing Enhanced Security Requirements for Controlled
Unclassified Information
ITIS112 SP 800-171A Assessing Security Requirements for Controlled
Unclassified Information
ITIS113 SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices
ITIS114 SP 800-163 Rev. 1 Vetting the Security of Mobile Applications
ITIS115 SP 800-162 Guide to Attribute-Based Access Control (ABAC)
Definition and Considerations

ITIS116	SP 800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
ITIS117	SP 800-160 Vol. 2 Rev. 1	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
ITIS118	SP 800-153	Guidelines for Securing Wireless Local Area Networks (WLANs)
ITIS119	SP 800-150	Guide to Cyber Threat Information Sharing
ITIS120	SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing
ITIS121	SP 800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment
ITIS122	SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
ITIS123	SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
ITIS124	SP 800-125	Guide to Security for Full Virtualization Technologies
ITIS125	SP 800-124 Rev. 2	Guidelines for Managing the Security of Mobile Devices in the Enterprise
ITIS126	SP 800-124 Rev. 1	Guidelines for Managing the Security of Mobile Devices in the Enterprise
ITIS127	SP 800-123	Guide to General Server Security
ITIS128	SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
ITIS129	SP 800-121 Rev. 2	Guide to Bluetooth Security
ITIS130	SP 800-115	Technical Guide to Information Security Testing and Assessment
ITIS131	SP 800-101 Rev. 1	Guidelines on Mobile Device Forensics
ITIS132	SP 800-98	Guidelines for Securing Radio Frequency
		Identification (RFID) Systems
ITIS133	SP 800-95	Guide to Secure Web Services
ITIS134	SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
ITIS135	SP 800-88 Rev. 1	Guidelines for Media Sanitization
ITIS136	SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
ITIS137	SP 800-84	Guide to Test, Training and Exercise Programs for IT Plans and Capabilities
ITIS138	SP 800-83 Rev. 1	Guide to Malware Incident Prevention and Handling for Desktops and Laptops
ITIS139	SP 800-82 Rev. 3	Guide to Operational Technology (OT) Security
ITIS140	SP 800-82 Rev. 2	Guide to Industrial Control Systems (ICS) Security

	SP 800-81-2 SP 800-66 Rev. 2	Secure Domain Name System (DNS) Deployment Guide Implementing the Health Insurance Portability and
		Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide
ITIS143	SP 800-61 Rev. 2	Computer Security Incident Handling Guide
	SP 800-55 Rev. 1	Performance Measurement Guide for Information Security
ITIS145	SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations
ITIS146	SP 800-53B	Control Baselines for Information Systems and Organizations
ITIS147	SP 800-53A Rev. 5	Assessing Security and Privacy Controls in Information Systems and Organizations
ITIS148	SP 800-50	Building an Information Technology Security Awareness and Training Program
ITIS149	SP 800-47 Rev. 1	Managing the Security of Information Exchanges
ITIS150	SP 800-46 Rev. 3	PRE-DRAFT Call for Comments: Guide to Enterprise Telework Security
ITIS151	SP 800-46 Rev. 2	Guide to Enterprise Telework, Remote Access, and Bring your Own Device (BYOD) Security
ITIS152	SP 800-45 Version 2	Guidelines on Electronic Mail Security
ITIS153	SP 800-44 Version 2	Guidelines on Securing Public Web Servers
ITIS154	SP 800-41 Rev. 1	Guidelines on Firewalls and Firewall Policy
ITIS155	SP 800-40 Rev. 4	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
ITIS156	SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
ITIS157	SP 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
ITIS158	SP 800-35	Guide to Information Technology Security Services
ITIS159	SP 800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems
ITIS160	SP 800-30 Rev. 1	Guide for Conducting Risk Assessments
ITIS161	SP 800-28 Version 2	Guidelines on Active Content and Mobile Code
ITIS162	SP 800-18 Rev. 1	Guide for Developing Security Plans for Federal Information Systems
ITIS163	SP 800-16	Information Technology Security Training Requirements: a Role- and Performance-Based Model
ITIS164	SP 800-12 Rev. 1	An Introduction to Information Security

IT Security - ISO27K standards

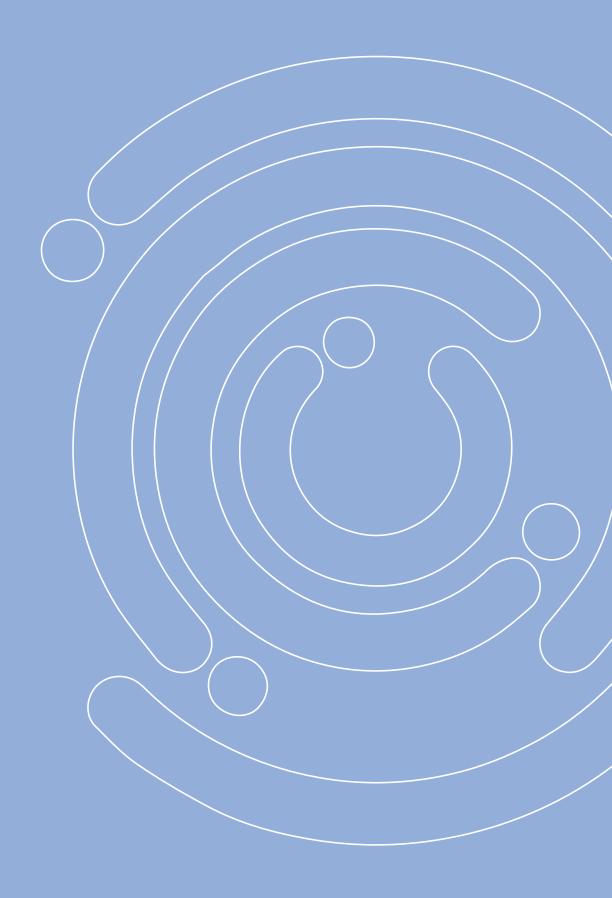
ITIS32		Information security management systems — Overview
ITIS33	ISO/IEC 27001	Information security, cybersecurity and privacy protection — Information security management systems
ITIS34	ISO/IEC 27002	Information security, cybersecurity and privacy protection
ITIS35	ISO/IEC 27003	 — Information security controls Information security management system implementation
		guidance
ITIS36	ISO/IEC 27004	Information security management — Monitoring,
171007	100 = 0 0700	measurement, analysis and evaluation
ITIS37	ISO/IEC 27005	Information security, cybersecurity and privacy protection — Guidance on managing information security risks
ITIS38	ISO/IEC 27006	Requirements for bodies providing audit and certification
	10.0 //= 0.070.7	of information security management systems
ITIS39	ISO/IEC 27007	Guidelines for information security management systems auditing (focused on auditing the management system)
ITIS40	ISO/IEC TR 27008	Guidance for auditors on ISMS controls (focused on
ITIC 41	100/150 07000	auditing the information security controls)
ITIS41	ISO/IEC 27009	Information technology — Security techniques — Sector- specific application of ISO/IEC 27001 — Requirements
ITIS42	ISO/IEC 27010	Information security management for inter-sector and
		inter-organizational communications
ITIS43	ISO/IEC 27011	Information security management guidelines for
		telecommunications organizations based on ISO/IEC 27002
ITIS44	ISO/IEC 27013	Guideline on the integrated implementation of
ITIS45	ISO/IEC 27014	ISO/IEC 27001 and ISO/IEC 20000-1 Information security governance (Based on Australian
111340	130/1LC 2/01 4	e-health.)
ITIS46	ISO/IEC TR 27015	Information security management guidelines for financial
		services
ITIS47	ISO/IEC TR 27016	information security economics
ITIS48	ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ITIS49	ISO/IEC 27018	Code of practice for protection of personally identifiable
		information (PII) in public clouds acting as PII processors
ITIS50	ISO/IEC 27019	Information security for process control in the energy industry
ITIS51	ISO/IEC 27021	Competence requirements for information security
ITIS52	ISO/IEC 27031	management systems professionals Guidelines for information and communication technology
		readiness for business continuity
ITIS53	ISO/IEC 27032	Guideline for cybersecurity
ITIS54	ISO/IEC 27033	Information technology — Security techniques — Network security
		Overview and concepts

- Overview and concepts
- Guidelines for the design and implementation of network security

gateways • Securing communications across networks using Virtual Private ITIS62 ISO/IEC 27034 Guideline for application security Organization normative framework Application security management process Validation and verification (under development) Protocols and application security controls data structure Protocols and application security controls data structure, XML schemas studies ITIS70 ISO/IEC 27035 Principles of incident management Guidelines for ICT incident response operations ITIS74 ISO/IEC 27036 Overview and concepts Requirements supply chain security ITIS79 ISO/IEC 27037 preservation of digital evidence ITIS80 ISO/IEC 27038 ITIS81 ISO/IEC 27039 Storage security ITIS82 ISO/IEC 27040 ITIS83 ISO/IEC 27041 Investigation assurance ITIS84 ISO/IEC 27042 ITIS85 ISO/IEC 27043 ITIS86 ISO/IEC 27050 Electronic discovery Overview and concepts • For governance and management of electronic discovery Code of practice for electronic discovery Technical readiness ITIS91 ISO/IEC TS 27110 ITIS92 ISO/IEC 27701 — Privacy Information Management System (PIMS). Information security management in health using ISO/IEC 27002 ITIS93 ISO 27799 personal health information using ISO/IEC 27002)

Threats, design techniques and control issues

Securing communications between networks using security





London - Duhai

www.educom.co info@educom.co















