

CyBOK Mapping Reference

Issue 1.2

Joseph Hallett | University of Bristol

Lata Nautiyal | University of Bristol

Benjamin Shreeve | University of
Bristol

Awais Rashid | University of Bristol

COPYRIGHT

© Crown Copyright, The National Cyber Security Centre 2020. This information is licensed under the Open Government Licence v3.0. To view this licence, visit:

<http://www.nationalarchives.gov.uk/doc/open-government-licence/> OGL

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK © Crown Copyright, The National Cyber Security Centre 2018, licensed under the Open Government Licence: **<http://www.nationalarchives.gov.uk/doc/open-government-licence/>**.

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at **contact@cybok.org** to let the project know how they are using CyBOK.

INTRODUCTION

This index provides a guide to where various topics are discussed within CyBOK. Reference terms are presented alphabetically, with the knowledge areas most likely to contain the term **shown in red**. If a term is likely to be found in multiple knowledge areas, then all are listed.

Note that this document is just a guide. It was produced by analysing the terms used in other professional bodies of knowledge. We do not claim that it is complete, nor do we guarantee that the knowledge areas we refer to discuss the terms in detail—just that if they are discussed in CyBOK this is where you'll most likely find them.

For the sake of brevity we refer to the knowledge areas through acronyms. The acronyms are expanded below:

Acronym	Knowledge Area
AAA	Authentication, Authorisation & Accountability
AB	Adversarial Behaviours
C	Cryptography
CI	CyBOK Introduction
CPS	Cyber-Physical Systems Security
DSS	Distributed Systems Security
F	Forensics
FMS	Formal Methods for Security
HF	Human Factors
HS	Hardware Security
LR	Law & Regulation
MAT	Malware & Attack Technology
NS	Network Security
OSV	Operating Systems & Virtualisation
PLT	Physical Layer & Telecommunications Security
POR	Privacy & Online Rights
RMG	Risk Management & Governance
SOIM	Security Operations & Incident Management
SS	Software Security
SSL	Secure Software Lifecycle
WAM	Web & Mobile Security

CHANGELOG

2020-03-06. Initial version of the mapping reference 1.1.

2020-10-08. Mapping reference 1.2beta1 including the addition of 115 new terms taken from *introduction* and *formal methods for security* knowledge trees.

2020-12-17. Mapping reference 1.2 including corrections to introduction text and a changelog.

0-9

*PROPERTY AAA
 .NET ARCHITECTURE AAA
 3-DES (TRIPLE DES) C
 3G PLT
 4G (LTE) PLT
 5G PLT

A

ABAC (ATTRIBUTE-BASED ACCESS CONTROL) AAA
 ABSOLUTE ADDRESSES HS
 ABSTRACT INTERPRETATION SS
 ABSTRACTION SSL
 ABUSE CASES SSL
 ACCEPTABLE INTERRUPTION WINDOW (AIW) SOIM
 ACCEPTABLE RISK RMG
 ACCEPTABLE USE POLICY HF
 ACCEPTANCE TESTING SSL
 ACCEPTED WAYS FOR HANDLING RISK RMG
 ACCESS AAA
 ACCESS CONTROL (AC) - LOGICAL AAA
 ACCESS - ABAC (ATTRIBUTE-BASED ACCESS CONTROL) AAA
 ACCESS APPLICATION AAA
 ACCESS CONTROL AAA OSV FMS
 ACCESS CONTROL - ACCESS AAA
 ACCESS CONTROL - CBAC AAA
 ACCESS CONTROL - DAC (DISCRETIONARY ACCESS CONTROL) AAA
 ACCESS CONTROL - DAC (DISCRETIONARY ACCESS CONTROL) - POLICY IMPLEMENTATION AAA
 ACCESS CONTROL - DAC (DISCRETIONARY ACCESS CONTROL) - RSBAC AAA
 ACCESS CONTROL - DEFINITION AAA
 ACCESS CONTROL - LOGICAL AAA
 ACCESS CONTROL - LOGICAL - EXECUTE AAA
 ACCESS CONTROL - LOGICAL - READ AND WRITE AAA
 ACCESS CONTROL - LOGICAL - READ ONLY AAA
 ACCESS CONTROL - MAC (MANDATORY ACCESS CONTROL) AAA
 ACCESS CONTROL - MANAGERIAL AAA
 ACCESS CONTROL - MANAGERIAL - GUIDELINES RMG
 ACCESS CONTROL - MANAGERIAL - POLICY DOCUMENTS RMG
 ACCESS CONTROL - MANAGERIAL - POLICY LIFECYCLE RMG
 ACCESS CONTROL - MANAGERIAL - PROCEDURES RMG
 ACCESS CONTROL - MANAGERIAL - STANDARDS RMG
 ACCESS CONTROL - MATRIX AAA
 ACCESS CONTROL - MODEL AAA
 ACCESS CONTROL - NDAC (NON-DISCRETIONARY ACCESS CONTROL) AAA
 ACCESS CONTROL - OBJECTS AAA
 ACCESS CONTROL - OPERATIONAL OSV
 ACCESS CONTROL - PUBLIC AAA
 ACCESS CONTROL - ROLE-BASED AAA
 ACCESS CONTROL - SUBJECTS AAA
 ACCESS CONTROL - TRBAC AAA
 ACCESS CONTROL IN DISTRIBUTED SYSTEMS AAA
 ACCESS CONTROL LIST AAA
 ACCESS CONTROL LIST (ACL) OSV
 ACCESS CONTROL LISTS OSV
 ACCESS CONTROL LOGICS AAA
 ACCESS CONTROL MATRIX AAA
 ACCESS CONTROL MATRIX - BELL-LAPADULA MODEL AAA
 ACCESS CONTROL MODEL AAA
 ACCESS CONTROL TABLE AAA
 ACCESS DEFINITION AAA
 ACCESS METHOD SOIM
 ACCESS NETWORK NS
 ACCESS PATH OSV
 ACCESS REMOTE DSS
 ACCESS RIGHTS AAA OSV
 ACCESS SYSTEM AAA
 ACCESS/ADMISSION CONTROL & ID MANAGEMENT DSS
 ACCOUNT MANAGEMENT AAA
 ACCOUNT VALIDATION OSV
 ACCOUNTABILITY AAA RMG
 ACCOUNTABILITY - EXTERNAL PROGRAM DRIVERS FOR LR
 ACCOUNTABLE/ACCOUNTABILITY AAA
 ACCREDITATION AAA RMG
 ACCREDITATION - MEASURING NUMBER OF SYSTEMS RMG
 ACCREDITATION - SYSTEM AUTHORIZATION AUTHORITY SOIM
 ACCREDITATION BOUNDARIES - ESTABLISHING RMG
 ACCURACY AS RECOVERY TEST METRIC F
 ACHIEVABLE GOALS RMG
 ACL (ACCESS CONTROL LIST) AAA
 ACPO (ASSOCIATION OF CHIEF POLICE OFFERS) LR
 ACPO GOOD PRACTICE GUIDE FOR DIGITAL EVIDENCE F
 ACQUISITION LIFECYCLE SOIM
 ACQUISITION/DEVELOPMENT PHASE SOIM
 ACQUISITIONS STRATEGY SOIM
 ACT (HIPAA) LR
 ACTION PLAN - FOR IMPLEMENTATION OF INFORMATION SECURITY GOVERNANCE RMG
 ACTION PLAN - FOR INCIDENT MANAGEMENT SOIM
 ACTION PLAN - GAP ANALYSIS AS BASIS FOR SOIM
 ACTIONS ON OBJECTIVES AB MAT

ACTIVE ATTACK AB
 ACTIVE DETECTION CPS
 ACTIVE DIRECTORY DOMAIN SERVICES (ADDS) AAA
 ACTIVE FAULT ATTACKS HS
 ACTIVEX SSL WAM
 ACTOR-ORIENTED APPROACHES RMG
 ACTS OF WAR CPS
 AD HOC MODE NS
 ADAPTATION AB
 ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE SSL
 ADDRESS - BUS OSV
 ADDRESS - RESOLUTION PROTOCOL (ARP) NS
 ADDRESS - SPACE LAYOUT RANDOMIZATION (ASLR) OSV
 ADDRESS BAR MANIPULATION ATTACKS WAM
 ADDRESS RESOLUTION PROTOCOL (ARP) NS
 ADDRESS SPACE NS
 ADDRESS VARIANCE DSS
 ADDRESSING NS
 ADDRESSING - IP NS
 ADDS (ACTIVE DIRECTORY DIRECTORY SERVICE) OSV
 ADHERENCE TO USE CASES SOIM
 ADMINISTRATION OF SECURITY PROGRAMS SOIM
 ADMINISTRATIVE ACTIVITIES SOIM
 ADMINISTRATIVE ACTIVITIES - ACCEPTABLE USE POLICY HF
 ADMINISTRATIVE ACTIVITIES - CULTURE AND REGIONAL VARIANCES LR
 ADMINISTRATIVE ACTIVITIES - ETHICS AS HF LR
 ADMINISTRATIVE ACTIVITIES - FOR INFORMATION SECURITY FRAMEWORK RMG
 ADMINISTRATIVE ACTIVITIES - LEGAL AND REGULATORY REQUIREMENTS AS LR
 ADMINISTRATIVE ACTIVITIES - PLAN-DO-CHECK-ACT AS SOIM
 ADMINISTRATIVE ACTIVITIES - PROGRAM DEVELOPMENT AS RMG
 ADMINISTRATIVE ACTIVITIES - PROGRAM MANAGEMENT EVALUATION RMG
 ADMINISTRATIVE ACTIVITIES - RISK MANAGEMENT AS RMG
 ADMINISTRATIVE ACTIVITIES - SECURITY AWARENESS TRAINING AND EDUCATION HF
 ADMINISTRATIVE ACTIVITIES - SECURITY PROBLEM MANAGEMENT RMG
 ADMINISTRATIVE CONTROLS SOIM
 ADMINISTRATIVE REQUIREMENTS RMG
 ADMISSION INTO EVIDENCE OF ELECTRONIC DOCUMENTS LR
 ADOPTION WAM
 ADS-B PLT
 ADVANCE FEE FRAUD AB
 ADVANCED ENCRYPTION STANDARD (AES) C
 ADVANCED NETWORK SECURITY TOPICS NS
 ADVANCED PERSISTENT THREATS MAT
 ADVANCED PERSISTENT THREATS (APTS) AB
 ADVANCED PROTOCOLS C
 ADWARE MAT
 ADWARE - BOTNETS MAT
 Aead C
 AES C
 AES (ADVANCED ENCRYPTION STANDARD) - CCMP C
 AES (ADVANCED ENCRYPTION STANDARD) - RIJNDAEL C
 AFFILIATE PROGRAMMES AB
 AFTP (ANONYMOUS FILE TRANSFER PROTOCOL) NS
 AGGREGATED RISK RMG
 AGGREGATION OSV
 AGILE AND DEVOPS SSL
 AGREEMENT AAA DSS
 AGREEMENTS - INITIATION OF SOIM
 AH (AUTHENTICATION HEADER) PROTOCOL NS
 AICPA SERVICE ORGANIZATION (SOC) REPORTS RMG
 AICPA/CICA TRUST SERVICES RMG
 AIR TRAFFIC COMMUNICATION NETWORKS PLT
 AIW (ACCEPTABLE INTERRUPTION WINDOW) SOIM
 AIW (ALLOWABLE INTERRUPTION WINDOW) SOIM
 ALARM FATIGUE HF
 ALE (ANNUALIZED LOSS EXPECTANCY) RMG
 ALERT CORRELATION SOIM
 ALERT MESSAGE LAYERS SOIM
 ALERT SITUATION SOIM
 ALERTS IN SECURITY INFORMATION AND EVENT MANAGEMENT SOIM
 ALGEBRAIC ATTACKS C
 ALGORITHMS C HS
 ALGORITHMS - ASYMMETRIC C
 ALGORITHMS - CONFIDENTIAL MESSAGES C
 ALGORITHMS - DIFFIE-HELLMAN C
 ALGORITHMS - ECC (ELLIPTIC CURVE CRYPTOGRAPHY) C
 ALGORITHMS - EL GAMAL C
 ALGORITHMS - ELLIPTIC CURVE CRYPTOSYSTEM C
 ALGORITHMS - ENCRYPTION C
 ALGORITHMS - OPEN MESSAGES C
 ALGORITHMS - RIJNDAEL C
 ALGORITHMS - RSA C
 ALGORITHMS - SYMMETRIC C
 ALIASING SS
 ALIVENESS AAA
 ALLOWABLE INTERRUPTION WINDOW (AIW) SOIM
 ALPHA TESTING SSL
 ALTERNATE FACILITIES SOIM
 ALTERNATE PROCESS SOIM
 ALTERNATE ROUTING NS
 ALTERNATE SITE SELECTION SOIM
 ALTERNATIVE PROCESSING SOIM
 ALTERNATIVE ROUTING NS
 AMBIGUITY ANALYSIS SSL
 AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI) RMG
 AMOUNT AS RECOVERY TEST METRIC F
 ANALYSE: ANALYSIS METHODS SOIM
 ANALYSING THE EVIDENCE AAA
 ANALYSIS - EQUIVALENCE-BASED FMS
 ANALYSIS - GAME-BASED FMS
 ANALYSIS - NETWORK F

ANALYSIS - REFINEMENT-BASED	FMS	ARCHITECTURE - INFORMATION SYSTEMS ARCHITECTURE	SSL
ANALYSIS - SEMANTICS-BASED	FMS	ARCHITECTURE - NETWORK ARCHITECTURE	NS
ANALYSIS - SIMULATION-BASED	FMS	ARCHITECTURE - TRUST ARCHITECTURE - DMZ	NS
ANALYSIS - SOFTWARE	F	ARCHITECTURE - TRUST ARCHITECTURE - EXTRANETS	NS
ANALYSIS ENVIRONMENTS	MAT	ARCHITECTURE - TRUST ARCHITECTURE - INTERNET	WAM
ANALYSIS TECHNIQUES	MAT	ARCHITECTURE - TRUST ARCHITECTURE - INTRANETS	NS
ANALYTIC ATTACK	C	ARCHIVING PROCEDURES	SOIM
ANCHORING IN INFORMATION SECURITY STRATEGY	HF	ARCHITECTURAL RISK ANALYSIS	SSL
ANNUAL LOSS EXPECTANCY (ALE)	RMG	ARM TRUSTZONE	HS OSV
ANNUALIZED LOSS EXPECTANCY (ALE)	RMG	ARP (ADDRESS RESOLUTION PROTOCOL)	NS
ANOMALY DETECTION	SOIM OSV	ARP SPOOFING	NS
ANOMALY MODELS	SOIM	ARPCAN	NS
ANOMALY-BASED IDS	NS	ARREST OF NATURAL PERSONS IN STATE TERRITORY	LR
ANONYMISATION	POR	ARTIFACT ANALYSIS	F
ANONYMITY	FMS	ARTIFACTS AND FRAGMENTS	F
ANONYMOUS COMMUNICATIONS NETWORKS	POR	AS/NZS 4360	RMG
ANONYMOUS FILE TRANSFER PROTOCOL (AFTP)	POR	ASLR	SS OSV
ANONYMOUS FILE TRANSFER PROTOCOL (ANONYMOUS FTP)	NS	ASLR (ADDRESS SPACE LAYOUT RANDOMIZATION)	OSV
ANONYMOUS PETITIONS	POR	ASP (APPLICATION SERVICE PROVIDER)	DSS
ANTI-ANALYSIS AND EVASION TECHNIQUES	MAT	ASSERTIONS	SS
ANTI-COLLISION PROTOCOL (RFID)	HS	ASSESS THE SECURE SOFTWARE LIFECYCLE	SSL
ANTI-MALWARE	OSV	ASSESSING THE EVIDENCE	AAA
ANTI-MALWARE - POLICIES	MAT	ASSESSMENT AND DECISION	RMG
ANTI-MALWARE - SYSTEMS	SOIM	ASSESSMENT CRITERIA	HF
ANTI-MALWARE SOFTWARE	MAT	ASSESSMENT FOCUS	SOIM
ANTI-MALWARE SYSTEMS INCIDENT RESPONSE AND	SOIM	ASSESSMENTS (US NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)	RMG
ANTI-PHISHING TRAINING	WAM	ASSET CLASSIFICATION	RMG
ANTI-SPAM SOFTWARE INCIDENT RESPONSE AND	WAM	ASSET IDENTIFICATION - IN INFORMATION RISK MANAGEMENT PROGRAM	RMG
ANTI-VIRUS SOFTWARE INCIDENT RESPONSE AND	MAT	ASSET IDENTIFICATION - IN RISK ASSESSMENT	RMG
ANTIVIRUS ENGINES	SOIM	ASSET IDENTIFICATION - IN RISK MANAGEMENT PROCESS	RMG
ANTIVIRUS SOFTWARE	MAT	ASSET MANAGEMENT	SOIM
API DESIGN	SS	ASSET OWNERSHIP	SOIM
API USABILITY	HF	ASSET SECURITY	SOIM
API VULNERABILITIES	SS	ASSET SEIZURE AND FORFEITURE	LR
APP DEVELOPMENT AND VULNERABILITIES	HF	ASSET VALUATION	RMG
APPLICATION	WAM	ASSET VALUATION - INTANGIBLE	RMG
APPLE TALK - DATA STREAM PROTOCOL (ADSP)	NS	ASSET VALUATION - TANGIBLE	RMG
APPLE TALK - SESSION PROTOCOL (ASP)	NS	ASSETS	AAA SSL RMG
APPLET	WAM	ASSISTANCE	RMG
APPLICATION	WAM	ASSOCIATION CONTROL SERVICE ELEMENT (ACSE)	NS
APPLICATION - AVAILABILITY	SOIM	ASSURANCE EVALUATION CRITERIA	OSV
APPLICATION - PROGRAMMING INTERFACE (API) - SECURITY	SS	ASSURANCE INTERNET PROTOCOL ENCRYPTOR (HAIBE)	C NS
APPLICATION ARTIFACTS	F	ASSURANCE INTERNET PROTOCOL ENCRYPTOR (HAIBE) - WORK FACTOR	C
APPLICATION CONTROLS	SSL	ASSURANCE PROCESS INTEGRATION - AS OUTCOME OF SECURITY PROGRAMS	SOIM
APPLICATION DEVELOPMENT	SSL	ASSURANCE PROCESS INTEGRATION - AS RESULT OF INFORMATION SECURITY GOVERNANCE	RMG
APPLICATION FORENSICS	F	ASSURANCE PROCESS INTEGRATION - IN INCIDENT MANAGEMENT	SOIM
APPLICATION GATEWAY	NS	ASSURANCE PROCESS INTEGRATION - IN INFORMATION SECURITY GOVERNANCE	RMG
APPLICATION ISOLATION	WAM	ASSURANCE PROVIDERS	RMG
APPLICATION LAYER	NS	ASYMMETRIC	C
APPLICATION LAYER (OSI) - PROTOCOLS	NS	ASYMMETRIC ADVANTAGES AND DISADVANTAGES	C
APPLICATION LAYER (OSI) - WEB-BASED LAYER	NS	ASYMMETRIC ALGORITHM	C
APPLICATION LAYER INTERPRETATION	SOIM	ASYMMETRIC ALGORITHM	C
APPLICATION LOGS: WEB SERVER LOGS AND FILES	SOIM	ASYMMETRIC CRYPTOGRAPHY	C
APPLICATION PROGRAMMING INTERFACE (API)	SS	ASYMMETRIC ENCRYPTION	C
APPLICATION SECURITY CONTROL DEFINITION	SSL	ASYMMETRIC KEY	C
APPLICATION SERVICE PROVIDER (ASP)	DSS	ASYMMETRIC KEY ENCRYPTION	C
APPLICATION SPECIFIC INTEGRATED CIRCUIT (ASIC)	HS	ASYMMETRIC MODE MULTIPROCESSING	C
APPLICATION STORES	WAM	ASYNCHRONOUS TRANSFER MODE (ATM)	NS
APPLICATION SYSTEM TESTING	SSL	ASYNCHRONOUS	C DSS
APPLICATION WHITELISTING	OSV	ASYNCHRONOUS TOKEN GENERATING METHOD	AAA
APPLICATION-LAYER PROTOCOLS	NS	ASYNCHRONOUS ENCRYPTION	SS
APPLICATION-LAYER SECURITY	NS	ASYNCHRONOUS PASSWORD TOKENS	AAA
APPLICATION-LEVEL PROXIES	WAM	ASYNCHRONOUS TIME DIVISION MULTIPLEXING (ATDM)	PLT
APPLICATION-SPECIFIC INTEGRATED CIRCUITS	NS	ASYNCHRONOUS TOKENS	AAA
APPLICATIONS	OSV	ASYNCHRONOUS TRANSFER MODE (ATM)	NS
APPLICATIONS - ACCESS CONTROL AND	OSV	ATOMICITY CONSISTENCY ISOLATION AND DURABILITY (ACID)	OSV
APPLICATIONS - VIRTUALIZATION	OSV	ATTACK	MAT
APPLICATIONS DEVELOPMENT	SSL	ATTACK ATTRIBUTION	SOIM
APPLYING LAW TO CYBERSPACE AND INFORMATION TECHNOLOGIES	LR	ATTACK DETECTION	MAT
APPROACHES TO API BASED RECOVERY	F	ATTACK GRAPHS	AB
APPROVED CRYPTOGRAPHIC ALGORITHMS	HS	ATTACK RESISTANCE ANALYSIS	SSL
APPROVING AUTHORITY - RESPONSIBILITIES OF	SOIM RMG	ATTACK SIGNATURE	MAT
APPROXIMATE ANALYSIS	F	ATTACK SURFACE	OSV
APTS (ADVANCED PERSISTENT THREATS) ATTACKS	AB	ATTACK TREES	AB RMG
ARCHITECTURE - DEFINED	SOIM	ATTACK TYPES	DSS
ARCHITECTURE - DYNAMIC INTERCONNECTIONS WITH	SOIM	ATTACK(S) 802.LQ	MAT
ARCHITECTURE - IN INFORMATION SECURITY APPROACH	RMG	ATTACK(S) ACCESS CONTROL (AC)	AAA
ARCHITECTURE - MEASUREMENT OF TECHNICAL SECURITY	SOIM	ATTACK(S) - ALGEBRAIC	C
ARCHITECTURE - OF SECURITY PROGRAMS	SOIM	ATTACK(S) - ANALYTIC	C
ARCHITECTURE - OF TECHNICAL CONTROLS	SOIM	ATTACK(S) - ARP	MAT
ARCHITECTURAL PRINCIPLES	SOIM	ATTACK(S) - BAITING	AB
ARCHITECTURAL THREATS	CPS	ATTACK(S) - BETWEEN-THE-LINES	SS
ARCHITECTURE	SSL	ATTACK(S) - BIRTHDAY	C
ARCHITECTURE (SABSA)	RMG	ATTACK(S) - CHOSEN-CIPHERTEXT	C
ARCHITECTURE - BELL-LAPADULA MODEL	AAA	ATTACK(S) - CHOSEN-PLAIN TEXT	C
ARCHITECTURE - BIBA MODEL	AAA	ATTACK(S) - CIPHERTEXT-ONLY	C
ARCHITECTURE - BREWER-NASH MODEL	AAA	ATTACK(S) - CROSS-SITE SCRIPTING (XSS)	MAT
ARCHITECTURE - CHINESE WALL MODEL	AAA	ATTACK(S) - CRYPTANALYTIC	C
ARCHITECTURE - CLARK-WILSON MODEL	AAA	ATTACK(S) - DICTIONARY	C
ARCHITECTURE - DESIGN	SOIM	ATTACK(S) - DOUBLE-ENCAPSULATED 802.LQ/NESTED VLAN	MAT
ARCHITECTURE - DESIGN - ACCOUNTABILITY	AAA	ATTACK(S) - FRAGGLE	MAT
ARCHITECTURE - DESIGN - AUTHORIZATION	AAA	ATTACK(S) - IP FRAGMENTATION	MAT
ARCHITECTURE - DESIGN - CONTROLS	SSL	ATTACK(S) - IP FRAGMENTATION - NFS	MAT
ARCHITECTURE - DESIGN - DEFENSE-IN-DEPTH	SSL	ATTACK(S) - IP FRAGMENTATION - OVERLAPPING FRAGMENT	MAT
ARCHITECTURE - DESIGN - DOCUMENTATION	SSL	ATTACK(S) - IP FRAGMENTATION - SMURF AND FRAGGLE	MAT
ARCHITECTURE - DESIGN - LEAST PRIVILEGE	SSL	ATTACK(S) - KNOWN-PLAINTEXT	C
ARCHITECTURE - DESIGN - RISK-BASED CONTROLS	SSL	ATTACK(S) - MAC FLOODING	MAT
ARCHITECTURE - DESIGN - SEPARATION OF DUTIES	SSL	ATTACK(S) - MAN IN THE MIDDLE (MITM)	C
ARCHITECTURE - ENTERPRISE ARCHITECTURE	SSL	ATTACK(S) - MULTICAST BRUTE FORCE	MAT
ARCHITECTURE - GRAHAM-DENNING MODEL	AAA	ATTACK(S) - PARKING LOT	AB
ARCHITECTURE - HARRISON-RUZZO-ULLMAN MODEL	AAA		

CAPACITY MANAGEMENT	SOIM	CHANGEOVER TECHNIQUE/GO-LIVE TECHNIQUE	SOIM
CAPACITY PLANNING	NS	CHANGES - RESPONDING TO	SOIM
CAPEC	SOIM	CHANGES - TRACKING IN THE ENVIRONMENT	SOIM
CAPTCHA SOLVING SERVICES	AB	CHANNEL - OF ATTACK	NS
CAPTCHAS	HF	CHANNEL SERVICE UNIT/DIGITAL SERVICE UNIT (CSU/DSU)	PLT
CARD READERS CONTACTLESS	HS	CHARACTERISATION OF ADVERSARIES	AB
CARD SKIMMING	AB	CHARACTERISTIC EXAMPLES	DSS
CARD TYPES	HS	CHARACTERISTICS	CPS DSS
CARDHOLDER UNIQUE IDENTIFIER (CHUID)	SOIM	CHARACTERISTICS OF GOOD METRICS	RMG
CARO (COMPUTER ANTIVIRUS RESEARCH ORGANIZATION)	MAT	CHECK DIGIT	AAA
CARRIER SENSE MULTIPLE ACCESS (CSMA)	PLT	CHECKING COMPLIANCE	SS
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA)	PLT	CHECKLIST TEST	SOIM
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)	PLT	CHECKSUM	C
CARRIER SENSE MULTIPLE ACCESS/COLLISION DETECTION (CSMA/CD)	NS	CHIEF EXECUTIVE OFFICER RESPONSIBILITIES OF	RMG
CARVING TECHNIQUES	F	CHIEF INFORMATION OFFICER (CIO)	RMG
CASBS (CLOUD ACCESS SECURITY BROKERS)	AAA	CHIEF INFORMATION SECURITY OFFICER (CISO)	RMG
CASCADING RISK	RMG	CHIEF RISK OFFICER (CRO)	RMG
CASCADING STYLE SHEETS (CSS)	WAM	CHIEF SECURITY OFFICER (CSO)	RMG
CASE STUDY - INCIDENT MANAGEMENT	SOIM	CHIEF TECHNOLOGY OFFICER (CTO)	RMG
CASE STUDY - INFORMATION SECURITY GOVERNANCE	RMG	CHILD PREDATION	AB
CASE STUDY - RISK MANAGEMENT	RMG	CHILDREN	HF
CAST	C	CHINESE WALL MODEL	AAA
CATALOGUE OF INTELLECTUAL PROPERTY RIGHTS	LR	CHIP-OFF TECHNIQUES	F
CATEGORIES OF VULNERABILITIES	SS	CHIRPING	PLT
CAUSAL CONSISTENCY	DSS	CHOSEN CIPHERTEXT ATTACK	C
CBAC (CONTEXT-BASED ACCESS CONTROL)	AAA	CHOSEN MESSAGE ATTACK	C
CBC	C	CHOSEN PLAINTEXT ATTACKS	C
CBC (CIPHER BLOCK CHAINING) BLOCK CIPHER MODE	C	CHOSEN-CIPHERTEXT ATTACK	C
CBC-MAC	C	CHOSEN-PLAINTEXT ATTACK	C
CBK - APPLYING SECURITY CONTROLS	SOIM	CIA TRIAD (CONFIDENTIALITY INTEGRITY AVAILABILITY)	MAT CI
CBK - ASSESSING SECURITY CONTROLS	SOIM	CICUIT LEVEL TECHNIQUES	HS
CBK - AUTHORIZING INFORMATION SYSTEMS	SOIM	CIDR (CLASSLESS INTER-DOMAIN ROUTING)	NS
CBK - CATEGORIZATION OF INFORMATION SYSTEMS	SOIM RMG	CIFS (COMMON INTERNET FILE SYSTEM)	OSV
CBK - MONITORING SECURITY CONTROLS	SOIM	CIM	SOIM
CCMP (CIPHER BLOCK CHAINING MESSAGE AUTHENTICATION CODE PROTOCOL)	C	CIO RESPONSIBILITIES OF	RMG
CDAC (CONTENT-DEPENDENT ACCESS CONTROL)	AAA	CIPHER(S)	C
CDM (CONTINUOUS DIAGNOSTICS AND MITIGATION)	SOIM	CIPHER(S) - BLOCK	C
CEE	SOIM	CIPHER(S) - BLOCK - MODES	C
CEF	SOIM	CIPHER(S) - BLOCK - MODES - CHAINING	C
CELL LAYOUT	HS	CIPHER(S) - BLOCK - MODES - COUNTER	C
CELLULAR DIGITAL PACKET DATA (CDPD)	PLT	CIPHER(S) - BLOCK - MODES - FEEDBACK	C
CELLULAR NETWORKS	PLT	CIPHER(S) - BLOCK - MODES - FEEDBACK - OUTPUT FEEDBACK	C
CENSORSHIP RESISTANCE AND FREEDOM OF SPEECH	POR	CIPHER(S) - BLOCK - MODES - STREAM	C
CENTER FOR INTERNET SECURITY (CIS)	RMG	CIPHER(S) - MONOALPHABETIC	C
CENTRAL IRT	SOIM	CIPHER(S) - NULL	C
CENTRALIZED APPROACH TO INFORMATION SECURITY	RMG	CIPHER(S) - PLAYFAIR	C
CERT/CC (COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER)	SOIM	CIPHER(S) - POLYALPHABETIC	C
CERTIFICATE	AAA	CIPHER(S) - RUNNING KEY	C
CERTIFICATE (CERTIFICATION) AUTHORITY (CA)	C	CIPHER(S) - SCYTAL	C
CERTIFICATE AUTHORITIES	NS	CIPHER(S) - STREAM	C
CERTIFICATE AUTHORITY (CA)	C	CIPHER(S) - STREAM-BASED	C
CERTIFICATE REVOCATION LIST (CRL)	C	CIPHER(S) - SUBSTITUTION	C
CERTIFICATE TRANSPARENCY	AAA	CIPHER(S) - TRANSPOSITION	C
CERTIFICATE(S)	C	CIPHERTEXT	C
CERTIFICATE(S) - CERTIFICATE AUTHORITY (CA)	C	CIPHERTEXT - CHOSEN	C
CERTIFICATE(S) - CERTIFICATE AUTHORITY (CA) - HIERARCHIES	AAA C	CIPHERTEXT-ONLY ATTACK	C
CERTIFICATE(S) - CHAINS	AAA C	CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION	AAA
CERTIFICATE(S) - CLIENT SSL	AAA	CIRCUIT-LEVEL GATEWAY	NS
CERTIFICATE(S) - ISSUING	AAA C	CIRCUIT-SWITCHED NETWORK	NS
CERTIFICATE(S) - MANAGING	AAA C	CIRCUIT-SWITCHED NETWORKS	NS
CERTIFICATE(S) - OBJECT-SIGNING	AAA	CIRCULAR A-130 - SENSITIVITY DEFINITION IN	LR
CERTIFICATE(S) - REPLACEMENT	C	CIRCUMVENTING COPYRIGHT TECHNOLOGICAL PROTECTION MEASURES	LR
CERTIFICATE(S) - REVOCATION LIST (CRL)	C	CIS (CENTER FOR INTERNET SECURITY)	RMG
CERTIFICATE(S) - S/MIME	AAA	CIS SECURITY METRICS	RMG
CERTIFICATE(S) - SERVER SSL	AAA	CISM CERTIFICATION	RMG
CERTIFICATE-BASED AUTHENTICATION	AAA	CISO - CREATION OF SECURITY PROCEDURES LIBRARY BY; 194	RMG
CERTIFICATES	C	CISO - DEFINITION OF CERTIFICATION PACKAGE REQUIREMENTS BY	RMG
CERTIFICATION	SOIM	CISO - DEVELOPMENT OF PROGRAM DOCUMENTATION BY	RMG
CERTIFICATION - AUTHORITY	C	CISO - DEVELOPMENT OF SYSTEM AUTHORIZATION WORK GROUP	RMG
CERTIFICATION - PROGRAMS	RMG	CISO - ESTABLISHING ACCREDITATION BOUNDARIES	RMG
CERTIFICATION - TEST PLAN DEVELOPMENT	SOIM	CISO - MANAGING PROGRAM ACTIVITIES	SOIM
CERTIFICATION AND ACCREDITATION (C&A)	LR	CISO - MEASURING PROGRAM PROGRESS	RMG
CERTIFICATION AUTHORITY	C	CISO - MONITORING COMPLIANCE	RMG
CERTIFICATION LEVELS OF EFFORT	RMG	CISO - PROGRAM INTEGRATION	RMG
CERTIFICATION PACKAGE - RESPONSIBILITY OF CISO FOR CONTENTS OF	RMG	CISO - PROGRAM OVERSIGHT	RMG
CERTIFICATION PRACTICE STATEMENT (CPS)	C	CISO - PROVIDING ADVICE AND ASSISTANCE	SOIM RMG
CERTIFICATION TEST PLAN DEVELOPMENT OF	SOIM	CISO - RESPONDING TO CHANGES	RMG
CERTIFICATION TESTING	SOIM	CISO - RESPONSIBILITIES OF	RMG
CERTIFICATION TESTING - CREATION OF RISK REMEDIATION PLANS FOLLOWING	SOIM	CISO - ROLE OF IN CONTINUOUS MONITORING	RMG
CERTIFICATION TESTING - DOCUMENTING RESULTS OF	SOIM	CISO - SYSTEM INVENTORY PROCESS RESPONSIBILITY OF	RMG
CERTIFICATION TESTING - EXECUTION OF	SOIM	CISO - SYSTEM INVENTORY VALIDATION	SOIM RMG
CERTIFICATION TESTING - ROLE OF HOST ORGANIZATION	SOIM	CISO - WORKING WITH UPPER MANAGEMENT	RMG
CERTIFICATION TESTING - SCOPE OF	SOIM	CISOS AND ANALYSTS	SOIM
CERTIFYING AGENT - INDEPENDENCE OF	SOIM	CISSP CERTIFICATION	RMG
CERTIFYING AGENT - RESPONSIBILITIES OF	SOIM	CIVIL LAW	LR
CERTIFYING PUBLIC KEY	C	CIVIL LIABILITY	LR
CFB	C	CLARK-WILSON	AAA
CFB (CIPHER FEEDBACK) BLOCK CIPHER MODE	C	CLARK-WILSON MODEL	AAA
CHAIN OF CUSTODY	F	CLASSES OF DISRUPTIONS	DSS
CHAIN OF EVIDENCE	F	CLASSES OF DISTRIBUTED SYSTEMS	DSS
CHALLENGE RESPONSE TOKENS	AAA	CLASSES OF VULNERABILITIES & THREATS	DSS
CHALLENGE/RESPONSE	AAA	CLASSIFICATION	LR
CHALLENGES OF LIVE FORENSICS	F	CLASSIFICATIONS OF JAMMERS	PLT
CHANGE - MANAGEMENT	SSL	CLASSIFY INFORMATION	SOIM
CHANGE CONTROL	SSL	CLASSLESS INTERDOMAIN ROUTING (CIDR)	NS
CHANGE MANAGEMENT DOCUMENTATION	SOIM	CLEAR ABSTRACTION	CI
CHANGE PERMISSIONS PERMISSION	OSV	CLEARING	SOIM
CHANGE RISK	RMG	CLEARTEXT	C
CHANGEOVER TECHNIQUE - ABRUPT CHANGEOVER	SOIM	CLICK FRAUD	AB
CHANGEOVER TECHNIQUE - PARALLEL CHANGEOVER	SOIM	CLICK FRAUD BOTNETS	AB MAT
CHANGEOVER TECHNIQUE - PHASED CHANGEOVER	SOIM	CLICKJACKING	WAM

CLIENT SIDE STORAGE	WAM	COMMAND AND CONTROL	AB MAT
CLIENT SIDE VULNERABILITIES AND MITIGATIONS	WAM	COMMAND AND CONTROL INFRASTRUCTURE	AB
CLIENT-BASED VULNERABILITIES	NS	COMMAND AND CONTROL TAKEDOWN	MAT
CLIENT-SERVER MODEL	DSS	COMMAND INJECTION	WAM
CLIENT-SERVER MODELS	DSS	COMMAND INJECTION VULNERABILITIES	SS
CLIENT-SIDE VALIDATION	WAM	COMMERCIAL LIABILITY (INSURANCE COVERAGE)	SOIM
CLOUD-NATIVE ARTIFACTS	F	COMMIT PROTOCOLS	DSS
CLOCK SKEW	PLT	COMMITMENT CONCURRENCY AND RECOVERY (CCR)	NS
CLOSED TRADING AND PAYMENT SYSTEMS	LR	COMMITTED INFORMATION RATE (CIR)	DSS
CLOSEST VECTOR PROBLEM	C	COMMITTEE OF SPONSORING ORGANIZATIONS (COSO)	RMG
CLOUD - COMPUTING - SERVICES	DSS	COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)	RMG
CLOUD ACCESS SECURITY BROKERS (CASBS)	AAA	COMMON - INTERNET FILE SYSTEM (CIFS)	NS
CLOUD COMPUTING	SSL DSS	COMMON - MANAGEMENT INFORMATION PROTOCOL (CMIP)	NS
CLOUD COMPUTING - CLASSIFICATION OF DATA	LR	COMMON - OBJECT REQUEST BROKER ARCHITECTURE (COREA)	SS
CLOUD COMPUTING - CONTROLS	DSS	COMMON CONTROL PROVIDER (CCP)	SOIM RMG
CLOUD COMPUTING - DEPLOYMENT MODELS	DSS	COMMON CONTROL PROVIDER - RESPONSIBILITIES OF	RMG
CLOUD COMPUTING - DLP (DATA LEAKAGE PREVENTION)	DSS	COMMON CONTROLS	SOIM
CLOUD COMPUTING - ENCRYPTION AND	DSS	COMMON CONTROLS - IDENTIFICATION OF	SOIM
CLOUD COMPUTING - ENCRYPTION AND - ALTERNATIVES	DSS	COMMON CRITERIA	SSL
CLOUD COMPUTING - EVENTS - ANALYSIS	SOIM	COMMON CRITERIA AND EMVCO	HS
CLOUD COMPUTING - EVENTS - LOGGING	DSS	COMMON GATEWAY INTERFACE (CGI)	WAM
CLOUD COMPUTING - EVENTS - SOURCES	DSS	COMMON LOG FORMAT	SOIM
CLOUD COMPUTING - EVENTS - STORAGE	SOIM	COMMON NETWORK ATTACKS	NS
CLOUD COMPUTING - LEGAL CONCERNS	LR	COMMON OBJECT REQUEST BROKER ARCHITECTURE (CORBA)	DSS
CLOUD COMPUTING - NETWORK ACCESS	DSS	COMMON REFERENCE STRINGS	C
CLOUD COMPUTING - P&DP (PRIVACY AND DATA PROTECTION)	LR	COMMON VULNERABILITIES AND EXPOSURES (CVE)	SOIM
CLOUD COMPUTING - PRIVACY CONCERNS	POR	COMMUNICATE	RMG
CLOUD COMPUTING - RESOURCE POOLING	DSS	COMMUNICATION	SOIM
CLOUD COMPUTING - SERVICE MODELS - IAAS	DSS	COMMUNICATION (H.245)	NS
CLOUD COMPUTING - SERVICE MODELS - PAAS	DSS	COMMUNICATION - AND RISK MONITORING	RMG
CLOUD COMPUTING - SERVICE MODELS - SAAS	DSS	COMMUNICATION - FOR INCIDENT RESPONSE	SOIM
CLOUD COMPUTING - STORAGE	DSS	COMMUNICATION - IN INCIDENT MANAGEMENT	SOIM
CLOUD COMPUTING - STORAGE - THREATS	DSS	COMMUNICATION - INCIDENT RESPONSE AND	SOIM
CLOUD COMPUTING - TRANSMISSION OF DATA	DSS	COMMUNICATION - MEASUREMENT OF	SOIM
CLOUD COMPUTING - VIRTUALIZATION	OSV	COMMUNICATION - OF RISK	RMG
CLOUD CONTROL MATRIX	RMG	COMMUNICATION - RISK OF	RMG
CLOUD FORENSICS	F	COMMUNICATION CHANNELS	SOIM
CLOUD MODEL	DSS	COMPARTMENTALISATION	SS
CLOUD SERVICE PROVIDERS	DSS	COMPARTMENTALIZATION	SOIM
CLOUD-NATIVE ARTIFACTS	F	COMPENSATING CONTROL	SOIM
CLOUDS	DSS	COMPLETE MEDIATION	CI
CLUSTER COMMUNICATION	DSS	COMPLETENESS	SS
CLUSTERING TECHNIQUES	POR	COMPLIANCE	SOIM RMG
CM (CONFIGURATION MANAGEMENT)	SSL	COMPLIANCE - ENFORCEMENT OF IN INFORMATION SECURITY STRATEGY	SOIM
CM (CONFIGURATION MANAGEMENT) - ACCOUNTING	SSL	COMPLIANCE - IN GOVERNANCE RISK MANAGEMENT AND COMPLIANCE	RMG
CM (CONFIGURATION MANAGEMENT) - AUDITING	SSL	COMPLIANCE - IN SECURITY PROGRAM MANAGEMENT	SOIM
CM (CONFIGURATION MANAGEMENT) - CONTROL	SSL	COMPLIANCE - IN SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
CM (CONFIGURATION MANAGEMENT) - DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS)	NS	COMPLIANCE - LEGISLATIVE AND REGULATORY	LR
CM (CONFIGURATION MANAGEMENT) - IDENTIFICATION	SSL	COMPLIANCE - MEASUREMENT OF	HF RMG
CM (CONFIGURATION MANAGEMENT) - SSH (SECURE SHELL)	SOIM	COMPLIANCE - MONITORING	SOIM
CM (CONFIGURATION MANAGEMENT) - TOOLS	SSL	COMPLIANCE - MONITORING AND ENFORCEMENT OF	SOIM
CMAC (CIPHER MESSAGE AUTHENTICATION CODE)	C	COMPLIANCE - PRIVACY REQUIREMENTS	LR
CME (COMMON MALWARE ENUMERATION)	MAT	COMPLIANCE - SECURITY PROCEDURES	SOIM
CMM	C	COMPLIANCE BUDGET	HF
CMMI (CAPABILITY MATURITY MODEL INTEGRATION)	RMG	COMPLIANCE FATIGUE	HF
CNSS	LR	COMPLIANCE TESTING	SOIM
CNSS - NATIONAL SECURITY SYSTEM REQUIREMENTS	RMG	COMPONENT VS SYSTEMS PRESPECTIVES	RMG
COAXIAL CABLE	PLT	COMPONENTS OF NETWORKS	NS
COBIT	RMG	COMPREHENSIVE GOALS	RMG
COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY)	RMG	COMPRESSION VIRUSES	MAT
COBIT - AS INFORMATION SECURITY METRIC	RMG	COMPROMISE OF ACCESS/ADMISSION CONTROL	DSS
COBIT - DEFINED	RMG	COMPROMISE OF BROKER	DSS
COBIT - FOR CLOUD COMPUTING	RMG	COMPROMISE OF COMMUNICATION	DSS
COBIT - FOR INFORMATION SECURITY STRATEGY	RMG	COMPROMISE OF RESOURCES	DSS
COBIT - FOR RISK ASSESSMENT	RMG	COMPROMISE OF SCHEDULER	DSS
COBIT - FOR RISK MANAGEMENT	RMG	COMPROMISE OF VM	DSS
COBIT - FOR SECURITY PROGRAMS	RMG	COMPROMISE ON MONITORING AND ACCOUNTING	DSS
COBIT - IN INFORMATION SECURITY STRATEGY DEVELOPMENT	RMG	COMPROMISE RECORDING	CI
COBIT - SECURITY ARCHITECTURE FRAMEWORK OF	RMG	COMPROMISING INTERENT-CONNECTED DEVICES	AB
COBIT 4.1 AND EARLIER	RMG	COMPUTATIONAL AND SYMBOLIC METHODS	CI
COCOMO	RMG	COMPUTATIONAL MODELLING	CI
CODE AND DATA INTEGRITY CHECKS	OSV	COMPUTER CRIME	LR
CODE CORRUPTION ATTACKS	SS	COMPUTER ETHICS INSTITUTE (CEI)	HF
CODE EMULATION	MAT	COMPUTER FORENSICS	F
CODE GENERATORS	SS	COMPUTER MISUSE ACT	F
CODE OF CONDUCT	HF	COMPUTER SECURITY ACT	LR
CODE OF ETHICS	POR	COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)	SOIM
CODE REPOSITORIES - SECURITY	SSL	COMPUTER-AIDED SOFTWARE ENGINEERING (CASE)	SSL
CODE REPOSITORIES - SECURITY - OPERATIONAL SECURITY	SOIM	COMPUTER/CYBER CRIME - CHILD PORNOGRAPHY SCAREWARE	MAT
CODE REPOSITORIES - SECURITY - SOFTWARE SECURITY	SOIM	COMPUTER/CYBER CRIME - CITADEL RANSOM WARE	MAT
CODE REPOSITORIES - SECURITY - SYSTEM SECURITY	OSV	COMPUTER/CYBER CRIME - CRYPTOLOCKER RANSOM WARE	MAT
CODE REVIEW	SSL	COMPUTER/CYBER CRIME - FAKE OR ROGUE ANTI-VIRUS SOFTWARE	MAT
CODE REVIEW (TOOLS)	SSL	COMPUTING - CLOUD - CHARACTERISTICS	DSS
CODE-BASED ACCESS CONTROL	AAA	COMPUTING - GRID	DSS
CODECS HOSTILE	MAT	CONCEALMENT CIPHER	C
CODES OF CONDUCT	LR	CONCENTRATORS	PLT
CODING GUIDELINES	SS	CONCEPTUAL MODELS	F
CODING PRACTICES	SS	CONCOLIC EXECUTION	MAT
CODING STANDARDS	SSL	CONCURRENCY	SS
COGNITIVE PASSWORDS	AAA	CONCURRENCY BUGS	SS
COGNITIVE TASK MODEL	F	CONCURRENCY BUGS AND DOUBLE FETCH	OSV
COHERENT AND UNMODIFIED MESSAGE CONTENTS	PLT	CONDUCT	RMG
COHERENT BUT MODIFIED MESSAGE CONTENTS	PLT	CONDUCTING THE BUSINESS IMPACT ANALYSIS (BIA)	SOIM
COLD SITE	SOIM	CONFIDENTIAL DATA DISPOSAL OF	POR
COLLABORATIVE COMPUTATION	POR	CONFIDENTIAL DATA SENSITIVITY	POR
COLLECTABILITY	PLT	CONFIDENTIALITY	SOIM POR MAT CI FMS
COLLISION	C	CONFIDENTIALITY INTEGRITY AND AVAILABILITY	DSS
COLLISIONS - ENCRYPTION	C	CONFIDENTIALITY LEVEL (CL)	AAA
COLLUSION	AB	CONFIGURATION MANAGEMENT	SOIM SSL
COLLUSION ATTACKS	DSS	CONFIGURATION MANAGEMENT/CONFIGURATION CONTROL	SSL

CONFIRMATION BIAS	HF	CONTROLS - TECHNICAL - IDENTIFICATION	AAA
CONFLICT OF LAW – CONTRACTS	LR	CONTROLS - TECHNICAL - LOGICAL	AAA
CONFLICT OF LAW – ELECTRONIC SIGNATURES AND TRUST SERVICES	LR	CONTROLS - TECHNICAL - PUBLIC ACCESS	AAA
CONFUSED DEPUTY ATTACKS	WAM	CONTROLS - TESTING	SOIM
CONFUSION	C	CONTROLS - VALIDATION	SOIM
CONSENSUS	AAA DSS	CONTROLS - WITH ARCHITECTURE	SOIM
CONSERVATIVE CONTROL	CPS	CONTROLS POLICY	SOIM
CONSISTENCY	DSS	CONVERGED COMMUNICATIONS	NS
CONSTANT	PLT	CONVERGED COMMUNICATIONS - FCOE (FIBRE CHANNEL OVER ETHERNET)	NS
CONSTANT TIME EXECUTION	HS	CONVERGED COMMUNICATIONS - ISCSI (INTERNET SMALL COMPUTER SYSTEM INTERFACE)	CPS
CONSTITUENCY FOR INCIDENT MANAGEMENT	SOIM	CONVERGED COMMUNICATIONS - MPLS (MULTI-PROTOCOL LABEL SWITCHING)	NS
CONSTRAINED DELEGATION	AAA	COOKIE-BASED TECHNIQUES	POR
CONSTRAINED RBAC	AAA	COOKIES	WAM F
CONSTRAINING ACTUATION	CPS	COORDINATED	MAT
CONSTRAINTS IN INFORMATION SECURITY STRATEGY DEVELOPMENT	SOIM	COORDINATED CLUSTERING ACROSS DISTRIBUTED RESOURCES AND SERVICES	DSS
CONSTRUCTIONS BASED ON ELLIPTIC CURVES	C	COORDINATED RESOURCES CLUSTERING	DSS
CONSTRUCTIONS BASED ON RSA	C	COORDINATED SPREAD SPECTRUM TECHNIQUES	PLT
CONSTRUCTIVE COST MODEL (COCOMO)	RMG	COORDINATING IRT	SOIM
CONSUMER CHOICE	CPS	COORDINATION CLASSES AND ATTACKABILITY	DSS
CONTACTLESS CARD READERS	HS	COORDINATION OF RESOURCES VS COORDINATION OF RESOURCES	DSS
CONTAINERS	OSV	COORDINATION PRINCIPLES	DSS
CONTAINMENT IN INCIDENT RESPONSE PLAN	SOIM	COPYRIGHT	LR
CONTENT - DISTRIBUTION NETWORKS	DSS	COQ	FMS
CONTENT FILTERING	WAM	CORE CONCEPTS	AAA
CONTENT GENERATION	AB	CORE REGULATORY PRINCIPLES	LR
CONTENT ISOLATION	WAM	CORPORATE GOVERNANCE	RMG
CONTENT SECURITY POLICY (CSP)	WAM	CORPORATE NETWORKS	CPS
CONTENT-BASED ACCESS	AAA	CORPORATE SECURITY	RMG
CONTEXT-BASED ACCESS	AAA	CORPORATE SECURITY POLICY	RMG
CONTEXTUAL INQUIRY	HF	CORRECT IMPLEMENTATION	SS
CONTINGENCY PLAN	SOIM	CORRECT USE	SS
CONTINUITY MANAGEMENT	RMG	CORRECTIVE ACTION - INCLUSION OF IN RISK REMEDIATION PLAN	SOIM
CONTINUOUS AND INTERMITTENT SIMULATION (CIS)	RMG	CORRECTIVE ACTION - VALIDATING	SOIM
CONTINUOUS AUDITING	RMG	CORRECTIVE CONTROLS	SSL
CONTINUOUS AUTHENTICATION	AAA	CORRELATION BETWEEN ALERTS	SOIM
CONTINUOUS MONITORING	SOIM	CORRELATION BETWEEN ALERTS AND EXTERNAL SERVICES	SOIM
CONTINUOUS MONITORING - CONFIGURATION MANAGEMENT/CONFIGURATION CONTROL	SOIM	CORRELATION BETWEEN ALERTS AND THE ENVIRONMENT	SOIM
CONTINUOUS MONITORING - INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) STRATEGY	SOIM	CORRELATION IN SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
CONTRACT	LR	CORRESPONDENCE PROPERTIES	AAA
CONTRACTS	SS	COSO (COMMITTEE OF SPONSORING ORGANIZATIONS)	RMG
CONTRIBUTION OF SIEM TO ANALYSIS AND DETECTION	SOIM	COST-BENEFIT ANALYSIS	RMG
CONTROL	SOIM POR CPS RMG	COST-EFFECTIVENESS	RMG
CONTROL ACTIVITIES	RMG	COSTS - AS INFORMATION SECURITY STRATEGY CONSTRAINT	RMG
CONTROL ANALYSIS	RMG	COSTS - LOWERING WITH CLOUD COMPUTING	DSS
CONTROL CENTER	SOIM	COSTS - METRICS FOR MEASURING	RMG
CONTROL FLOW INTEGRITY	SS HS	COSTS - OF RISK ASSESSMENT	RMG
CONTROL FUNCTIONS	SOIM	COTTONMOUTH	HS MAT
CONTROL IMPLEMENTATION	SOIM	COUNTER MODE WITH CIPHER BLOCK CHAINING MESSAGE AUTHENTICATION CODE PROTOCOL (CCMP)	C
CONTROL MATRIX	AAA	COUNTERMEASURE SELECTION	SOIM
CONTROL MONITORING	SOIM	COUNTERMEASURES	HS PLT
CONTROL OBJECTS FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)	RMG	COUNTERMEASURES - DEFINED	MAT
CONTROL RECOMMENDATIONS	RMG	COUNTERMEASURES - FOR INFORMATION SECURITY STRATEGY	SOIM
CONTROL REQUIREMENTS	SOIM RMG	COUNTERMEASURES - FOR SECURITY PROGRAMS	MAT
CONTROL RISK	RMG	COUNTERMEASURES - IN RISK MANAGEMENT	RMG
CONTROL SELF-ASSESSMENT (CSA)	SOIM	COUNTERMEASURES - IN SECURITY PROGRAM MANAGEMENT	SOIM
CONTROL TECHNOLOGY CATEGORIES	OSV	COVERAGE - CONDITION	SS
CONTROL TYPES	SOIM	COVERAGE - DATA FLOW	SS
CONTROL(S) - ADMINISTRATIVE	SOIM	COVERAGE - DECISION (BRANCH)	SS
CONTROL(S) - ASSESSMENT/MONITORING	SOIM	COVERAGE - LOOP	SS
CONTROL(S) - COMPENSATING	SOIM	COVERAGE - MULTI-CONDITION	SS
CONTROL(S) - CORRECTIVE	SOIM	COVERAGE - PATH	SS
CONTROL(S) - DATA SECURITY	SOIM	COVERAGE - STATEMENT	SS
CONTROL(S) - DETECTIVE	SOIM	COVERT CHANNEL(S)	SS
CONTROL(S) - DETERRENT	SOIM	COVERT CHANNEL(S) - CONTROLS	SS
CONTROL(S) - DIRECTIVE	SOIM	COVERT CHANNEL(S) - STORAGE CHANNELS	SS
CONTROL(S) - FRAMEWORKS - COMPREHENSIVE	AAA	COVERT CHANNEL(S) - TIMING CHANNELS	SS
CONTROL(S) - FRAMEWORKS - CONSISTENT	SOIM	COVERT CHANNELS	SS
CONTROL(S) - FRAMEWORKS - MEASURABLE	SOIM	CPS DOMAINS	CPS
CONTROL(S) - FRAMEWORKS - MODULAR	AAA	CRAFTED PACKETS	MAT
CONTROL(S) - FRAMEWORKS - STANDARDIZED	SOIM	CRAFTED PACKETS - SOURCE ROUTING EXPLOITATION	MAT
CONTROL(S) - FUNCTIONS	SOIM	CRAMM (CCTA RISK ANALYSIS AND MANAGEMENT METHOD)	RMG
CONTROL(S) - LAYER	NS	CRC (CYCLICAL REDUNDANCY CHECK)	C
CONTROL(S) - LOGICAL (TECHNICAL)	SOIM	CREATE FILES/WRITE DATA PERMISSION	OSV
CONTROL(S) - PREVENTATIVE	SOIM	CREATE FOLDERS/APPEND DATA PERMISSION	OSV
CONTROL(S) - RECOVERY	SOIM	CREATE OR IMPORT A CODESIGNING CERTIFICATE	WAM MAT
CONTROL(S) - SERVER	NS	CREATION OF CONFIDENCE	RMG
CONTROL(S) - TYPES	SOIM	CREATIVE SECURITY ENGAGEMENTS	HF
CONTROL-FLOW HIJACK ATTACKS	SS	CREDENTIAL	AAA
CONTROL-FLOW INTEGRITY	OSV	CREDENTIAL HARVESTER ATTACK METHOD	MAT
CONTROL-FLOW RESTRICTIONS	OSV	CREDENTIAL MANAGEMENT SYSTEMS	OSV
CONTROLLER AND PROCESSOR	LR	CREDIT CARD PROCESSORS	AB
CONTROLS	SOIM SSL	CREDIT CARD SAFETY	SOIM
CONTROLS - ANALYSIS OF	SOIM	CRIME - COMPUTER	HF
CONTROLS - AS STRATEGY IMPLEMENTATION RESOURCES	SOIM	CRIME - SCENE	F
CONTROLS - CATEGORIES OF	SOIM	CRIME SCRIPTING	AB
CONTROLS - DEFINED	SOIM	CRIMES AGAINST INFORMATION SYSTEMS	LR
CONTROLS - DESIGN	SSL	CRIMINAL LAW	LR
CONTROLS - FOR INFORMATION SECURITY STRATEGY	SOIM	CRIMINAL LIABILITY	LR
CONTROLS - FOR SECURITY PROGRAMS	SOIM	CRITICAL FUNCTION LAYER	SOIM
CONTROLS - FUNCTIONALITY VERSUS EFFECTIVENESS	SOIM	CRITICAL INFORMATION INFRASTRUCTURE ACT OF 2002	LR
CONTROLS - IN RISK ASSESSMENT	RMG	CRITICAL INFRASTRUCTURE INFORMATION DEFINITION OF	LR
CONTROLS - IN RISK MANAGEMENT	RMG	CRITICAL PATH METHOD (CPM)	SSL
CONTROLS - MODIFICATION OF	SOIM	CRITICAL SUCCESS FACTORS (CSFS)	SOIM
CONTROLS - OPERATIONAL	SOIM	CRITICALITY	SOIM
CONTROLS - PREVENTIVE	SSL	CRITICALITY - ASSESSMENT	SOIM RMG
CONTROLS - RECOVERY	SSL	CRITICALITY - CHANGES IN	RMG
CONTROLS - TECHNICAL	SOIM	CRITICALITY - DEFINED	SOIM
CONTROLS - TECHNICAL - AUDIT TRAILS	AAA	CRITICALITY - OF ASSETS	SOIM
CONTROLS - TECHNICAL - AUTHENTICATION	AAA	CRITICALITY - RANKING	SOIM RMG

CRITICALITY - SYSTEM OWNER VIEW	SOIM RMG	CSMA/CD (CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION)	PLT
CRITICALITY ANALYSIS	SOIM	CSO (CHIEF SECURITY OFFICER)	RMG
CRL (CERTIFICATE REVOCATION LIST)	C	CTO (CHIEF TECHNOLOGY OFFICER)	RMG
CRO (CHIEF RISK OFFICER)	RMG	CTR	C
CROSS-BORDER CRIMINAL INVESTIGATION	LR	CTR (COUNTER) BLOCK CIPHER MODE	C
CROSS-REFERENCING MALCODE NAMES	MAT	CULTURAL NEEDS	HF
CROSS-SITE REQUEST FORGERY (CSRF)	WAM	CULTURE	HF
CROSS-SITE RESOURCE SHARING	AAA	CULTURE - AND SECURITY PROGRAMS	HF
CROSS-SITE SCRIPTING	AAA	CULTURE - AS ENABLERS	HF
CROSS-SITE SCRIPTING (XSS)	WAM	CULTURE - AS INFORMATION SECURITY STRATEGY CONSTRAINT	HF
CROSSCUTTING SECURITY	CPS	CULTURE - DYNAMIC INTERCONNECTIONS WITH	HF
CROSSTALK	PLT	CULTURE - IN INFORMATION SECURITY	HF
CRYPTANALYSIS	C	CULTURE - IN SECURITY PROGRAMS	HF
CRYPTANALYSIS - DIFFERENTIAL	C	CURRENT	HS
CRYPTANALYSIS - LINEAR	C	CURRENT RISK STATE OF	RMG
CRYPTANALYTIC - ALGEBRAIC	C	CUSTODIANSHIP	SOIM
CRYPTANALYTIC - BIRTHDAY	C	CUSTOMERS DON'T APPLY PATCHES	SSL
CRYPTANALYTIC - BRUTE FORCE	C	CVE	SOIM
CRYPTANALYTIC - CIPHERTEXT CHOSEN	C	CVE (COMMON VULNERABILITIES AND EXPOSURES)	SOIM
CRYPTANALYTIC - CIPHERTEXT-ONLY	C	CVES AND CWES	SS
CRYPTANALYTIC - DICTIONARY	C	CVSS	SOIM SSL
CRYPTANALYTIC - DIFFERENTIAL CRYPTANALYSIS	C	CWE	SOIM
CRYPTANALYTIC - FACTORING	C	CYBER ATTACK	AB
CRYPTANALYTIC - FREQUENCY ANALYSIS	C	CYBER CRIME	F
CRYPTANALYTIC - IMPLEMENTATION ATTACKS	C	CYBER DOMAIN	F
CRYPTANALYTIC - LINEAR CRYPTANALYSIS	C	CYBER ESPIONAGE IN PEACETIME	LR
CRYPTANALYTIC - PLAINTEXT	C	CYBER INSURANCE MODELS	SOIM
CRYPTANALYTIC - RAINBOW TABLES	C	CYBER KILL CHAIN	MAT
CRYPTANALYTIC - RANDOM NUMBER GENERATORS	C	CYBER SECURITY DEFINITION	CI
CRYPTANALYTIC - REPLAY	C	CYBER SECURITY KNOWLEDGE MANAGEMENT	SOIM
CRYPTANALYTIC - REVERSE ENGINEERING	C	CYBER-CONFLICT	CPS
CRYPTANALYTIC - SOCIAL ENGINEERING	C	CYBER-DEPENDENT ORGANIZED CRIME	AB
CRYPTANALYTIC - TEMPORARY FILES	C	CYBER-ENABLED CRIME VS CYBER-DEPENDENT CRIME	AB
CRYPTANALYTIC ATTACKS - ALGEBRAIC	C	CYBER-ENABLED ORGANIZED CRIME	AB
CRYPTANALYTIC ATTACKS - BIRTHDAY	C	CYBER-PHYSICAL SYSTEMS	CPS
CRYPTANALYTIC ATTACKS - BRUTE FORCE	C	CYBER-THREAT INTELLIGENCE	SOIM
CRYPTANALYTIC ATTACKS - CIPHERTEXT CHOSEN	C	CYBER-THREAT INTELLIGENCE (CTI)	SOIM
CRYPTANALYTIC ATTACKS - CIPHERTEXT-ONLY	C	CYBERBULLYING	AB
CRYPTANALYTIC ATTACKS - DICTIONARY	C	CYBERCRIME	LR
CRYPTANALYTIC ATTACKS - DIFFERENTIAL CRYPTANALYSIS	C	CYBERCRIMINALS	CPS
CRYPTANALYTIC ATTACKS - FACTORING	C	CYBERSECURITY (INSURANCE COVERAGE)	SOIM
CRYPTANALYTIC ATTACKS - FREQUENCY ANALYSIS	C	CYBERSTALKING	AB
CRYPTANALYTIC ATTACKS - IMPLEMENTATION ATTACKS	C	CYCLICAL REDUNDANCY CHECK (CRC)	C
CRYPTANALYTIC ATTACKS - LINEAR CRYPTANALYSIS	C		
CRYPTANALYTIC ATTACKS - PLAINTEXT	C		
CRYPTANALYTIC ATTACKS - RAINBOW TABLES	C		
CRYPTANALYTIC ATTACKS - RANDOM NUMBER GENERATORS	C		
CRYPTANALYTIC ATTACKS - REPLAY	C		
CRYPTANALYTIC ATTACKS - REVERSE ENGINEERING	C		
CRYPTANALYTIC ATTACKS - SOCIAL ENGINEERING	C		
CRYPTANALYTIC ATTACKS - TEMPORARY FILES	C		
CRYPTOCURRENCIES	AB		
CRYPTOCURRENCY MINING	HS		
CRYPTOGRAM	C		
CRYPTOGRAPHIC - LIFECYCLE	C		
CRYPTOGRAPHIC - PROTECTIONS	C		
CRYPTOGRAPHIC - SYSTEMS	C		
CRYPTOGRAPHIC ALGORITHM	C		
CRYPTOGRAPHIC ALGORITHMS AT RTL LEVEL	HS		
CRYPTOGRAPHIC HASHES	F		
CRYPTOGRAPHIC HASHING	F		
CRYPTOGRAPHIC SECURITY MODELS	C		
CRYPTOGRAPHIC STRENGTH	C		
CRYPTOGRAPHY	C		
CRYPTOGRAPHY - HISTORY	C		
CRYPTOGRAPHY - ASYMMETRIC	C		
CRYPTOGRAPHY - ASYMMETRIC - ALGORITHMS	C		
CRYPTOGRAPHY - ASYMMETRIC - CONFIDENTIAL MESSAGES	C		
CRYPTOGRAPHY - ASYMMETRIC - DIFFIE-HELLMAN	C		
CRYPTOGRAPHY - ASYMMETRIC - ECC	C		
CRYPTOGRAPHY - ASYMMETRIC - EL GAMAL	C		
CRYPTOGRAPHY - ASYMMETRIC - OPEN MESSAGES	C		
CRYPTOGRAPHY - ASYMMETRIC - RSA	C		
CRYPTOGRAPHY - DIGITAL SIGNATURES	C		
CRYPTOGRAPHY - HASH FUNCTIONS	C		
CRYPTOGRAPHY - HASH FUNCTIONS - ATTACKS	C		
CRYPTOGRAPHY - HASH FUNCTIONS - HAVAL	C		
CRYPTOGRAPHY - HASH FUNCTIONS - MD (MESSAGE DIGEST) 2 4 AND 5	C		
CRYPTOGRAPHY - HASH FUNCTIONS - RIPEMD-160	C		
CRYPTOGRAPHY - HASH FUNCTIONS - SHA (SECURE HASH ALGORITHM) 0 1 AND 2	C		
CRYPTOGRAPHY - HMAC	C		
CRYPTOGRAPHY - HYBRID	C		
CRYPTOGRAPHY - MAC (MESSAGE AUTHENTICATION CODE)	C		
CRYPTOGRAPHY - MESSAGE DIGESTS	C		
CRYPTOGRAPHY - NON-REPUDIATION	C		
CRYPTOGRAPHY - PGP	C		
CRYPTOGRAPHY - QUANTUM CRYPTOGRAPHY	C		
CRYPTOGRAPHY - SYMMETRIC	C		
CRYPTOGRAPHY - SYMMETRIC - DES	C		
CRYPTOGRAPHY AND ACCESS CONTROL	AAA		
CRYPTOGRAPHY-BASED ACCESS CONTROL	POR		
CRYPTOJACKING	AB		
CRYPTOLOGY	C		
CRYPTOSYSTEM	C		
CRYPTOVARIABLE	C		
CRYPTOVERIF	FMS		
CSA STAR CERTIFICATION	RMG		
CSFS (CRITICAL SUCCESS FACTORS)	SOIM		
CSM (CONFIGURATION SETTING MANAGEMENT)	SOIM		
CSMA (CARRIER SENSE MULTIPLE ACCESS)	PLT		
CSMA/CA (CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE)	PLT		
		DAC (DISCRETIONARY ACCESS CONTROL)	AAA
		DAMAGE ASSESSMENT TEAMS	SOIM
		DAMAGE EVALUATION	SOIM
		DAMAGE OF INFORMATION	CI
		DANGEROUS FUNCTIONS	SS
		DAR (DATA AT REST)	DSS
		DAS (DIRECT ATTACHED STORAGE)	OSV
		DATA - ACCESS	SOIM
		DATA - ACCESS CONTROL	OSV
		DATA - ANALOG	NS
		DATA - AT REST	POR
		DATA - AUDIT	SOIM
		DATA - BREACHES	SOIM LR
		DATA - CENTER BRIDGING EXCHANGE PROTOCOL (DCBX)	NS
		DATA - CLEANING	SOIM
		DATA - COMMUNICATIONS	NS
		DATA - CONNECTIVITY	HS
		DATA - CUSTODIAN	SOIM
		DATA - CUSTODIANSHIP	SOIM
		DATA - DEGAUSSING	SOIM
		DATA - DIDDLING	AB
		DATA - DIGITAL	NS
		DATA - DISCLOSURE	SOIM LR
		DATA - DISPOSAL	SOIM LR
		DATA - DLP	SOIM
		DATA - DLP - BLOCKING	SOIM
		DATA - DLP - DATA DISCOVERY	SOIM
		DATA - DLP - DETECTION/MONITORING	SOIM
		DATA - DLP - LABELING	SOIM
		DATA - DLP - POLICY CREATION	SOIM
		DATA - DLP - PREVENTING	SOIM
		DATA - DLP - REPORTING	SOIM
		DATA - DOCUMENTATION	SOIM
		DATA - ENCRYPTION KEYS	C
		DATA - ENCRYPTION STANDARD (DES)	C
		DATA - ENCRYPTION STANDARD (DES) - DOUBLE DES	C
		DATA - ENCRYPTION STANDARD (DES) - TRIPLE DES (3DES)	C
		DATA - ERASING	SOIM
		DATA - EXECUTION PREVENTION (DEP)	OSV
		DATA - FLOW CONTROL	SS
		DATA - HIDING	SSL
		DATA - HISTORIAN	CPS
		DATA - IN TRANSIT	POR
		DATA - INFORMATION - BUSINESS OWNERS	SOIM RMG
		DATA - INFORMATION - CUSTODIAN/STEWARD	SOIM RMG
		DATA - IRM	AAA
		DATA - LEAK/LOSS PREVENTION (DLP)	SOIM
		DATA - LIFECYCLE CONTROL	SOIM
		DATA - MANAGEMENT	SOIM

D

DATA - MINING	POR	DCB (DATA CENTER BRIDGING) STANDARDS - DCBX (DCB EXCHANGE PROTOCOL)	CPS
DATA - OUTPUT	F	DCB (DATA CENTER BRIDGING) STANDARDS - ETS (ENHANCED TRANSMISSION SELECTION)	CPS
DATA - OVERWRITING	SOIM	DCB (DATA CENTER BRIDGING) STANDARDS - PFC (PRIORITY-BASED FLOW CONTROL)	CPS
DATA - OWNER	SOIM	DCB (DATA CENTER BRIDGING) STANDARDS - QCN (QUANTIZED CONGESTION NOTIFICATION)	CPS
DATA - OWNERSHIP	SOIM	DDOS (DISTRIBUTED DENIAL-OF SERVICE)	NS
DATA - POLICY	SOIM	DDOS (DISTRIBUTED DENIAL-OF-SERVICE) ATTACK	NS
DATA - PUBLISHING	SOIM	DDOS ATTACKS	CPS
DATA - QUALITY	SOIM	DDOS DEFENCES	NS
DATA - REFORMATTING	SOIM	DDOS DETECTION	MAT
DATA - REMANENCE	SOIM	DE MINIMIS EXCEPTIONS TO CRIMES AGAINST INFORMATION SYSTEMS	LR
DATA - RETENTION	SOIM LR	DE-ANONYMISATION	LR
DATA - SCRUBBING	POR	DEADLOCK	OSV
DATA - SECURITY	POR	DEADLOCKS (DOS)	OSV
DATA - STANDARDS	SOIM	DEBUGGING	SS
DATA - STORAGE	HS	DECENTRALISED P2P MODELS	DSS
DATA - VULNERABILITIES - DE DUPLICATION	SOIM	DECENTRALISED POINT-TO-POINT INTERACTIONS ACROSS DISTRIBUTED ENTITIES WITHOUT A CENTRALISED COORDINATION SERVICE	DSS
DATA - VULNERABILITIES - DISPOSAL	SOIM LR	DECENTRALIZATION	DSS
DATA - VULNERABILITIES - ENCRYPTION KEYS	C	DECIPHER	C
DATA - VULNERABILITIES - IRM	AAA	DECISION ALGORITHMS	AAA
DATA - VULNERABILITIES - OUTPUT	F	DECISION SUPPORT SYSTEMS (DSS)	SOIM
DATA - VULNERABILITIES - RETENTION	SOIM LR	DECISIONISTIC	RMG
DATA - VULNERABILITIES - SCRUBBING	POR	DECODING	C
DATA - VULNERABILITIES - STORAGE	HS	DECODING ENCRYPTION	C
DATA ABSTRACTION LAYERS	F	DECRYPTION	C
DATA ACCESS CENSORSHIP RESISTANCE	POR	DECRYPTION KEY	C
DATA ACQUISITION	F	DEFAULT PASSWORDS AND CREDENTIALS	SSL
DATA AGGREGATION	POR	DEFENSE-IN-DEPTH	SSL
DATA ANALYSIS EVENT DATA ANALYSIS	SOIM	DEFENSE-IN-DEPTH DESIGN	SSL
DATA ANALYTICS AS A SERVICE	DSS	DEFENSIVE PROGRAMMING	SS
DATA ANONYMIZATION	POR	DEFINE METRICS AND COMPLIANCE REPORTING	SSL
DATA CENTER	DSS	DEFINE SECURITY REQUIREMENTS	SSL
DATA CLASSIFICATION	AAA	DEFINING INCIDENT MANAGEMENT PROCESSES (CMU/SED)	SOIM
DATA CLASSIFICATION - DOCUMENTATION	SOIM POR	DEFINITION OF CYBER SECURITY	CI
DATA CLASSIFICATION - LLC (LOGICAL LINK CONTROL)	NS	DEFINITIONS	F LR
DATA CLASSIFICATION - MAC (MEDIA ACCESS CONTROL)	NS	DEFINITIONS AND CONCEPTUAL MODELS	F
DATA COLLECTION	SOIM	DEGAUSS	HS
DATA COLLECTION - RISK ASSESSMENT PROCESS	RMG	DEGAUSSING	SOIM
DATA COMMUNICATION	NS	DEGRADED PERFORMANCE	SOIM F
DATA CONFIDENTIALITY	POR	DELEGATION AND REVOCATION	AAA
DATA CONSISTENCY	DSS	DELETE PERMISSION	OSV
DATA CUSTODIAN	DSS	DELETING DATA	LR
DATA DELETION	LR	DELIVERY	AB MAT
DATA DICTIONARY	OSV	DELPHI METHOD	RMG POR
DATA DICTIONARY/DIRECTORY SYSTEM (DD/DS)	OSV	DELPHI METHOD - EVENT TREE ANALYSIS	RMG
DATA DIDDLING	AB	DELPHI METHOD - FAULT TREE ANALYSIS	RMG
DATA ENCRYPTION	C	DELTA RELEASE	SSL
DATA ENCRYPTION AND KEY MANAGEMENT	SSL	DEMAND MANAGEMENT	CPS
DATA ENCRYPTION MECHANISMS	C	DEMATERIALIZATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICES	LR
DATA ENCRYPTION STANDARD (DES)	C	DEMILITARISED ZONE (DMZ)	SOIM
DATA FILE CONTROL PROCEDURES	F	DEMILITARIZED ZONE (DMZ)	NS
DATA HIDING	SSL	DENIAL OF AUTHORIZATION	RMG
DATA HISTORIAN	CPS	DENIAL OF SERVICE	NS AB SOIM
DATA INTEGRITY	OSV	DENIAL OF SERVICE (DOS)	DSS
DATA INTEGRITY	OSV	DENIAL-OF-SERVICE (DOS) ATTACK	NS
DATA LEAK PROTECTION (DLP)	OSV	DENSE-WAVE DIVISION MULTIPLEXERS (DWDMS)	PLT
DATA LEAKAGE	POR	DEP (DATA EXECUTION PREVENTION)	OSV
DATA LEAKS	AB	DEPENDENCY MODELLING	RMG
DATA MASKING	C	DEROGATIONS ALLOWING TRANSFERS	LR
DATA MINING	POR	DES	C
DATA NORMALIZATION	POR	DES (DATA ENCRYPTION STANDARD)	C
DATA OBFUSCATION	C	DES (DATA ENCRYPTION STANDARD) - ADVANTAGES	C
DATA OWNER	POR LR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE	C
DATA OWNER SENSITIVITY ASSESSMENT RESPONSIBILITY OF	POR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - ACCOUNTABILITY	C
DATA PROTECTION	LR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - AUTHORIZATION	C
DATA PROTECTION DIRECTIVES	LR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - CONTROLS	C
DATA PUBLISHING CENSORSHIP RESISTANCE	POR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - DEFENSE-IN-DEPTH	C
DATA RECOVERY & FILE CONTENT CARVING	F	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - DOCUMENTATION	C
DATA REDUNDANCY	SOIM	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - LEAST PRIVILEGE	C
DATA RETENTION	LR	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - RISK-BASED CONTROLS	C
DATA SECURITY	POR DSS	DES (DATA ENCRYPTION STANDARD) - ARCHITECTURE - SEPARATION OF DUTIES	C
DATA SENSITIVITY - ASSESSMENT PROCESS	SOIM	DES (DATA ENCRYPTION STANDARD) - BLOCK CIPHER MODES	C
DATA SENSITIVITY - ASSESSMENT RESPONSIBILITY	SOIM	DES (DATA ENCRYPTION STANDARD) - DETAILED DESIGN	C
DATA SENSITIVITY - CHANGES IN	RMG	DES (DATA ENCRYPTION STANDARD) - DISADVANTAGES	C
DATA SENSITIVITY - RANKING	SOIM	DES (DATA ENCRYPTION STANDARD) - DOUBLE DES	C
DATA SOVEREIGNTY	LR	DES (DATA ENCRYPTION STANDARD) - GENERAL DESIGN DOCUMENT	C
DATA STORAGE AS A SERVICE	DSS	DES (DATA ENCRYPTION STANDARD) - MEET-IN-THE-MIDDLE	C
DATA SUBJECT, PERSONAL DATA (AND PII)	LR	DES (DATA ENCRYPTION STANDARD) - RELEASE MANAGEMENT	C
DATA TERMINAL EQUIPMENT	HS	DES (DATA ENCRYPTION STANDARD) - STREAM MODES	C
DATA TRANSPORTATION	DSS	DES (DATA ENCRYPTION STANDARD) - SYMMETRIC CRYPTOGRAPHY	C
DATA WAREHOUSE	DSS	DESIGN	SSL
DATA WIPING	SOIM	DESIGN AND DEVELOPMENT	SSL
DATA-DEPENDENCY	PLT	DESIGN AND FABRICATION OF SILICON INTEGRATED CIRCUITS	HS
DATA-FLOW INTEGRITY	OSV	DESIGN AND USE CRYPTOGRAPHY STANDARDS	SSL
DATA-ONLY-ATTACKS	SS	DESIGN BY CONTRACT	SS
DATA-TRANSFER	NS	DESIGN CHOICES	OSV
DATABASE - BACKUP	SOIM	DESIGN PROCESS	HS
DATABASE - INTERFACE LANGUAGES	OSV	DESIGNATED APPROVING AUTHORITY (DAA)	SOIM RMG
DATABASE - INTERFACE LANGUAGES - ONLINE ANALYTICAL PROCESSING (OLAP)	OSV	DESIRED STATE FOR INFORMATION SECURITY	RMG
DATABASE - INTERFACE LANGUAGES - OPEN DATABASE CONNECTIVITY (ODBC)	OSV	DESKTOP VIRTUALIZATION	OSV
DATABASE - MAINTENANCE	OSV	DESTRUCTION	SOIM
DATABASE - MANAGEMENT SYSTEM (DBMS) - ARCHITECTURE	OSV	DESTRUCTION - MEDIA	SOIM
DATABASE - MODEL - OBJECT-ORIENTED	OSV	DETAILED DESIGN	SSL
DATABASE - SECURITY	OSV	DETECT (INCIDENT MANAGEMENT PROCESSES)	SOIM
DATABASE - VULNERABILITIES	MAT	DETECTING ATTACKS	CPS
DATABASE ADMINISTRATOR (DBA)	RMG	DETECTING BOTNETS BY DNS	SOIM
DATABASE MANAGEMENT SYSTEM (DBMS)	OSV	DETECTION AND REPORTING	RMG
DATABASE SPECIFICATIONS	OSV	DETECTION OF VULNERABILITIES	SS
DATABASES	WAM OSV DSS		
DATABASES - ENCRYPTION	C		
DATASETS	SOIM		
DCB (DATA CENTER BRIDGING) STANDARDS	CPS		

DETECTIVE CONTROLS	SOIM	DISTANCE BOUNDING PROTOCOLS	PLT
DETENSE IN DEPTH	SOIM	DISTANCE FRAUD	PLT
DETERMINATION - DE VIGENERE BLAIS	C	DISTANCE HIJACKING	PLT
DETERMINATION - OF IMPACT	RMG	DISTANCE MEASUREMENT TECHNIQUES	PLT
DETERMINATION - OF RISK	RMG	DISTRIBUTED - CONTROL SYSTEMS (DCS)	DSS
DETERMINISTIC ROUTING	NS	DISTRIBUTED - DENIAL OF SERVICE (DDOS)	NS
DETERRENT CONTROLS	SSL	DISTRIBUTED - DENIAL OF SERVICE (DDOS) - ZOMBIES	NS
DEVELOP	RMG	DISTRIBUTED - SYSTEMS	DSS
DEVELOP A SECURE UPGRADE PROCESS	SSL	DISTRIBUTED - TRANSACTION PROCESSING (DTP)	NS
DEVELOPERS AND PASSWORD SECURITY	HF	DISTRIBUTED COMPUTING ENVIRONMENT	DSS
DEVELOPMENT	SSL	DISTRIBUTED COMPUTING ENVIRONMENT (DCE)	DSS
DEVELOPMENT - ENDPOINT SECURITY - APPLICATION WHITELISTING	OSV	DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK	NS
DEVELOPMENT - ENDPOINT SECURITY - ENCRYPTION	C	DISTRIBUTED HASH TABLE	DSS
DEVELOPMENT - ENDPOINT SECURITY - HIDS	NS	DISTRIBUTED IRT	SOIM
DEVELOPMENT - ENDPOINT SECURITY - HOST-BASED FIREWALLS	NS	DISTRIBUTED LEDGERS	POR
DEVELOPMENT - ENDPOINT SECURITY - MDM	WAM	DISTRIBUTED LOGS	AAA
DEVELOPMENT - ENDPOINT SECURITY - SECURE BROWSING	WAM	DIT (DIRECTORY INFORMATION TREE)	AAA
DEVELOPMENT - ENDPOINT SECURITY - TRUSTED PLATFORM MODULE	HS	DITSCAP	RMG
DEVELOPMENT - FORENSICS AND	F	DITSCAP - LIFE-CYCLE PHASES	LR
DEVELOPMENT - PERIPHERAL DEVICE RECOGNITION	AAA	DIU (DATA IN USE)	DSS
DEVELOPMENT - SYNCHRONOUS TOKEN DEVICES	AAA	DIVERSE ROUTING	NS
DEVELOPMENT - WATERFALL MODEL	SSL	DLLS (DYNAMIC LINK LIBRARIES)	SS
DEVICE CAPABILITIES AND LIMITATIONS	HF	DLP (DATA LEAK PROTECTION)	SOIM
DEVICE FINGERPRINTS	PLT	DLP (DATA LEAKAGE PREVENTION)	SOIM
DEVICE METADATA	POR	DMA	OSV
DEVICE UNDER IDENTIFICATION	PLT	DMZ (DEMILITARIZED ZONE)	NS
DEVOPS	SOIM	DN (DISTINGUISHED NAME)	AAA
DFRWS	F	DNS	SOIM
DFRWS (DIGITAL FORENSIC SCIENCE RESEARCH WORKSHOP)	F	DNS (DOMAIN NAME SYSTEM) - CACHE-POISONING	NS
DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)	NS	DNS (DOMAIN NAME SYSTEM) - DDOS (DISTRIBUTED DENIAL-OF-SERVICE)	NS
DIACAP	RMG	DNS (DOMAIN NAME SYSTEM) - DOS (DENIAL-OF-SERVICE)	NS
DIACAP - LIFE-CYCLE PHASES	LR	DNS (DOMAIN NAME SYSTEM) - FAST FLUX	NS
DIAL-UP ACCESS CONTROLS	PLT	DNS (DOMAIN NAME SYSTEM) - REGISTRATION TAKE OVER	NS
DICTIONARY ATTACK	C	DNS (DOMAIN NAME SYSTEM) - TUNNELS	NS
DIFFERENCES FROM FINANCIALLY MOTIVATED ATTACKS	AB	DNS (DOMAIN NAME SYSTEM) - ZONE ENUMERATION	NS
DIFFERENT PERMISSION APPROACHES	WAM	DNS (DOMAIN NAME SYSTEMS)	NS
DIFFERENTIAL ANALYSIS	F	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - CACHE-POISONING	NS
DIFFERENTIAL BACKUPS	SOIM	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - DDOS	NS
DIFFERENTIAL CRYPTANALYSIS	C	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - DOS	NS
DIFFERENTIAL POWER ANALYSIS	HS	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - FAST FLUX	NS
DIFFERENTIAL PRIVACY	POR	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - QUERY INTERCEPTION	NS
DIFFIE-HELLMAN ALGORITHM	C	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - QUERY REDIRECTION	NS
DIFFIE-HELLMAN KEY AGREEMENT	C	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - REGISTRATION TAKE OVER	NS
DIFFIE-HELLMAN PROBLEM	C	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - TUNNELS	NS
DIFFUSION	C	DNS (DOMAIN NAME SYSTEMS) - ATTACKS - ZONE ENUMERATION	NS
DIFICULTY OF DEFENCE	POR	DNS (DOMAIN NAME SYSTEMS) - AUTHORITATIVE SERVER	NS
DIGITAL (FORENSIC) TRACE	F	DNS (DOMAIN NAME SYSTEMS) - FQDN	NS
DIGITAL - CERTIFICATE	C	DNS (DOMAIN NAME SYSTEMS) - HIERARCHY	NS
DIGITAL - RIGHTS MANAGEMENT (DRM)	POR	DNS (DOMAIN NAME SYSTEMS) - QUERY MANIPULATION	NS
DIGITAL - SIGNATURE	C	DNS (DOMAIN NAME SYSTEMS) - RECURSION	NS
DIGITAL - SUBSCRIBER LINE (DSL)	PLT	DNS (DOMAIN NAME SYSTEMS) - RECURSIVE RESOLVER	NS
DIGITAL CERTIFICATE	C	DNS (DOMAIN NAME SYSTEMS) - RESOLUTION PROCESS	NS
DIGITAL CODE SIGNING	C	DNS (DOMAIN NAME SYSTEMS) - RESOLVER	NS
DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS	PLT	DNS (DOMAIN NAME SYSTEMS) - RR (RESOURCE RECORD)	NS
DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS (DECT)	PLT	DNS (DOMAIN NAME SYSTEMS) - SPOOFING	NS
DIGITAL ENVELOPE	C	DNS (DOMAIN NAME SYSTEMS) - WEB-BASED ATTACKS AND	NS
DIGITAL FORENSICS	F	DNS (DOMAIN NAME SYSTEMS) - ZONE TRANSFERS	NS
DIGITAL RIGHTS MANAGEMENT	POR	DNS (DOMAIN NAME SYSTEMS) - ZONES	NS
DIGITAL RIGHTS MANAGEMENT (DRM)	AAA POR	DNS AS DDOS AMPLIFIER	SOIM
DIGITAL SIGNATURES	C	DNS ATTACKS	NS
DIGITAL SUBSCRIBER LINES (DSL)	PLT	DNS FAST-FLUX	MAT
DIM (DATA IN MOTION)	LR	DNS HIJACKING	NS
DIMENSIONS	MAT	DNS QUERIES - MANIPULATION	AB OSV
DIRECT ATTACHED STORAGE (DAS)	OSV	DNS SECURITY EXTENSIONS	NS
DIRECT INWARD DIAL (DID)	PLT	DNS SPOOFING	NS
DIRECT SEQUENCY SPREAD SPECTRUM	PLT	DNSSEC	SOIM NS
DIRECTIVE CONTROLS	SSL	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS)	NS
DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS	AB	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - DC1 - CONFIGURATION	NS
DIRECTORY - ACCESS PROTOCOL (DAP)	AAA	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - DC1 - TRUST ANCHORS	NS
DIRECTORY - INFORMATION SHADOWING PROTOCOL (DISP)	AAA	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - DC1 - ZONE SIGNING	NS
DIRECTORY - MANAGEMENT	AAA	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - DNS1 CONFIGURATION	NS
DIRECTORY - SYSTEM PROTOCOL (DSP)	AAA	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - HARDWARE	NS
DIRECTORY - TECHNOLOGIES	AAA	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - SOFTWARE	NS
DISABILITY	HF	DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIONS) - SOFTWARE	NS
DISASTER - PREPAREDNESS	SOIM	REQUIREMENTS	NS
DISASTER - RECOVERY (DR)	SOIM	REQUIREMENTS - AS POSTINCIDENT ACTIVITY	SOIM
DISASTER - RECOVERY (DR) - PROCESS	SOIM	DOCUMENTATION - CERTIFICATION TEST PLAN PROCEDURES	SOIM
DISASTER RECOVERY AS A SERVICE (DRAAS)	DSS	DOCUMENTATION - FOR RISK MANAGEMENT	HF
DISASTER RECOVERY MANAGEMENT/PLANNING	SOIM	DOCUMENTATION - IN RISK MANAGEMENT FRAMEWORK	RMG
DISASTER RECOVERY PLAN - DEFINED	SOIM	DOCUMENTATION - REVIEW OF DURING CERTIFICATION TESTING	SOIM
DISASTER RECOVERY PLAN - IN INCIDENT MANAGEMENT	SOIM	DOCUMENTATION - RISK ASSESSMENT	RMG
DISASTER RECOVERY PLAN - TESTING	SOIM	DOCUMENTATION - ROLES AND RESPONSIBILITIES	RMG
DISASTER RECOVERY PLAN DESK CHECKING	SOIM	DOCUMENTATION - SECURITY AUDITS	SOIM
DISASTER RECOVERY PLAN WALK-THROUGH	SOIM	DOCUMENTATION - SYSTEM SECURITY PLANS	SOIM
DISASTER RECOVERY PLANNING (DRP)	SOIM	DODAF (DEPT OF DEFENSE ARCHITECTURE FRAMEWORK)	SOIM
DISASTER RECOVERY PROCEDURES	SOIM	DOLEV-YAO ADVERSARIAL MODEL	NS
DISASTER/BUSINESS RECOVERY DOCUMENTATION	SOIM	DOMAIN - LITIGATION	AB
DISCONNECTS BETWEEN DEVELOPERS AND USERS	HF	DOMAIN FLUX	AB
DISCRETE LOGARITHM PROBLEM	C	DOMAIN-NAME GENERATION ALGORITHMS	MAT
DISCRETE-TIME CONTROL	CPS	DOS (DENIAL-OF-SERVICE)	NS
DISCRETIONARY ACCESS CONTROL (DAC)	AAA	DOS (DENIAL-OF-SERVICE) ATTACK	NS
DISCRETIONARY ACCESS CONTROLS	OSV	DOUBLE FILE EXTENSIONS	AB
DISCRETIONARY ACCESS CONTROLS (DAC)	AAA	DOWNLOADED FILES	F
DISGRUNTLED EMPLOYEES	CPS	DOWNTIME REPORT	SOIM
DISINFORMATION	AB	DOXING	AB
DISK WIPING	SOIM	DRAAS (DISASTER RECOVERY AS A SERVICE)	DSS
DISPLACEMENT	AB	DRAWBACKS	OSV
DISPOSITION PHASE	SSL	DRIVE-BY DOWNLOAD ATTACKS	AB
DISRUPTING MALWARE OPERATIONS	MAT	DRIVE-BY-DOWNLOAD ATTACKS	WAM
DISTANCE BOUNDING	PLT	DRIVER SIGNING	OSV
DISTANCE BOUNDING AND SECURE POSITIONING	PLT	DRM (DIGITAL RIGHTS MEASUREMENT)	POR

DROPPERS	MAT
DRP (DISASTER RECOVERY PLAN)	SOIM
DRUG DEALING	AB
DSA	C
DUAL CONTROL	AAA
DUAL CONTROL AUTHENTICATION	AAA
DUAL-HOMED FIREWALL	NS
DUE - CARE	SOIM
DUE DILIGENCE	SOIM RMG
DUE PROFESSIONAL CARE	RMG
DUMMY ADDITION	POR
DUMPSTER DIVING	AB
DUMPZ	AB
DUPLICATE SITE	SOIM
DYNAMIC - LINK LIBRARIES (DLLS)	OSV
DYNAMIC ANALYSIS	MAT
DYNAMIC CHECKS	SS
DYNAMIC DETECTION	SS
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)	NS
DYNAMIC PACKET FILTERING	NS
DYNAMIC PASSWORDS	AAA
DYNAMIC PASSWORDS - SYNCHRONOUS	AAA
DYNAMIC QUERIES VULNERABILITIES AND	SS
DYNAMIC ROUTING TABLES	NS
DYNAMIC SUBSYSTEMS NIST SP 800-37 REVISION 1 GUIDANCE ON	RMG
DYNAMIC SYMBOLIC EXECUTION	SS
DYNAMICALLY UPDATABLE	MAT

E

E-COMMERCE SUPPORTING TRANSACTIONS	DSS
E-GOVERNMENT ACT OF 2002	LR
E-MAIL - PHISHING	WAM
E-MAIL - SPOOFING	WAM
EZEE	POR
EASYCRYPT	FMS
EAVESDROPPING	F AB
ECB	C
ECB (ELECTRONIC CODE BOOK) BLOCK CIPHER MODE	C
ECC (ELLIPTIC CURVE CRYPTOGRAPHY)	C
ECIES	C
ECLIPSE ATTACKS	DSS
ECOMMERCE	SSL WAM
ECOMMERCE ARCHITECTURES	WAM
ECOMMERCE REQUIREMENTS	WAM
ECOMMERCE RISK	RMG
ECONOMICS OF DEVIANT SECURITY	CI
ECONOMY OF MECHANISM	CI
EDUCATION	HF RMG
EDUCATION - IN INFORMATION SECURITY FRAMEWORK	HF
EFFECTIVE GOALS	RMG
EFFECTIVE INCIDENT MANAGEMENT	SOIM
EFFECTIVE INFORMATION SECURITY GOVERNANCE	RMG
EFFECTIVE INFORMATION SECURITY GOVERNANCE - AND BUSINESS GOALS AND OBJECTIVES	RMG
EFFECTIVE INFORMATION SECURITY GOVERNANCE - ASSURANCE PROCESS	RMG
INTEGRATION	RMG
EFFECTIVE RISK MANAGEMENT	RMG
EFFECTIVENESS	HF
EFFECTIVENESS OF SECURITY PROCESSES	CI
EFFECTS OF CONTRACT ON NON-CONTRACTING PARTIES	LR
EFFICIENCY	HF CPS
EFFICIENCY CONCERNS	POR
EFFORT DETERMINATION OF LEVEL OF	RMG
EGRESS MONITORING	SOIM
EISA (ENTERPRISE INFORMATION SECURITY ARCHITECTURE)	RMG
EL CARNAL	C
EL GAMAL ALGORITHM	C
ELASTICITY	DSS
ELECTRIC POWER GRIDS	CPS
ELECTRO-MAGNETIC RADIATION ATTACKS	HS
ELECTROMAGNETIC INTERFERENCE	HS
ELECTROMAGNETIC INTERFERENCE (EMI)	PLT
ELECTRONIC DATA INTERCHANGE (EDD)	NS
ELECTRONIC DESIGN AUTOMATION (EDA)	HS
ELECTRONIC FUNDS TRANSFER	WAM
ELECTRONIC PAYMENTS	AB
ELECTRONIC SIGNATURES AND INDENTITY TRUST SERVICES	LR
ELECTRONIC VAULTING BACKUPS	SOIM
ELECTRONIC VOTING	POR
ELEMENTS OF A MALICIOUS OPERATIONS	AB
ELEMENTS OF RISK	RMG
ELIABILITY VERIFIABILITY	POR
ELLIPTIC CURVE CRYPTOGRAPHY (ECC)	C
EMAIL	WAM
EMAIL REGULATION	AB
EMAIL SPAM	AB
EMBEDDED AUDIT MODULES	RMG
EMBEDDED SYSTEMS	CPS
EMBRACING SECURITY	OSV
EMERGENCY - MANAGEMENT ORGANIZATION (EMO)	SOIM RMG
EMERGENCY - NOTIFICATION LIST	SOIM
EMERGENCY ACTION TEAMS	SOIM
EMERGENCY MANAGEMENT TEAM	SOIM
EMERGENCY MANAGEMENT TEAMS	SOIM

EMERGING THREATS	SOIM
EMPLOYEES	HF
ENACTING SECURITY POLICY	RMG
ENCAPSULATING SECURITY PAYLOAD (ESP)	NS
ENCAPSULATING SECURITY PAYLOAD (ESP) - PROTOCOL	NS
ENCAPSULATION	NS OSV
ENCAPSULATION SECURITY PAYLOAD	C NS
ENCAPSULATION SECURITY PAYLOAD (ESP)	NS
ENCIPHERK	C
ENCODING	SOIM C
ENCODING ENCRYPTION	C
ENCOURAGING SECURITY STANDARDS VIA CONTRACT	LR
ENCRYPTED EMAIL	C
ENCRYPTION	SOIM C
ENCRYPTION - AES	C
ENCRYPTION - ALGORITHMS	C
ENCRYPTION - ALGORITHMS - CHARACTERISTICS	C
ENCRYPTION - ALGORITHMS - EVALUATION	C
ENCRYPTION - ASYNCHRONOUS	C
ENCRYPTION - AVALANCHE EFFECT	C
ENCRYPTION - BLOCK CIPHERS	C
ENCRYPTION - BLOWFISH	C
ENCRYPTION - CA (CERTIFICATE AUTHORITY)	C
ENCRYPTION - CIPHERTEXT	C
ENCRYPTION - CLEARTEXT	C
ENCRYPTION - CLOUD COMPUTING AND	DSS
ENCRYPTION - COLLISIONS	C
ENCRYPTION - CONCEPTS	C
ENCRYPTION - CONFUSION	C
ENCRYPTION - CRYPTANALYSIS	C
ENCRYPTION - CRYPTOGRAM	C
ENCRYPTION - CRYPTOLOGY	C
ENCRYPTION - CRYPTOSYSTEM	C
ENCRYPTION - CRYPTOVARIABLES	C
ENCRYPTION - DATABASES	C
ENCRYPTION - DECODING	C
ENCRYPTION - DECRYPTION	C
ENCRYPTION - DEFINITION	C
ENCRYPTION - DES (DATA ENCRYPTION STANDARD)	C
ENCRYPTION - DIFFUSION	C
ENCRYPTION - DIGITAL CERTIFICATES	C
ENCRYPTION - DIGITAL SIGNATURES	C
ENCRYPTION - ENCODING	C
ENCRYPTION - END-TO-END	C
ENCRYPTION - ENDPOINT	C
ENCRYPTION - HASH FUNCTIONS	C
ENCRYPTION - IV (INITIALIZATION VECTOR)	C
ENCRYPTION - KEYS	C
ENCRYPTION - KEYS - ASYMMETRIC	C
ENCRYPTION - KEYS - AUTOMATED GENERATION	C
ENCRYPTION - KEYS - CERTIFICATE REPLACEMENT	C
ENCRYPTION - KEYS - CERTIFICATE REVOCATION	C
ENCRYPTION - KEYS - CLUSTERING	C
ENCRYPTION - KEYS - DESTRUCTION	C
ENCRYPTION - KEYS - DISTRIBUTION	C
ENCRYPTION - KEYS - DUTIES	C
ENCRYPTION - KEYS - ESCROW	C
ENCRYPTION - KEYS - FINANCIAL INSTITUTIONS	C
ENCRYPTION - KEYS - KEY ENCRYPTING KEYS	C
ENCRYPTION - KEYS - LENGTH	C
ENCRYPTION - KEYS - MANAGEMENT	C
ENCRYPTION - KEYS - PUBLIC	C
ENCRYPTION - KEYS - RANDOMNESS	C
ENCRYPTION - KEYS - RECOVERY	F
ENCRYPTION - KEYS - SPACE	C
ENCRYPTION - KEYS - STORAGE	C
ENCRYPTION - KEYS - WEB OF TRUST	C
ENCRYPTION - KEYS - WRAPPING	C
ENCRYPTION - KEYS - X-KISS	C
ENCRYPTION - KEYS - X-KRSS	C
ENCRYPTION - KEYS - XKMS	C
ENCRYPTION - KIMP (KEY MANAGEMENT INTEROPERABILITY PROTOCOL)	C
ENCRYPTION - LINK	C
ENCRYPTION - NONREPUDIATION	C
ENCRYPTION - PERMUTATION	C
ENCRYPTION - PLAINTEXT	C
ENCRYPTION - PUBLIC KEY	C
ENCRYPTION - RA (REGISTRATION AUTHORITY)	C
ENCRYPTION - RC2	C
ENCRYPTION - RC6	C
ENCRYPTION - SP-NETWORK	C
ENCRYPTION - STREAM-BASED CIPHERS	C
ENCRYPTION - SUBSTITUTION	C
ENCRYPTION - SYMMETRIC-KEY	C
ENCRYPTION - SYNCHRONOUS	C
ENCRYPTION - SYSTEMS	C
ENCRYPTION - TOOLS	C
ENCRYPTION - TOOLS - FILE ENCRYPTION SOFTWARE	C
ENCRYPTION - TOOLS - MEDIA ENCRYPTION SOFTWARE	C
ENCRYPTION - TOOLS - SELF-ENCRYPTING USE DRIVES	HS
ENCRYPTION - TRANSPOSITION	C
ENCRYPTION - VULNERABILITIES AND	C
ENCRYPTION - WORK FACT	C
ENCRYPTION - WORK FACTOR	C
ENCRYPTION CONCERNS	F
ENCRYPTION-BASED PROTOCOLS	C
END POINT SECURITY	HF
END-TO-END ENCRYPTION	C
ENDPOINT SECURITY - DEVICES	NS
ENDPOINT SECURITY - ENCRYPTION	C
ENDURING GOALS	RMG

ENFORCEABLE POLICIES	AAA
ENFORCEMENT – REMEDIES	LR
ENFORCEMENT AND PENALTIES	LR
ENFORCEMENT JURISDICTION	LR
ENFORCEMENT OF PRIVACY LAWS	LR
ENFORCING ACCESS CONTROL	AAA
ENGINEERING LIFE CYCLE	SSL
ENHANCED - SIMPLE MAIL TRANSFER PROTOCOL (ESMTP)	WAM
ENHANCED - TRANSMISSION SELECTION (ET S)	NS
ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL	PLT
ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)	PLT
ENISA	SOIM
ENRICH	F
ENTERPRISE ARCHITECTURE	RMG
ENTERPRISE ARCHITECTURE (EA)	SSL
ENTERPRISE DATA FLOW ARCHITECTURE	RMG
ENTERPRISE GOVERNANCE	RMG
ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)	RMG
ENTERPRISE RISK ASSESSMENT	RMG
ENTERPRISE RISK MANAGEMENT (ERM)	RMG
ENTERPRISE RISK MANAGEMENT STRATEGY - INFORMATION SYSTEM LEVEL (TIER 3)	SOIM RMG
ENTERPRISE RISK MANAGEMENT STRATEGY - MISSION/BUSINESS PROCESS LEVEL (TIER 2)	RMG
ENTERPRISE RISK MANAGEMENT STRATEGY - ORGANIZATION LEVEL (TIER 1)	RMG
ENTERPRISE SECURITY ARCHITECTURE	SOIM
ENTERPRISE SECURITY AUTHORIZATION PROGRAM - DEFINITION	SOIM RMG
ENTERPRISE SECURITY AUTHORIZATION PROGRAM - SPECIAL ISSUES	SOIM
ENTERPRISE SYSTEM AUTHORIZATION POLICY SAMPLE	SOIM
ENTERPRISE SYSTEM AUTHORIZATION PROGRAM - EXPERT SYSTEMS	SOIM
ENTERPRISE SYSTEM AUTHORIZATION PROGRAM - KEY ELEMENTS OF	RMG
ENTROPY GENERATING BUILDING BLOCKS	HS
ENVIRONMENT CONDITIONS (ABAC)	AAA
ENVIRONMENTAL CRIMINOLOGY	AB
ENVIRONMENTAL THREATS	SOIM
ENVIRONMENTS	MAT
EQUAL ERROR RATE	AAA
EQUIPMENT LIFECYCLE	SOIM
EQUIVALENCE-BASED ANALYSIS	FMS
ERADICATION (INCIDENT RESPONSE PLAN)	SOIM
ERADICATION INCIDENT RESPONSE AND	SOIM
ERASING DATA	SOIM
ERRONEOUS EXECUTION	SS
ERROR HANDLING VULNERABILITIES AND	SS
ERRORS AND OMISSIONS (INSURANCE COVERAGE)	SOIM
ESCALATION	SOIM
ESCALATION PROCESS FOR INCIDENT MANAGEMENT	SOIM
ESCROW	SOIM
ESMTP (ENHANCED SIMPLE MAIL TRANSFER PROTOCOL)	NS
ESP (ENCAPSULATING SECURITY PAYLOAD)	NS
ESPIONAGE	AB
ESTABLISH A STANDARD INCIDENT RESPONSE PROCESS	SSL
ESTABLISH DESIGN REQUIREMENTS	SSL
ESTABLISH INCIDENT RESPONSE CAPABILITY	RMG
ESTABLISHMENT PROCESSES	PLT
ETERNITY SERVICE	POR
ETHERNET	NS PLT
ETHERNET (IEEE 802.3)	NS
ETHICS	HF LR
ETHICS - (ISC)2 CODE	HF
ETHICS - AS INFORMATION SECURITY STRATEGY CONSTRAINT	POR
ETHICS - CODES	HF
ETHICS - COMPUTER	HF
ETHICS - FALLACIES	HF
ETHICS - HACKER	HF
ETHICS - IN SECURITY PROGRAM MANAGEMENT	POR
ETHICS - PROFESSIONAL	HF
ETSI TS 103 645	CPS
EUROPEAN - NETWORK AND INFORMATION SECURITY AGENCY (ENISA)	RMG
EUROPEAN - UNION (EU)	LR
EUROPEAN PAYMENT SERVICES DIRECTIVE 2	WAM
EVALUATION ASSURANCE LEVEL (EAL)	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-1	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-2	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-3	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-4	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-5	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-6	SSL
EVALUATION ASSURANCE LEVEL (EAL) - EAL-7	SSL
EVALUTATION - DAMAGE	SOIM
EVASION AND COUNTERMEASURES	MAT
EVENT DATA ANALYSIS	SOIM
EVENT TREE ANALYSIS	RMG
EVENTS	SOIM
EVENTS - ANALYSIS	SOIM
EVENTS - LOGGING	SOIM
EVENTS - STORAGE	SOIM
EVENTUAL CONSISTENCY	DSS
EVIDENCE	F
EVIDENCE - CHAIN OF	F
EVIDENCE - LEGAL ASPECTS OF FORENSIC	F
EVIDENCE - REQUIREMENTS FOR	F
EVIDENCE AND PROOF	LR
EVIDENCE COLLECTION	F
EXECUTABLE CODE	OSV
EXECUTE: MITIGATION AND COUNTERMEASURES	SOIM
EXECUTION MONITORS	AAA
EXECUTIVE MANAGEMENT	RMG
EXECUTIVE MANAGEMENT - COMMUNICATE RISKS	RMG
EXECUTIVE MANAGEMENT RESPONSIBILITIES OF	RMG
EXPERT-BSM	SOIM

EXPLOIT	F
EXPLOIT KITS	AB
EXPLOITATION	AB MAT
EXPLOITATION FRAMEWORKS	MAT
EXPLORE	F
EXPORT ADMINISTRATION REGULATIONS (EAR)	LR
EXPOSURE	C
EXTENDABLE OUTPUT FUNCTION	C
EXTENDED COMMON LOG FORMAT	SOIM
EXTENSIBLE - ACCESS CONTROL MARKUP LANGUAGE (XACML)	AAA
EXTENSIBLE - MARKUP LANGUAGE (XML)	WAM
EXTENSIBLE - MESSAGING AND PRESENCE PROTOCOL (XMPP)	WAM
EXTENSIBLE AUTHENTICATION PROTOCOL	NS
EXTERIOR GATEWAY PROTOCOL (EGP)	NS
EXTERNAL AUDITS	SOIM
EXTERNAL DATA SOURCES	F
EXTERNAL PROGRAM DRIVERS	LR
EXTERNAL PROJECTS TRACKING	SOIM
EXTERNAL SUBSYSTEMS NIST SP 800-37 REVISION 1 GUIDANCE ON	RMG
EXTRA EXPENSE (INSURANCE COVERAGE)	SOIM
EXTRADITION OF NATURAL PERSONS	LR
EXTRANET	NS
EYE FEATURES (BIOMETRICS)	AAA

F

FABRIC SHORTEST PATH FIRST (FSPF)	NS
FACETS OF AUTHENTICATION	AAA
FACIAL IMAGE	AAA
FACIAL RECOGNITION	AAA
FACILITATED RISK ANALYSIS PROCESS (FRAP)	RMG
FACILITATING AND ACTING ON VULNERABILITY DISCLOSURE	LR
FACILITY MANAGER RESPONSIBILITIES OF	RMG
FACTOR ANALYSIS OF INFORMATION RISK (FAIR)	RMG
FACTORING ATTACKS	C
FACTORIZATION	C
FAIL-OVER	SOIM
FAIL-SAFE	SOIM
FAIL-SAFE DEFAULTS	CI
FAILURE - MODES	SSL
FAILURE - MODES AND EFFECT ANALYSIS (FMEA)	SSL
FAILURE OF DEVICE	CI
FAILURE OF NETWORK	CI
FAILURE OF SERVICE	CI
FAILURE TO CAPTURE	AAA
FAILURE-TO-ENROLL RATE (FER)	AAA
FAILURES AND INCIDENTS	CI
FAIR	RMG
FAKE ACCOUNTS	AB
FALL-THROUGH LOGIC	SS
FALLBACK (ROLLBACK)	SOIM
FALSE ACCEPTS	AAA
FALSE REJECTS	AAA
FALSE-REJECTION RATE (FRR)	AAA
FAST FLUX	AB
FAULT - TOLERANCE	SOIM
FAULT - TREE ANALYSIS	SSL
FAULT TOLERANCE	CPS
FAULT TREE ANALYSIS	SSL
FAULT-INJECTION ATTACKS	SS
FC (FUNCTION CONTROL MODULE)	OSV
FC OVER IP (FCIP)	NS
FCOE (FIBRE CHANNEL OVER ETHERNET)	NS
FCP (FIBER CHANNEL PROTOCOL)	NS
FDDI (FIBER DISTRIBUTED DATA INTERFACE)	NS
FEAR UNCERTAINTY AND DOUBT	HF
FEASIBILITY STUDY	RMG
FEATURE REPLAY	PLT
FEATURES	PLT
FEDERAL - INFORMATION PROCESSING STANDARDS (FIPS)	RMG
FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)	RMG
FEDERATED ACCESS CONTROL	AAA
FEDERATED IDENTITY	AAA
FEDERATED IDENTITY - MANAGEMENT	AAA
FEDERATED IDENTITY MANAGEMENT	DSS
FEEDBACK-BASED TRANSPARENCY	POR
FEEDTHROUGH	NS MAT
FEISTEL NETWORKS	C
FF (FILE FLAG MODULE)	OSV
FIBER - DISTRIBUTED DATA INTERFACE (FDDI)	PLT
FIBER-OPTIC	PLT
FIBRE CHANNEL OVER ETHERNET (FCOE)	NS
FIDELITY COVERAGE (INSURANCE COVERAGE)	SOIM
FIDO UAF	AAA
FIELD PROGRAMMABLE GATA ARRAY (FPGA)	HS
FIELDBUS	CPS
FIELDBUS PROTOCOL	CPS
FILE - CONTENTS	F
FILE - TRANSFER ACCESS AND MANAGER (FTAM)	NS
FILE - TRANSFER PROTOCOL (FTP)	NS
FILE - TRANSFER PROTOCOL (FTP) - ANONYMOUS	NS
FILE EXTENSIONS MALCODE AND	MAT
FILE INFECTORS	MAT
FILE INFORMATION	F
FILE INTEGRITY CHECKERS	C

H

H.245 (CALL CONTROL PROTOCOL FOR MULTIMEDIA COMMUNICATION)	NS	HUMAN ERROR	SSL HF
HACK-BACK	LR	HUMAN FACTORS AND RISK COMMUNICATION	RMG
HACKER	AB	HUMAN FACTORS IN INFORMATION SECURITY	HF
HACKING	HF	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
HACKTIVISTS	AB	HUMAN RIGHTS	LR
HAIPE (HIGH ASSURANCE INTERNET PROTOCOL ENCRYPTOR)	NS	HUMAN SERVICES	AB
HALF DUPLEX	PLT	HUMAN-MACHINE INTERFACE (HMI)	CPS
HAND GEOMETRY	AAA	HWAM (HARDWARE ASSET MANAGEMENT)	SOIM
HANDLE: ACTUAL INCIDENT RESPONSE	SOIM	HYBRID	DSS
HANDLING - REQUIREMENTS	SOIM	HYBRID CONTROLS	SOIM
HANDSHAKING	NS	HYBRID CRYPTOGRAPHY	C
HARD PROBLEMS	C	HYBRID EXECUTION	MAT
HARD TOKEN	AAA	HYBRID MICROKERNEL ARCHITECTURE	OSV
HARDENED	SSL	HYBRID P2P PROTOCOLS	DSS
HARDWARE - SEGMENTATION	OSV	HYBRID SYSTEMS	CPS
HARDWARE - FORENSICS AND	F	HYPertext MARKUP LANGUAGE (HTML)	WAM
HARDWARE - INSIDER THREATS	AB HS	HYPertext TRANSFER PROTOCOL (HTTP)	WAM NS
HARDWARE - NETWORKS	NS	HYPertext TRANSFER PROTOCOL (HTTP) - PROXYING	WAM
HARDWARE - SEGMENTATION	HS	HYPertext TRANSFER PROTOCOL (HTTP) - TUNNELING	WAM
HARDWARE - VULNERABILITIES AND	HS	HYPervisor SUPPORTED INTROSPECTION	OSV
HARDWARE DESIGN CYCLE	HS	HYPervisors	OSV
HARDWARE DESIGN FOR CRYPTOGRAPHIC ALGORITHMS	HS		
HARDWARE DESIGN PROCESS	HS		
HARDWARE SECURITY MODULE (HSM)	HS		
HARDWARE SHADOW STACKS	HS		
HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS		
HARMFUL EFFECT OF DESIGN CHOICES	CI		
HARRISON, RUZO AND ULLMAN MODEL	AAA		
HASH	C	IAAA MODEL OF ACCESS CONTROL	AAA
HASH ALGORITHMS	HS	IAAS	F DSS
HASH FUNCTION	C	IAAS (INFRASTRUCTURE AS A SERVICE)	DSS
HASH FUNCTIONS	C	IBM 4758 SECURE COPROCESSOR	HS
HASH FUNCTIONS - ATTACKS	C	ICMP (INTERNET CONTROL MESSAGE PROTOCOL)	NS
HASH FUNCTIONS - BIRTHDAY PARADOX	C	ICMP REDIRECT ATTACKS	NS
HASH FUNCTIONS - HAVAL	C	ICS AND CNI	RMG
HASH FUNCTIONS - MD (MESSAGE DIGEST) 2 4 AND 5	C	IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM)	C
HASH FUNCTIONS - RIPEMD-160	C	IDENTIFICATION	AAA PLT
HASH FUNCTIONS - SALTING	C	IDENTIFICATION AND AUTHENTICATION	AAA
HASH FUNCTIONS - SHA (SECURE HASH ALGORITHM) 0 1 AND 2	C	IDENTIFICATION METHODS	AAA
HASH-CHAIN	AAA	IDENTIFICATION METHODS - ACCOUNT NUMBER/PIN	AAA
HASHED MESSAGE AUTHENTICATION CODE (HMAC)	C	IDENTIFICATION METHODS - IP ADDRESS	AAA
HAVAL	C	IDENTIFICATION METHODS - MAC ADDRESS	AAA
HAYSTACK AND NIDES	SOIM	IDENTIFICATION METHODS - RADIO FREQUENCY IDENTIFICATION (RFID)	AAA
HEAD OF AGENCY RESPONSIBILITIES OF	RMG	IDENTIFICATION METHODS - USER ID	AAA
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)	LR	IDENTIFICATION SIGNALS	PLT
HEARTBLEED	WAM	IDENTIFYING THE PRESENCE OF MALWARE	MAT
HEURISITIC STATIC DETECTION	SS	IDENTITY - AS A SERVICE (IDAAS)	AAA
HEURISTICS	MAT	IDENTITY - MANAGEMENT	AAA
HIDING	HS	IDENTITY AS A SERVICE (IDAAS)	AAA
HIDS (HOST-BASED IDS)	SOIM	IDENTITY BASED ACCESS CONTROL	AAA
HIERARCHICAL DATABASE	OSV	IDENTITY MANAGEMENT	AAA
HIERARCHICAL FILESYSTEMS	OSV	IDENTITY THEFT BOTNETS	MAT
HIERARCHICAL P2P PROTOCOLS	DSS	IDENTITY-BASED ENCRYPTION	C
HIERARCHICAL RBAC	AAA	IDMEF	SOIM
HIERARCHIES - DNS	NS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS)	SOIM
HIGH AVAILABILITY	SOIM	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - IDSES (INTRUSION DETECTION SYSTEMS)	NS
HIGH PERFORMANCE COMPUTING	DSS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - INCIDENT RESPONSE AND SOIM	
HIGH-AVAILABILITY CONSIDERATIONS	OSV	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - NETWORK TAPS	NS
HIGH-LEVEL DATA LINK CONTROL (HDLC)	PLT	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - NETWORKS	NS
HIGH-PROFILE REAL-WORLD ATTACKS	CPS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - SCANNERS	NS
HIGHER-ORDER INJECTION VULNERABILITIES	SS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - SEM (SECURITY EVENT MANAGEMENT)	SOIM
HINFO (HOST INFORMATION RECORDS)	NS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - SIEM (SECURITY INCIDENT AND EVENT MANAGEMENT)	SOIM
HISTORICAL ANOMALIES	CPS	IDPS (INTRUSION DETECTION AND PREVENTION SYSTEMS) - WIRELESS NETWORKS	NS
HISTORICAL SIGNATURES	MAT	IDS (INTRUSION DETECTION SYSTEM)	SOIM
HISTORY-CENTRIC	F	IDS ANALYSIS ENGINE METHODS	SOIM
HMAC (HASHED MAC)	C	IDSES (INTRUSION DETECTION SYSTEMS)	NS
HMI (HUMAN-MACHINE INTERFACE)	CPS	IDSES (INTRUSION DETECTION SYSTEMS) - HIDS (HOST-BASED IDS)	NS
HOAXES	MAT	IDSES (INTRUSION DETECTION SYSTEMS) - IDPS AND	SOIM
HOL	FMS	IDSES (INTRUSION DETECTION SYSTEMS) - INCIDENT RESPONSE AND	SOIM
HOLISTIC APPROACHES TO LEGAL RISK ANALYSIS	LR	IDSES (INTRUSION DETECTION SYSTEMS) - MOTION ACTIVATED CAMERAS	SOIM
HOMOMORPHIC ENCRYPTION	POR OSV	IEC 104	CPS
HOMOMORPHIC ENCRYPTION SCHEMES	HS	IEC 31010:2009	RMG
HOMOMORPHIC ENCRYPTION-BASED SCHEMES	POR	IEC 62351	CPS
HONEYNET	SOIM	IED (INTELLIGENT ELECTRONIC DEVICES)	CPS
HONEYPOT	SOIM	IEEE 802.1AE (MACSEC)	NS
HONEYPOTS AND HONEYNETS	SOIM	IEEE 802.1AR	HS
HOST INTRUSION DETECTION SYSTEM	NS	IEEE 802.1X	NS
HOST-BASED	MAT	IEEE 802.LAE (MACSEC)	RMG
HOST-BASED FIREWALLS	NS	IEEE 802.LAR	RMG
HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)	OSV	IEEE CENTER FOR SECURE DESIGN PRINCIPLES	SSL
HOSTING ORGANIZATION ROLE OF IN CERTIFICATION - TESTING	SOIM	IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)	NS
HOSTING ORGANIZATION ROLE OF IN CERTIFICATION - TESTING - CT ANALYSIS	RMG	IKE (INTERNET KEY EXCHANGE)	C
HOSTNAMES DNS AND	NS	IM (INSTANT MESSAGING) ATTACKS	WAM MAT
HOSTS FILES	OSV	IMAP (INTERNET MESSAGE ACCESS PROTOCOL)	WAM
HOT PRODUCTS	AB	IMAP (INTERNET MESSAGE ACCESS PROTOCOL) - NETWORK MAPPING AND	WAM
HOT SITES	SOIM	IMMUNIZER	MAT
HOT SPOTS	AB	IMMUTABLE STATE	SS
HTML5 LOCAL STORAGE	F	IMPACT	RMG
HTML5-BASED STORAGE	WAM	IMPACT - AS KEY RISK INDICATOR	RMG
HTTP (HYPertext TRANSFER PROTOCOL)	NS	IMPACT - IN RISK ASSESSMENT	RMG
HTTP AUTHENTICATION	WAM	IMPACT - RISK LIKELIHOOD	RMG
HTTP/HTTPS	NS	IMPACT ANALYSIS	RMG
HTTPS	NS	IMPACT ASSESSMENT	RMG
HTTPS MISCONFIGURATIONS	WAM	IMPACT OF USER RATINGS AND REVIEWS ON APPLICATION SECURITY	WAM
HUBS	NS	IMPERSONATION	NS AB
HUMAN BIASES	HF		
HUMAN CAPABILITIES AND LIMITATIONS	HF		

IMPLANTABLE MEDICAL DEVICES	CPS	INDUSTRY PRACTICES AND STANDARDS	CPS
IMPLEMENTATION	SOIM	INDUSTRY-SPECIFIC REGULATIONS	LR
IMPLEMENTATION - FASTER WITH CLOUD COMPUTING	DSS	INERTIAL RESETS	CPS
IMPLEMENTATION - IN RISK MANAGEMENT FRAMEWORK	RMG	INFECTED FACTORY BUILDS	AB
IMPLEMENTATION - OF INFORMATION SECURITY GOVERNANCE ACTION PLAN FOR RMG		INFECTION VECTORS	AB
IMPLEMENTATION - OF RESPONSE AND RECOVERY STRATEGIES	SOIM	INFERENCE	AB POR
IMPLEMENTATION - OF RISK MANAGEMENT	RMG	INFERRED CHARACTERISTICS	PLT
IMPLEMENTATION ATTACKS	SS	INFORMATION	SOIM RMG
IMPLEMENTATION PHASE	SSL	INFORMATION - DISCLOSURE	SOIM AB
IMPORT/EXPORT	LR	INFORMATION - GATHERING	AB
IMPROPER ACCESS TO A SYSTEM	LR	INFORMATION - INFRASTRUCTURE - AS A SERVICE (IAAS)	DSS
IMPROPER INTERCEPTION OF COMMUNICATION	LR	INFORMATION - INFRASTRUCTURE - MODE	NS
IMPROPER INTERFERENCE WITH DATA	LR	INFORMATION - SECURITY CONTINUOUS MONITORING (ISCM)	RMG
IMPROPER INTERFERENCE WITH SYSTEMS	LR	INFORMATION - SECURITY EFFORTS	SOIM
IMPROVEMENTS MEASURING	SOIM	INFORMATION - SECURITY MANAGEMENT SYSTEM (ISMS)	SOIM
IMPROVING MEMORY	HF	INFORMATION - SECURITY OFFICER - RESPONSIBILITIES	RMG
IN-LINE REFERENCE MONITORS	AAA	INFORMATION - SECURITY STRATEGIES	RMG
IN-SPECIFICATION	PLT	INFORMATION - SYSTEMS	RMG
INBOUND TRANSACTIONS	NS	INFORMATION - SYSTEMS - AUDITOR	SOIM
INCENTIVES	CPS	INFORMATION - SYSTEMS - SECURITY - EVALUATION MODELS	SSL
INCENTIVES AND REGULATION	CPS	INFORMATION - SYSTEMS - SECURITY - PROFESSIONAL	SOIM
INCIDENT	SOIM	INFORMATION - TECHNOLOGY (IT) - SECURITY EVALUATION CRITERIA (ITSEC)	SOIM
INCIDENT AND INFORMATION EXCHANGE	SOIM	INFORMATION AS A SERVICE (IAAS)	DSS
INCIDENT HANDLING AND RESPONSE	SOIM	INFORMATION ASSET CLASSIFICATION	RMG
INCIDENT MANAGEMENT	SOIM CPS	INFORMATION ASSURANCE (IA) CONTROLS	SSL
INCIDENT MANAGEMENT - BUSINESS CONTINUITY PLANS	SOIM RMG	INFORMATION CATEGORIES	POR
INCIDENT MANAGEMENT - CURRENT STATE OF	SOIM	INFORMATION DISCLOSURE SPOOFING	AB
INCIDENT MANAGEMENT - DEFINITION OF	SOIM	INFORMATION FLOW	SS FMS
INCIDENT MANAGEMENT - DISASTER RECOVERY PLANS	SOIM	INFORMATION FLOW ANALYSIS	SS HS
INCIDENT MANAGEMENT - IN ORGANIZATION	SOIM	INFORMATION GATHERING	AB
INCIDENT MANAGEMENT - INCIDENT RESPONSE PLAN	SOIM	INFORMATION HIDING	OSV
INCIDENT MANAGEMENT - INCIDENT RESPONSE PROCEDURES	SOIM	INFORMATION LEAK ATTACK	SS
INCIDENT MANAGEMENT - METRICS FOR	SOIM	INFORMATION LEAKS IN ANDROID APPLICATIONS	WAM
INCIDENT MANAGEMENT - OBJECTIVES OF	SOIM	INFORMATION OWNER/CUSTODIAN RESPONSIBILITIES OF	RMG
INCIDENT MANAGEMENT - OVERVIEW OF	SOIM	INFORMATION OWNER/STEWARDS RESPONSIBILITIES OF	RMG
INCIDENT MANAGEMENT - POST-INCIDENT ACTIVITIES AND INVESTIGATION	SOIM	INFORMATION OWNERS	RMG
INCIDENT MANAGEMENT - PROCEDURES FOR	SOIM	INFORMATION PROCESSING FACILITY (IPF)	DSS
INCIDENT MANAGEMENT - SELF-ASSESSMENT	SOIM	INFORMATION RECONCILIATION	PLT
INCIDENT MANAGEMENT - TESOURCES FOR	SOIM	INFORMATION SECURITY ARCHITECT RESPONSIBILITIES OF	RMG
INCIDENT MANAGEMENT - TESTING INCIDENT RESPONSE	SOIM	INFORMATION SECURITY ARCHITECT RESPONSIBILITIES OF - M) STRATEGY NIST GUIDANCE ON	SOIM
INCIDENT MANAGEMENT SYSTEMS	SOIM	INFORMATION SECURITY GOVERNANCE	RMG
INCIDENT RESPONSE	SOIM	INFORMATION SECURITY GOVERNANCE - ACTION PLAN FOR IMPLEMENTATION OF RMG	
INCIDENT RESPONSE - ANALYSIS	SOIM	INFORMATION SECURITY GOVERNANCE - DEFINED	RMG
INCIDENT RESPONSE - ANTI-MALWARE SYSTEMS AND	SOIM	INFORMATION SECURITY GOVERNANCE - DETERMINING CURRENT STATE OF	RMG
INCIDENT RESPONSE - AS OPERATIONAL ACTIVITY	SOIM	INFORMATION SECURITY GOVERNANCE - EFFECTIVE	RMG
INCIDENT RESPONSE - COMMUNICATION - LAW ENFORCEMENT	SOIM	INFORMATION SECURITY GOVERNANCE - METRICS FOR	SOIM RMG
INCIDENT RESPONSE - COMMUNICATION - MEDIA AND	SOIM	INFORMATION SECURITY GOVERNANCE - OVERVIEW OF	RMG
INCIDENT RESPONSE - COMMUNICATION - OFFICIAL ORGANIZATIONS/AGENCIES	SOIM	INFORMATION SECURITY GOVERNANCE - PROGRAM OBJECTIVES	SOIM
INCIDENT RESPONSE - COMMUNICATION - PLANNING	SOIM	INFORMATION SECURITY GOVERNANCE - RISK MANAGEMENT ROLES AND RESPONSIBILITIES IN	RMG
INCIDENT RESPONSE - COMMUNICATION - PUBLIC RELATIONS AND	SOIM	INFORMATION SECURITY GOVERNANCE - ROLES AND RESPONSIBILITIES IN	RMG
INCIDENT RESPONSE - CONTAINMENT	SOIM	INFORMATION SECURITY GOVERNANCE - SELF-ASSESSMENT	RMG
INCIDENT RESPONSE - COUNTERMEASURES IMPLEMENTATION	SOIM	INFORMATION SECURITY GOVERNANCE - STRATEGY CONSTRAINTS	RMG
INCIDENT RESPONSE - DEFINED	SOIM	INFORMATION SECURITY MANAGER	RMG
INCIDENT RESPONSE - DETECTION	SOIM	INFORMATION SECURITY PROBLEM MANAGEMENT	SOIM
INCIDENT RESPONSE - ERADICATION	SOIM	INFORMATION SECURITY PROGRAM	SOIM
INCIDENT RESPONSE - FORENSICS	F	INFORMATION SECURITY STRATEGY - ACTION PLAN TO IMPLEMENT	RMG
INCIDENT RESPONSE - FORENSICS - CRIME SCENES	F	INFORMATION SECURITY STRATEGY - CONSTRAINTS FOR	RMG
INCIDENT RESPONSE - FORENSICS - EMBEDDED DEVICE ANALYSIS	F	INFORMATION SECURITY STRATEGY - DETERMINING CURRENT STATE OF SECURITY FOR	RMG
INCIDENT RESPONSE - FORENSICS - EVIDENCE GATHERING	F	INFORMATION SHARING AND ANALYSIS CENTER (ISAC)	SOIM
INCIDENT RESPONSE - FORENSICS - EVIDENCE IDENTIFICATION	F	INFORMATION SHARING AND ANALYSIS CENTRES	SOIM
INCIDENT RESPONSE - FORENSICS - FINDINGS	F	INFORMATION SYSTEM - CATEGORIZATION	SOIM
INCIDENT RESPONSE - FORENSICS - GUIDELINES	F	INFORMATION SYSTEM LEVEL (TIER 3) RISK MANAGEMENT FOR	SOIM RMG
INCIDENT RESPONSE - FORENSICS - HARDWARE ANALYSIS	F	INFORMATION SYSTEM RISK MANAGEMENT FUNDAMENTAL CONCEPTS OF	RMG
INCIDENT RESPONSE - FORENSICS - INVESTIGATIONS	SOIM F	INFORMATION SYSTEM RISK MANAGEMENT FUNDAMENTAL CONCEPTS OF - RMATION	
INCIDENT RESPONSE - FORENSICS - MEDIA ANALYSIS	F	SYSTEM SECURITY ENGINEER RESPONSIBILITIES OF	RMG
INCIDENT RESPONSE - FORENSICS - NETWORK ANALYSIS	F	INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)	RMG
INCIDENT RESPONSE - FORENSICS - PROCEDURES	F	INFORMATION TECHNOLOGY SECURITY MANAGER SYSTEM INVENTORY PROCESS	
INCIDENT RESPONSE - FORENSICS - SOFTWARE ANALYSIS	F	RESPONSIBILITY OF	RMG
INCIDENT RESPONSE - IDS AND	SOIM	INFORMATION TECHNOLOGY SECURITY PROGRAM STEERING COMMITTEE	
INCIDENT RESPONSE - IN SECURITY PROGRAM MANAGEMENT	SOIM	RESPONSIBILITIES OF	RMG
INCIDENT RESPONSE - INDICATORS	SOIM	INFORMATION-THEORETICALLY SECURE CONSTRUCTIONS	C
INCIDENT RESPONSE - IPSS AND	SOIM	INFORMATIONAL COMPONENTS FOR INFORMATION SECURITY FRAMEWORK	SOIM
INCIDENT RESPONSE - NIST GUIDELINES	SOIM	INFORMATIONAL SYSTEMS	DSS
INCIDENT RESPONSE - NVD (NATIONAL VULNERABILITY DATABASE)	SOIM	INFRARED DATA ASSOCIATION (IRDA)	NS
INCIDENT RESPONSE - PHASES	SOIM	INFRASTRUCTURE	AB
INCIDENT RESPONSE - POLICIES	SOIM	INFRASTRUCTURE - MONITORING SECURITY ACTIVITIES IN	SOIM
INCIDENT RESPONSE - PRECURSORS	SOIM	INFRASTRUCTURE - OF SECURITY PROGRAMS	SOIM
INCIDENT RESPONSE - RECOVERY - BACKUPS	SOIM	INFRASTRUCTURE - TESTING IN INCIDENT MANAGEMENT	SOIM
INCIDENT RESPONSE - RECOVERY - CONTINUITY AND	SOIM	INFRASTRUCTURE MODE	NS
INCIDENT RESPONSE - RECOVERY - DISASTER RECOVERY	SOIM	INHERENT RISK	RMG
INCIDENT RESPONSE - RECOVERY - PLAN TESTING	SOIM	INHERITANCE	SS
INCIDENT RESPONSE - SIEM SOLUTIONS AND	F	INHERITANCE PERMISSIONS	OSV
INCIDENT RESPONSE - TEAM	SOIM	INITIALIZATION VECTOR (IV)	C
INCIDENT RESPONSE - TESTING	SOIM	INJECTION VULNERABILITIES	WAM
INCIDENT RESPONSE - USER REPORTS	SOIM	INPUT SANITISATION	WAM
INCIDENT RESPONSE AND	SOIM	INPUT/OUTPUT (I/O) - SERVER	CPS
INCIDENT RESPONSE PLAN (IRP)	SOIM	INSIDER THREATS	AB
INCIDENT RESPONSE PROCEDURES	SOIM	INSTALLATION	AB MAT
INCIDENT RESPONSE TEAMS (IRTS)	SOIM	INSTANT MESSAGE ACCESS PROTOCOL (IMAP)	NS
INCIDENTS AND FEEDBACK	SSL	INSTANT MESSAGING	WAM
INCOMPLETE PARAMETER CHECK	SS	INSURANCE	RMG
INCREMENTAL BACKUPS	SOIM	INSURANCE - AND SECURITY PROGRAMS	SOIM
IDENTIFYING THE ANALYSIS ENVIRONMENT	MAT	INSURANCE - IN INCIDENT RESPONSE PLAN	SOIM
INDEPENDENT AUDITS	SOIM	INSURANCE - IN INFORMATION SECURITY STRATEGY	RMG
INDICATORS OF COMPROMISE	SOIM	INTEGRATED - SERVICES DIGITAL NETWORK (ISDN)	PLT
INDIRECT BRANCH TRACKING	OSV	INTEGRATED GOALS	RMG
INDISTINGUISHABILITY	C	INTEGRATED SERVICES DIGITAL NETWORK (ISDN)	PLT
INDUSTRIAL CONTROL SYSTEMS	CPS		
INDUSTRIAL CONTROL SYSTEMS (ICS)	CPS		
INDUSTRIAL ESPIONAGE	AB		

INTEGRATION PLATFORM AS A SERVICE (1PAAS)	DSS	EXPLOITATION	NS
INTEGRATION TESTING/INTERFACE TESTING	SSL	IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - TEARDROP	NS
INTEGRITY	MAT OSV FMS CI	IP (INTERNET PROTOCOL) - NETWORKS CLASSES	NS
INTEGRITY CODES	PLT	IP (INTERNET PROTOCOL) - ROUTING TABLES	NS
INTEL MPK	OSV	IP ADDRESS SPOOFING	NS
INTEL MPX	OSV	IP MASQUERADING	NS
INTEL SGX	OSV	IP NETWORK	NS
INTEL SOFTWARE GUARD EXTENSION (SGX)	HS	IP SECURITY (IPSEC)	NS
INTELLECTUAL PROPERTY	LR	IP SPOOFING	NS
INTELLECTUAL PROPERTY - LAWS	LR	IPAAS (INTEGRATION PLATFORM AS A SERVICE)	DSS
INTELLIGENT AND CONNECTED VEHICLES INITIATIVE	SSL	IPS (INTRUSION PREVENTION SYSTEM)	SOIM
INTELLIGENT ELECTRONIC DEVICES (IED)	CPS	IPSEC	NS
INTER-ASTERISK EXCHANGE (IAX)	NS	IPSEC - AUTHENTICATION	AAA
INTER-NETWORK PACKET EXCHANGE (IPX)	NS	IPSS (INTRUSION PREVENTION SYSTEMS)	SOIM
INTER-SWITCH LINK PROTOCOL (ISL)	NS	IPSS (INTRUSION PREVENTION SYSTEMS) - INCIDENT RESPONSE AND	SOIM
INTERACTION CONTEXT	HF	IPSS (INTRUSION PREVENTION SYSTEMS) - WIRELESS NETWORKS	NS
INTERCEPTION	F	IPV6	NS
INTERCEPTION BY A STATE	LR	IRC (INTERNET RELAY CHAT) - ATTACKS	MAT
INTERCEPTION BY PERSONS OTHER THAN STATES	LR	IRIS PATTERNS	AAA
INTERCONNECTION (ISO/OSD)	NS	IRIS SCAN	AAA
INTERCONNECTIVITY AGREEMENTS - INITIATION OF	SOIM	IRM (INFORMATION RIGHTS MANAGEMENT)	AAA
INTERDEPENDENCY	RMG	IRP (INCIDENT RESPONSE PLAN)	SOIM
INTERNAL AUDITS	SOIM	IRREGULARITIES	LR
INTERNAL CONTROL	RMG	IRTS (INCIDENT RESPONSE TEAMS)	SOIM
INTERNAL POLICIES AND STANDARDS	SSL	IS AUDIT	SOIM
INTERNAL USE DATA	POR	IS AUDIT FUNCTION	RMG
INTERNATIONAL - DATA ENCRYPTION ALGORITHM (IDEA)	C	IS CONTROL	SOIM
INTERNATIONAL - EXPORT CONTROLS	C	IS21434	SSL
INTERNATIONAL - ORGANIZATION FOR STANDARDIZATION (ISO)	RMG	ISA 99/IEC 62443	CPS
INTERNATIONAL - SECURITY IMPLEMENTATION GUIDELINES	SSL	ISABELLE	FMS
INTERNATIONAL - TELECOMMUNICATIONS UNION (ITU)	PLT	ISACA CISM CERTIFICATION	RMG
INTERNATIONAL - TELECOMMUNICATIONS UNION-TELECOMMUNICATIONS (ITU-T)	PLT	ISACA CODE OF PROFESSIONAL ETHICS	POR
INTERNATIONAL - TRAFFIC IN ARMS REGULATIONS (ITAR)	LR	ISACA IS AUDIT AND ASSURANCE STANDARDS	RMG
INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC)	RMG	ISAKMP (INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL)	WAM
INTERNATIONAL LEGAL ASSISTANCE	LR	ISATAP (INTRA-SITE AUTOMATIC TUNNEL ADDRESSING PROTOCOL)	NS
INTERNATIONAL NORMS	LR	ISCSI (INTERNET SMALL COMPUTER SYSTEM INTERFACE)	CPS
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)	RMG	ISDN (INTEGRATED SERVICES DIGITAL NETWORK)	NS
INTERNATIONAL TREATMENT AND CONFLICT OF LAW	LR	ISNS (INTERNET STORAGE NAME SERVICE)	NS
INTERNATIONALISED DOMAIN NAME HOMOGRAPHS ATTACKS	WAM	ISO	RMG
INTERNET	NS	ISO 20000	RMG
INTERNET - ACTIVITIES BOARD (IAB)	HF	ISO 27002:2013	RMG
INTERNET - CONTROL MESSAGE PROTOCOL (ICMP)	NS	ISO 2700X	RMG
INTERNET - CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)	NS	ISO 31000	RMG
INTERNET - ENGINEERING TASK FORCE (IETF)	RMG	ISO 31000:2009	RMG
INTERNET - FC PROTOCOL (IFCP)	NS	ISO/IEC 15504	RMG
INTERNET - GROUP MANAGEMENT PROTOCOL (IGMP)	NS	ISO/IEC 17799	RMG
INTERNET - KEY EXCHANGE (IKE)	C	ISO/IEC 27000 SERIES	RMG
INTERNET - PROTOCOL (IP)	NS	ISO/IEC 27001:2003	RMG
INTERNET - RELAY CHAT (IRC)	NS	ISO/IEC 27001:2013 - ACCESS CONTROL	AAA
INTERNET - SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL (ISAKMP)	NS	ISO/IEC 27001:2013 - ASSET MANAGEMENT	SOIM
INTERNET - SMALL COMPUTER SYSTEM INTERFACE (ISCSI)	HS	ISO/IEC 27001:2013 - COMMUNICATIONS SECURITY	RMG
INTERNET - SOCKET (SOCKS)	NS	ISO/IEC 27001:2013 - COMPLIANCE	RMG
INTERNET - STORAGE NAME SERVICE (ISNS)	NS	ISO/IEC 27001:2013 - CRYPTOGRAPHY	C
INTERNET ARCHITECTURE	NS	ISO/IEC 27001:2013 - DEVELOPMENT AND MAINTENANCE	SSL
INTERNET CONTROL MESSAGE PROTOCOL (ICMP)	NS	ISO/IEC 27001:2013 - INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY	SOIM
INTERNET INTERMEDIARIES	LR	ISO/IEC 27001:2013 - INFORMATION SECURITY POLICIES	SOIM
INTERNET KEY EXCHANGE PROTOCOL	NS	ISO/IEC 27001:2013 - ISO/IEC 27005	RMG
INTERNET OF THINGS	CPS	ISO/IEC 27001:2013 - MANAGEMENT	RMG
INTERNET OF THINGS SECURITY	NS	ISO/IEC 27001:2013 - OPERATIONS SECURITY	SOIM
INTERNET PROTOCOL (IP)	NS	ISO/IEC 27001:2013 - ORGANIZATION OF INFORMATION SECURITY	SOIM
INTERNET SERVICE PROVIDER (ISP)	NS DSS	ISO/IEC 27002 SERIES	RMG
INTERPERSONAL CRIMES	AB	ISO/IEC 27004:2009	RMG
INTERRUPTION WINDOW	SOIM	ISO/IEC 27005	RMG
INTERRUPTS - MASKABLE	OSV	ISO/IEC 27005:2011	RMG
INTRANET	WAM	ISO/IEC 27034	RMG
INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR	ISO/IEC 31000	RMG
INTRUDER	AB	ISO/IEC PROCESS STEPS	RMG
INTRUSION - DETECTION - PROTOCOL ANOMALY-BASED	SOIM	ISO/IEC PROCESS STEPS - LEGAL AND REGULATORY REQUIREMENTS IN	LR
INTRUSION - DETECTION - STATEFUL MATCHING	SOIM	ISO/IEC PROCESS STEPS - METHODOLOGIES OF	RMG
INTRUSION - DETECTION - STATISTICAL ANOMALY-BASED	SOIM	ISOAEC 27001	RMG
INTRUSION - DETECTION - TRAFFIC ANOMALY-BASED	SOIM	ISOAEC 27002:2013	SOIM RMG
INTRUSION - DETECTION SYSTEM (IDS) - ARCHITECTURE	NS	ISOAEC 27005	RMG
INTRUSION - DETECTION SYSTEM (IDS) - MANAGEMENT	SOIM	ISOLATION	HS OSV
INTRUSION - RESPONSE	SOIM	ISP (INTERNET SERVICE PROVIDER)	DSS
INTRUSION DETECTION	SOIM CPS MAT	ISSO - RESPONSIBILITIES OF	RMG
INTRUSION DETECTION SYSTEM (IDS)	SOIM	ISSO - RESPONSIBILITIES OF - SECURITY PLANNING	SOIM
INTRUSION DETECTION SYSTEMS	NS	ISSO - ROLE OF IN CONTINUOUS MONITORING	RMG
INTRUSION PREVENTION SYSTEM	NS	ISSO - SYSTEM INVENTORY PROCESS RESPONSIBILITY OF	RMG
INTRUSION PREVENTION SYSTEM (IPS)	SOIM	ISSO - USE OF RISK REMEDIATION PLAN BY	SOIM RMG
INTRUSION PREVENTION SYSTEMS	SOIM	ISSUES - LEGAL AND REGULATORY	LR
INTRUSIONS	AB	IT - AS OPERATIONAL ACTIVITY	SOIM
INVENTORY CHANGE FORM	SOIM	IT - IN SECURITY PROGRAM MANAGEMENT	SOIM
INVENTORY DATA REQUIREMENTS	SOIM	IT AUDIT	RMG
INVESTIGATION	SOIM	IT EQUIPMENT AND FACILITIES (INSURANCE COVERAGE)	SOIM
INVESTIGATION AND PREVENTION OF CRIME	LR	IT GOVERNANCE	RMG
INVESTIGATIVE PHASE	SOIM	IT INFRASTRUCTURE LIBRARY (ITIL)	RMG
INVOLVEMENT	RMG	IT INFRASTRUCTURE LIBRARY (ITIL) - SERVICE DESIGN	RMG
IO (INPUT/OUTPUT) SERVER	CPS	IT INFRASTRUCTURE LIBRARY (ITIL) - SERVICE STRATEGY	RMG
IOCE (INTERNATIONAL ORGANIZATION OF COMPUTER EVIDENCE)	F	IT INFRASTRUCTURE LIBRARY (ITIL) - SERVICE TRANSITION	RMG
IOT	SOIM SSL CPS OSV	IT OPERATIONS MANAGEMENT	SOIM
IP (INTERNET PROTOCOL)	NS	IT RISK MANAGEMENT	SOIM RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - FRAGGLE	NS	IT RISK MANAGEMENT LIFE CYCLE	SOIM RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - NFS	NS	IT RISK STRATEGY	RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - NNTP SECURITY	NS	IT STEERING COMMITTEE	RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - NTP	NS	IT STRATEGIC PLAN	RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - OVERLAPPING FRAGMENT	NS	IT STRATEGY COMMITTEE	RMG
ATTACK	NS	IT SYSTEM DEVELOPMENT LIFE CYCLE	SSL
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - SMURF	NS	ITAF	RMG
IP (INTERNET PROTOCOL) - FRAGMENTATION ATTACKS - SOURCE ROUTING	NS	ITAM (IT ASSET MANAGEMENT)	SOIM

ITIL RMG
ITSEC (INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA) SSL
IV (INITIALIZATION VECTOR) C

J

JABBER WAM
JAILS SS
JAMMING AND JAMMING-RESILIENT COMMUNICATION PLT
JAVA SS
JAVA - APPLET WAM
JAVA - SECURITY SS
JAVA APPLET ATTACK WAM MAT
JAVA APPLETS WAM
JAVA SECURITY MODEL AAA
JAVASCRIPT WAM
JERICO FORUM* SELF-ASSESSMENT SCHEME RMG
JITTER NS
JOB - TRAINING HF
JOINT ANALYSIS DEVELOPMENT (JAD) SSL
JURISDICTION LR
JUST CULTURE RMG

K

K-ANONYMITY POR
KADEMLIA DSS
KALI VIRTUAL - CONFIGURATION SOIM
KALI VIRTUAL - DOWNLOADING SOIM
KALI VIRTUAL - SCANS LAUNCHING SOIM
KAOS SSL
KASLR OSV
KASPERSKY SOIM
KDC (KEY DISTRIBUTION CENTER) C
KDFS (KEY DERIVATION FUNCTIONS) C
KEEP CREDENTIALS SAFE SSL
KEK (KEY ENCRYPTING KEYS) C
KERBEROS AAA C
KERCKHOFF'S PRINCIPLE C
KERCKHOFFS' PRINCIPLE C
KERNEL OSV
KERNEL MODE OSV
KERNEL-MODE ROOTKITS MAT
KEY C
KEY - CLUSTERING C
KEY - DERIVATION FUNCTIONS (KDFS) C
KEY - DISTRIBUTION C
KEY - ESCROW C
KEY - LENGTH C
KEY - MANAGEMENT C
KEY - RECOVERY C
KEY - STORAGE C
KEY - WRAPPING C
KEY AGREEMENT PROTOCOLS C
KEY CONFIRMATION C
KEY DERIVATION FUNCTIONS C
KEY DISTRIBUTION DSS
KEY ENCAPSULATION MECHANISMS C
KEY ESTABLISHMENT BASED ON CHANNEL RECIPROCITY PLT
KEY GOAL INDICATOR (KGI) RMG
KEY PERFORMANCE INDICATOR (KPI) RMG
KEY RISK INDICATOR (KRD) RMG
KEY RISK INDICATOR - EFFECTIVENESS RMG
KEY RISK INDICATOR - MAINTENANCE RMG
KEY RISK INDICATOR - OPTIMIZATION RMG
KEY RISK INDICATOR - SELECTION RMG
KEY RISK INDICATORS (KRIS) RMG
KEY TRANSPORT C
KEY VERIFICATION PLT
KEY-CENTRIC ACCESS CONTROL AAA
KEY-DERIVATION NS
KEY-POLICY ATTRIBUTE-BASED ENCRYPTION AAA
KEYLOGGERS MAT
KEYS C
KEYS - CLUSTERING C
KEYS - ENCRYPTION C
KEYS - ENCRYPTION - ASYMMETRIC C
KEYS - ENCRYPTION - AUTOMATED GENERATION C
KEYS - ENCRYPTION - CERTIFICATE REPLACEMENT C
KEYS - ENCRYPTION - CERTIFICATE REVOCATION C
KEYS - ENCRYPTION - CLUSTERING C
KEYS - ENCRYPTION - DESTRUCTION C
KEYS - ENCRYPTION - DISTRIBUTION C
KEYS - ENCRYPTION - DUTIES C
KEYS - ENCRYPTION - ESCROW C
KEYS - ENCRYPTION - FINANCIAL INSTITUTIONS C
KEYS - ENCRYPTION - KEY ENCRYPTING KEYS C
KEYS - ENCRYPTION - KMIP C
KEYS - ENCRYPTION - LENGTH C

KEYS - ENCRYPTION - MANAGEMENT C
KEYS - ENCRYPTION - PUBLIC C
KEYS - ENCRYPTION - RANDOMNESS C
KEYS - ENCRYPTION - RECOVERY F
KEYS - ENCRYPTION - SPACE C
KEYS - ENCRYPTION - STORAGE C
KEYS - ENCRYPTION - WEB OF TRUST C
KEYS - ENCRYPTION - WRAPPING C
KEYS - ENCRYPTION - X-KISS C
KEYS - ENCRYPTION - X-KRSS C
KEYS - ENCRYPTION - XKMS C
KEYS - FOREIGN KEYS C
KEYS - PRIMARY C
KEYS - PRIVATE C
KEYSPACE C
KEYSTREAM GENERATOR C
KEYSTROKE DYNAMICS AAA
KILL CHAINS AB
KINDS MAT
KMIP (KEY MANAGEMENT INTEROPERABILITY PROTOCOL) C
KNOWLEDGE (AUTHENTICATION) AAA
KNOWLEDGE: INTELLIGENCE AND ANALYTICS SOIM
KNOWN-PLAINTEXT ATTACK C
KOH SPEECH CPS
KPIS SSL

L

L-DIVERSITY POR
LANGUAGE DESIGN AND TYPE SYSTEMS SS
LANS (LOCAL AREA NETWORKS) - CONTROL PLANE NS
LANS (LOCAL AREA NETWORKS) - DATA PLANE NS
LARGE TRANSACTIONS DSS
LARGE-SCALE CONNECTED SYSTEMS CI
LAST-MILE CIRCUIT PROTECTION PLT
LATENCY NS
LATENT DESIGN CONDITIONS CI
LATENT USABILITY FAILURES IN SYSTEMS-OF-SYSTEMS HF
LATTICE-BASED CONSTRUCTIONS C
LATTICES AAA
LAW ENFORCEMENT F POR LR
LAW ENFORCEMENT INCIDENT RESPONSE AND LR
LAYER 2 TUNNELING PROTOCOL (L2TP) NS
LAYERED OPERATING SYSTEM ARCHITECTURE OSV
LAYERING WITH ARCHITECTURE SOIM
LAYERS OF SYSTEM STACK MAT
LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL) AAA
LEARNING RMG
LEASED LINES PLT
LEAST COMMON MECHANISM CI
LEAST PRIVILEGE SSL
LEDGERS DSS
LEEF SOIM
LEGACY SYSTEMS SOIM
LEGAL AND INDUSTRY REQUIREMENTS SSL
LEGAL AND REGULATORY FRAMEWORK LR
LEGAL AND REGULATORY REQUIREMENTS - FOR SECURITY PROGRAMS LR
LEGAL AND REGULATORY REQUIREMENTS - IN RISK ASSESSMENT LR
LEGAL ASPECTS - OF FORENSIC EVIDENCE F
LEGAL ASPECTS - OF INFORMATION SECURITY STRATEGY LR
LEGAL CHALLENGES F
LEGAL CONCERNS AND THE DAUBERT STANDARD F
LEGAL DEPARTMENT LR
LEGAL TERMINOLOGY LR
LEVEL OF EFFORT - CERTIFICATION SOIM
LEVEL OF EFFORT - DETERMINATION OF RMG
LEVEL OF EFFORT - EXAMPLE SECURITY MATRIX - IMPLEMENTATION OF RMF TASKS RMG
AND RMG
LEVEL OF EFFORT - EXAMPLE SECURITY MATRIX - METRICS TO MEASURE RMG
LEVELS OF PERCEIVED RISK RMG
LIABILITY SOIM RMG LR
LIABILITY AND COURTS LR
LICENSING AND INTELLECTUAL PROPERTY LR
LICENSING ISSUES LR
LIFE CYCLE PROCESSES - OF INCIDENT MANAGEMENT SOIM
LIFE-CYCLE PHASES - COMPARISON OF SOIM
LIGHT HF
LIGHT-WEIGHT SOLUTIONS HS
LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) AAA
LIGHTWEIGHT SECURITY CPS
LIKELIHOOD RMG
LIKELIHOOD AND CONSEQUENCES RATING RMG
LIKELIHOOD DETERMINATION RMG
LIKELIHOOD OF RISK RMG
LIMIT CHECK SOIM
LIMIT REGISTERS OSV
LIMITATIONS MAT
LIMITATIONS OF LIABILITY AND EXCLUSIONS OF LIABILITY LR
LIMITED CAPACITY SECURITY PROTOCOLS NS
LIMITED USER ACCOUNTS OSV
LIMITING PRIVILEGES SS
LINEAR CRYPTANALYSIS C
LINEARISABILITY DSS
LINEARLY HOMOMORPHIC ENCRYPTION C
LINK CONTROL PROTOCOL (LCP) PLT

LINK ENCRYPTION	NS	MALCODE/MALWARE - COUNTERMEASURES - TROJANS	MAT
LINK LAYER SECURITY	NS	MALCODE/MALWARE - COUNTERMEASURES - VIRUSES	MAT
LINK-STATE ROUTING PROTOCOL	NS	MALCODE/MALWARE - COUNTERMEASURES - WORMS	MAT
LIST FOLDER/READ DATA PERMISSION	OSV	MALCODE/MALWARE - DETECTION SYSTEM REQUIREMENTS	MAT
LIVENESS DETECTION	AAA	MALCODE/MALWARE - DOUBLE FILE EXTENSIONS	MAT
LLC (LOGICAL LINK CONTROL)	NS	MALCODE/MALWARE - DROPPERS	MAT
LNFIBAND (IB)	CPS	MALCODE/MALWARE - E-MAIL	MAT
LOAD BALANCERS	WAM	MALCODE/MALWARE - FAKE ICONS	MAT
LOAD BALANCING	NS	MALCODE/MALWARE - FAKE RELATED EXTENSION	MAT
LOAD-ALTERING ATTACKS	CPS	MALCODE/MALWARE - FEEDTROUGH	NS MAT
LOCAL AREA NETWORK (LAN)	NS	MALCODE/MALWARE - FILE INFECTORS	MAT
LOCAL FILE INCLUSION	WAM	MALCODE/MALWARE - INSIDER THREATS	AB
LOCALISED ECLIPSE ATTACKS	DSS	MALCODE/MALWARE - KEYLOGGERS	MAT
LOCATION AS BASIS FOR RECOVERY SITE SELECTION	SOIM	MALCODE/MALWARE - LOGIC BOMBS	MAT
LOCATION METADATA	POR	MALCODE/MALWARE - LOGIC BOMBS - COUNTERMEASURES	MAT
LOG - MANAGEMENT	SOIM	MALCODE/MALWARE - LONG FILE EXTENSIONS	MAT
LOG - REVIEWS	SOIM	MALCODE/MALWARE - MACRO VIRUSES	MAT
LOG FILES - CENTRALIZED LOGGING	SOIM	MALCODE/MALWARE - MITIGATION	MAT
LOG FILES - EVENT CORRELATION SYSTEMS	SOIM	MALCODE/MALWARE - MITM (MAN-IN-THE-MIDDLE)	MAT
LOG FILES - EVENT DATA ANALYSIS	SOIM	MALCODE/MALWARE - NAMING - CARO-LIKE STANDARDS	MAT
LOG FILES - EVENT SOURCE CONFIGURATION	SOIM	MALCODE/MALWARE - NAMING - CME	MAT
LOG FILES - FULL PACKET CAPTURE	NS	MALCODE/MALWARE - NAMING - CROSS-REFERENCING	MAT
LOG FILES - HOST LOGS	SOIM	MALCODE/MALWARE - NAMING - PUBLIC MULTISCANNERS	MAT
LOG FILES - HOSTED SERVICES	SOIM	MALCODE/MALWARE - NAMING - VGREP	MAT
LOG FILES - INCIDENT RESPONSE AND	SOIM	MALCODE/MALWARE - PAYLOADS	MAT
LOG FILES - NETFLOW (CISCO)	SOIM	MALCODE/MALWARE - PHISHING	AB
LOG FILES - SFLOW	SOIM	MALCODE/MALWARE - POC (PROOF OF CONCEPT)	MAT
LOGIC	HS	MALCODE/MALWARE - POP-UPS	WAM
LOGIC BOMBS	MAT	MALCODE/MALWARE - RAR	MAT
LOGICAL ACCESS CONTROLS	AAA	MALCODE/MALWARE - SOCIAL ENGINEERING - BAITING	MAT
LOGICAL ADDRESSES	NS	MALCODE/MALWARE - SOCIAL ENGINEERING - PHONE PHISHING	MAT
LOGICAL CONTROLS	SOIM	MALCODE/MALWARE - SOCIAL ENGINEERING - PRETEXTING	MAT
LOGICAL DATA ACQUISITION	F	MALCODE/MALWARE - SOCIAL ENGINEERING - SET (SOCIAL ENGINEERING TOOLKIT)	AB
LOGICAL SECURITY	SOIM	MALCODE/MALWARE - SOCIAL ENGINEERING - VISHING	MAT
LOGICAL VOLUMES	F	MALCODE/MALWARE - SPAM	WAM AB
LOGON LIMITATION	SOIM	MALCODE/MALWARE - SPOOFING	AB
LOGS	AAA	MALCODE/MALWARE - SPYWARE	MAT
LONG FILE EXTENSIONS	AB	MALCODE/MALWARE - SYSTEM REQUIREMENTS	MAT
LONG TERM MEMORY	HF	MALCODE/MALWARE - THIRD-PARTY CERTIFICATIONS	MAT
LONG-HAUL NETWORK DIVERSITY	NS PLT	MALCODE/MALWARE - TROJANS	MAT
LONG-TERM THINKING	SOIM RMG	MALCODE/MALWARE - TROJANS - BACKDOOR	MAT
LORA	SOIM	MALCODE/MALWARE - TROJANS - COUNTERMEASURES	MAT
LOW ORBIT ION CANNON	AB	MALCODE/MALWARE - VECTORS	MAT
LOW-END DEVICES AND IOT	OSV	MALCODE/MALWARE - VIRUSES	MAT
LPI AND COVERT COMMUNICATION	PLT	MALCODE/MALWARE - VIRUSES - BOOT SECTOR VIRUSES	MAT
LUA (LEAST USER ACCESS)	SSL	MALCODE/MALWARE - VIRUSES - COUNTERMEASURES	MAT
LUCKY THIRTEEN	NS	MALCODE/MALWARE - VIRUSES - MACRO VIRUSES	MAT
		MALCODE/MALWARE - VIRUSES - POLYMORPHIC	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - APTS	WAM
		MALCODE/MALWARE - WEB-BASED ATTACKS - BEHAVIOR ANALYSIS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - BEHAVIORAL ANALYSIS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - BRUTE FORCE	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - COUNTERMEASURES	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - DEGRADED PERFORMANCE	SOIM F
		MALCODE/MALWARE - WEB-BASED ATTACKS - DNS CHANGES AND	NS
		MALCODE/MALWARE - WEB-BASED ATTACKS - EXPLOITATION FRAMEWORKS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - FILE LOCATION INSPECTION	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - HOSTS FILES AND	OSV
		MALCODE/MALWARE - WEB-BASED ATTACKS - IM (INSTANT MESSAGING)	WAM MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - INFECTED FACTORY BUILDS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - IRC	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - P2P NETWORKS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - POP-UPS	WAM
		MALCODE/MALWARE - WEB-BASED ATTACKS - PROCESS INSPECTION	OSV
		MALCODE/MALWARE - WEB-BASED ATTACKS - REMOTE SITE TESTING	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - ROGUE PRODUCTS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - SANDBOX SOLUTIONS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - STATIC FILE ANALYSIS	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - VIRTUALIZED ENVIRONMENTS TESTING	MAT
		MALCODE/MALWARE - WEB-BASED ATTACKS - WINDOWS REGISTRY INSPECTION	SOIM
		MALCODE/MALWARE - WEB-BASED ATTACKS - XSS	SS
		MALCODE/MALWARE - WEB-BASED ATTACKS - ZERO-DAY EXPLOITS	MAT
		MALCODE/MALWARE - WILDLIST	MAT
		MALCODE/MALWARE - WINDOWS ROOTKIT	MAT
		MALCODE/MALWARE - WORMS	MAT
		MALCODE/MALWARE - WORMS - COUNTERMEASURES	MAT
		MALCODE/MALWARE - ZIP FILES	MAT
		MALICIOUS ACTIVITIES BY MALWARE	MAT
		MALICIOUS ATTACHMENTS	AB
		MALICIOUS BROWSER EXTENSIONS	MAT
		MALICIOUS CODE	MAT
		MALICIOUS EXTENSIONS	OSV
		MALWARE	MAT
		MALWARE - ASSURANCE	MAT
		MALWARE - CONTROL	MAT
		MALWARE - PROTECTION	MAT
		MALWARE - TYPES	MAT
		MALWARE ANALYSIS	MAT
		MALWARE DETECTION	MAT
		MALWARE DISTRIBUTION METHODS	MAT
		MALWARE INFECTION SITES	MAT
		MALWARE RESPONSE	MAT
		MALWARE TAXONOMY	MAT
		MAN (METROPOLITAN AREA NETWORK)	NS
		MAN LEFT IN THE MIDDLE ATTACK METHOD	WAM MAT
		MAN-HOUR PLANNING ESTIMATES	SOIM RMG
		MAN-IN-THE-MIDDLE	NS
		MAN-IN-THE-MIDDLE ATTACK (MITM)	MAT
		MAN-MADE THREATS	AB
MAC (MANDATORY ACCESS CONTROL)	AAA		
MAC (MEDIA ACCESS CONTROL)	C		
MAC (MESSAGE AUTHENTICATION CODE)	C		
MAC LAYER INTERPRETATION	SOIM		
MAC SPOOFING	NS		
MACHINE EMULATOR	MAT		
MACHINE LANGUAGE	MAT		
MACHINE LEARNING	SOIM		
MACHINE LEARNING ATTACKS	HS		
MACHINE LEARNING BASED TECHNIQUES	POR		
MACHINE LEARNING COUNTERMEASURES	MAT		
MACHINE LEARNING FOR MALWARE DETECTION	SOIM		
MACHINE LEARNING-BASED SECURITY ANALYTICS	MAT		
MACRO VIRUSES	MAT		
MACSEC (MEDIA ACCESS CONTROL SECURITY)	NS		
MAFIA FRAUD	PLT		
MAGNETIC CARD READERS	HS		
MAIL - TRANSFER AGENT (MTA)	WAM		
MAIL - USER AGENT (MUA)	WAM		
MAIL RELAY SERVER	NS		
MAIN MEMORY FORENSICS	F		
MAINFRAMES	DSS		
MAINTAIN	RMG		
MAINTENANCE - SECURITY PLANS	SOIM		
MAINTENANCE - SECURITY PROCEDURES	SOIM		
MAINTENANCE - SYSTEM INVENTORY PROCESS	SOIM		
MAINTENANCE HOOKS	MAT		
MALCODE/MALWARE - ADWARE	MAT		
MALCODE/MALWARE - BOOT SECTOR VIRUSES	MAT		
MALCODE/MALWARE - BOTNETS	MAT		
MALCODE/MALWARE - BOTS	MAT		
MALCODE/MALWARE - CIA TRIAD	MAT		
MALCODE/MALWARE - CODECS HOSTILE	MAT		
MALCODE/MALWARE - CONFIGURATION SYSTEM REQUIREMENTS	MAT		
MALCODE/MALWARE - COTTONMOUTH	HS MAT		
MALCODE/MALWARE - COUNTERMEASURES - APPLICATION CODE	MAT		
MALCODE/MALWARE - COUNTERMEASURES - BACKDOORS	MAT		
MALCODE/MALWARE - COUNTERMEASURES - BUFFER OVERFLOW ATTACK	MAT		
MALCODE/MALWARE - COUNTERMEASURES - CODE SIGNING	MAT		
MALCODE/MALWARE - COUNTERMEASURES - COVER CHANNELS	MAT		
MALCODE/MALWARE - COUNTERMEASURES - DIRECTORY TRAVERSAL	MAT		
MALCODE/MALWARE - COUNTERMEASURES - LOGIC BOMBS	MAT		
MALCODE/MALWARE - COUNTERMEASURES - POINTER OVERFLOW ATTACK	MAT		
MALCODE/MALWARE - COUNTERMEASURES - SANDBOXING	MAT		
MALCODE/MALWARE - COUNTERMEASURES - SCANNERS	MAT		

M

MANAGE SECURITY FINDINGS	SSL	METADATA CONFIDENTIALITY	POR
MANAGE THE SECURITY RISK OF USING THIRD-PARTY COMPONENTS	SSL	METASPLOIT BROWSER EXPLOIT METHOD	MAT
MANAGEMENT	SOIM RMG	METASPLOITABLE	SOIM
MANAGEMENT COMPONENTS FOR INFORMATION SECURITY FRAMEWORK	SOIM	METHOD (GRAMM)	RMG
MANAGEMENT CONTROLS	RMG	METHODOLOGICAL DESIGN	SSL
MANAGEMENT FRAMEWORK	RMG	METHODOLOGICAL TESTING	SSL
MANAGEMENT MODEL - HIERARCHICAL DATABASE	OSV	METHODS OF ATTACK	SSL
MANAGEMENT MODEL - NETWORK DATABASE	OSV	METRICS	RMG
MANAGEMENT MODEL - RELATIONAL DATABASE	OSV	METRICS - FOR ACTION PLAN	HF
MANAGEMENT SUPPORT - FOR INCIDENT MANAGEMENT	SOIM	METRICS - FOR INCIDENT MANAGEMENT	SOIM
MANAGEMENT SUPPORT - FOR INFORMATION SECURITY	RMG	METRICS - FOR INFORMATION SECURITY GOVERNANCE	SOIM RMG
MANAGEMENT SUPPORT TECHNOLOGIES	SOIM	METRICS - FOR RECOVERY TESTS	F
MANAGERIAL CONTROLS	RMG	METRICS - FOR SECURITY PROGRAMS	SOIM
MANAGERIAL CONTROLS - GUIDELINES	RMG	METRICS - SECURITY PLAN	SOIM
MANAGERIAL CONTROLS - POLICY DOCUMENTS	RMG	METRO ETHERNET	NS
MANAGERIAL CONTROLS - POLICY LIFECYCLE	RMG	MICRO-ARCHITECTURAL EFFECTS	SS
MANAGERIAL CONTROLS - PROCEDURES	RMG	MICRO-ARCHITECTURAL SIDE-CHANNELS	HS
MANAGERIAL CONTROLS - STANDARDS	RMG	MICRO-CODE UPDATES	HS
MANDATORY - ACCESS CONTROL (MAC)	AAA	MICROCHIP	HS
MANDATORY ACCESS CONTROL (MAC)	AAA	MICROCOMPUTER	CPS
MANDATORY ACCESS CONTROLS	AAA OSV	MICROECONOMIC THEORY	CI
MANDATORY ACCESS CONTROLS (MAC)	AAA	MICROKERNEL ARCHITECTURE	OSV
MANDATORY ACCESS CONTROLS (MACS)	AAA	MICROKERNEL BASED MULTI-SERVER	OSV
MANUAL CODE REVIEW	SSL	MICROSOFT SDL	SSL
MANUFACTURING MESSAGING SERVICE (MMS)	NS	MIDDLEWARE	SOIM DSS
MAPE-K	SOIM	MILESTONES	RMG
MARKING	SOIM	MILESTONES - INCLUSION OF IN RISK REMEDIATION PLAN	SOIM
MARKOV ANALYSIS	RMG	MIME (MULTIPURPOSE INTERNET MAIL EXTENSION)	WAM
MASKABLE INTERRUPT	OSV	MIMICKING	POR
MASKING	SOIM HS	MIMO-SUPPORTED APPROACHES	PLT
MASQUERADERS	AB	MINIMISE CENTRALIZATION	POR
MASQUERADING	NS	MINIMISE COLLECTION	POR
MASTER FILE	NS	MINIMISE DISCLOSURE	POR
MATRIX OF LOSS SCENARIOS	SOIM	MINIMISE LINKABILITY	POR
MATTERS CLASSIFIED AS SECRET BY A STATE	LR	MINIMISE REPLICATION	POR
MATURITY MODELS	SSL	MINIMIZE RISK	POR
MAXIMUM TOLERABLE DOWNTIME	SOIM	MINIMIZE TRUST	POR
MAXIMUM TOLERABLE OUTAGE - AND INCIDENT RESPONSE	SOIM	MINIMUM SECURITY BASELINE	SOIM RMG
MAXIMUM TOLERABLE OUTAGE - AS BASIS FOR RECOVERY SITE SELECTION	SOIM	MINIMUM SECURITY BASELINE (MSB)	SOIM RMG
MAXIMUM TOLERABLE OUTAGE - DEFINED	SOIM	MINIMUM SECURITY BASELINE (MSB) - DEVELOPMENT OF	SOIM RMG
MAXIMUM TOLERABLE OUTAGE - IN INFORMATION RISK MANAGEMENT	RMG	MINIMUM SECURITY BASELINE (MSB) - OBSERVATIONS	SOIM RMG
MBR (MASTER BOOT RECORD)	OSV	MINIMUM SECURITY BASELINE (MSB) - STANDARDS	SOIM
MD (MESSAGE DIGEST) 2 4 AND 5	C	MINIMUM SECURITY BASELINE (MSB) - USE OF	RMG
MD5 MESSAGE DIGEST ALGORITHM	C	MINIMUM SECURITY BASELINE - PROJECT PLANNING	SOIM RMG
MEAN TIME - BETWEEN FAILURES (MTBF)	SOIM	MIRAI MALWARE	NS
MEAN TIME - TO REPAIR (MTTR)	SOIM	MIRROR SITE	SOIM
MEASURED SERVICE	DSS	MIRRORING	SOIM
MEASUREMENT - OF COMPLIANCE	HF RMG	MISRA	SS
MEASUREMENT - OF INFORMATION SECURITY MANAGEMENT PERFORMANCE	SOIM	MISREPRESENTATION	AB
MEASUREMENT - OF INFORMATION SECURITY RISK AND LOSS	SOIM	MISSION ASSURANCE CATEGORY (MAC)	SSL
MEASUREMENT - OF MANAGEMENT FRAMEWORK AND RESOURCES	RMG	MISSION FOR INCIDENT MANAGEMENT	SOIM
MEASUREMENT - OF MONITORING AND COMMUNICATION	SOIM	MISSION STATEMENT	RMG
MEASUREMENT - OF ORGANIZATIONAL AWARENESS	HF	MISSION-CRITICALITY	SOIM RMG
MEASUREMENT - OF PERFORMANCE IN INCIDENT MANAGEMENT	SOIM	MISSION/BUSINESS PROCESS LEVEL (TIER 2) RISK MANAGEMENT FOR	RMG
MEASUREMENT - OF SECURITY COST-EFFECTIVENESS	RMG	MISUSE DETECTION	SOIM
MEASUREMENT - OF TECHNICAL SECURITY ARCHITECTURE	SOIM	MITIGATE AGAINST FAILURES AND INCIDENTS	CI
MEASURING HARDWARE SECURITY	HS	MITIGATING ATTACKS	CPS
MEDIA - ACCESS CONTROL (MAC)	AAA	MITIGATING EXPLOITATION	SS
MEDIA - REMOVABLE	OSV	MITIGATION	SOIM
MEDIA ACCESS CONTROL (MAC)	C	MITIGATION OF RISK	RMG
MEDIA ACCESS CONTROL ADDRESS (MAC ADDRESS)	NS	MITIGATIONS	AB MAT DSS
MEDIA INCIDENT RESPONSE AND	SOIM	MITM (MAN-IN-THE-MIDDLE ATTACK)	MAT
MEDIA RECONSTRUCTION (INSURANCE COVERAGE)	SOIM	MITM (MAN-IN-THE-MIDDLE ATTACKS - MODES - EAVESDROPPING	NS
MEDIA TRANSPORTATION (INSURANCE COVERAGE)	SOIM	MITM (MAN-IN-THE-MIDDLE ATTACKS - MODES - SNIFFING	NS
MEDIATION	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - MOTIVATIONS	AB
MEDICAL DEVICES	CPS	MITM (MAN-IN-THE-MIDDLE ATTACKS - MULTI-ATTACK WEB METHOD	MAT
MEET-IN-THE-MIDDLE	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - PASSIVE	MAT
MEET-IN-THE-MIDDLE ATTACK	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - REPLAY	NS
MELTDOWN	HS OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SCADA	CPS
MEMORANDA OF AGREEMENT - INITIATION OF	SOIM	MITM (MAN-IN-THE-MIDDLE ATTACKS - SIDE-CHANNEL	C
MEMORY - PROTECTION	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SMURF ATTACK	NS
MEMORY AND STORAGE	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SOCIAL ENGINEERING	AB
MEMORY CORRUPTION (HARDWARE)	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING	NS
MEMORY ERRORS (SOFTWARE)	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - DNS	NS
MEMORY MANAGEMENT MITIGATIONS	SS	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - DNS QUERY MANIPULATION	NS
MEMORY MANAGEMENT VULNERABILITIES	SS	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - E-MAIL	WAM
MEMORY PROTECTION	HS	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - INFORMATION DISCLOSURE	AB
MEMORY PROTECTION AND ADDRESS SPACES	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - IP ADDRESS SPOOFING	NS
MEMORY PROTECTION UNIT	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - SESSION HIJACKING	MAT
MEMORY TAGGING EXTENSIONS	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - SPOOFING - SYN SCANNING	NS
MEMORY-BASED ROOTKITS	MAT	MITM (MAN-IN-THE-MIDDLE ATTACKS - STATISTICAL ATTACK	AB
MEMORY-RESIDENT MALWARE	MAT	MITM (MAN-IN-THE-MIDDLE ATTACKS - SURFACE	MAT
MENTAL MODELS OF CYBER RISKS AND DEFENCES	HF	MITM (MAN-IN-THE-MIDDLE ATTACKS - SYN FLOODING	NS
MERKEL-DAMGÅRD CONSTRUCTION	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - TABNABBING ATTACK METHOD	WAM MAT
MERKLE HASH TREES	OSV	MITM (MAN-IN-THE-MIDDLE ATTACKS - TELECOMMUNICATIONS	PLT
MESH TOPOLOGY	NS	MITM (MAN-IN-THE-MIDDLE ATTACKS - TOC/TOU (TIME-OF-CHECK/TIME-OF-USE)	SS
MESSAGE - AUTHENTICATION CODE (MAC)	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - VIRTUAL ENVIRONMENTS	OSV
MESSAGE - CONFIDENTIAL	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - VLANS	NS
MESSAGE - CONFIDENTIAL - PROOF OF ORIGIN	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - WEB JACKING ATTACK METHOD	WAM MAT
MESSAGE - DIGESTS	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - WEB-BASED	WAM
MESSAGE - INTEGRITY CONTROLS (MICS)	C	MITM (MAN-IN-THE-MIDDLE ATTACKS - WORMHOLES	NS
MESSAGE - OPEN	C	MIX NETWORKS	POR
MESSAGE - ORIENTED TEXT INTERCHANGE STANDARD (MOTIS)	NS	MIXED TRANSACTIONS	DSS
MESSAGE AUTHENTICATION CODE	AAA	MIXED-MODE THINKING	HF
MESSAGE AUTHENTICATION CODES	C	MOBILE	SSL
MESSAGE AUTHENTICATION-BASED PROTOCOLS	C	MOBILE PHONE DATA ACQUISITION	F
MESSAGE DIGEST	C WAM	MOBILE - APPLICATIONS	WAM
MESSAGE MODIFICATION	C	MOBILE - CODE - CONTROLS	WAM
MESSAGE PASSING	DSS	MOBILE - DEVICES	WAM
METADADA FILTERING	WAM	MOBILE APP SECURITY CHECKLIST	SSL
METADATA	F LR	MOBILE APPLICATION ARCHITECTURE	SSL

NETWORK MANAGEMENT	RMG	NIST - GUIDANCE ON COMPLEX SYSTEMS	RMG
NETWORK MAPPING PENETRATION TESTING - FINGERPRINTING	SS	NIST - GUIDANCE ON DYNAMIC SUBSYSTEMS	RMG
NETWORK MAPPING PENETRATION TESTING - FIREWALKING	NS	NIST - GUIDANCE ON EXTERNAL SUBSYSTEMS	RMG
NETWORK MAPPING PENETRATION TESTING - ICMP ECHO REQUESTS	NS	NIST - GUIDANCE ON IMPLEMENTATION OF SECURITY CONTROLS	SOIM
NETWORK MAPPING PENETRATION TESTING - IMAP	WAM	NIST - GUIDANCE ON SECURITY CONTROL ALLOCATION	RMG
NETWORK MAPPING PENETRATION TESTING - LANSPY	NS	NIST - GUIDANCE ON SECURITY CONTROLS SELECTION	RMG
NETWORK MAPPING PENETRATION TESTING - NMAP	NS	NIST - GUIDANCE ON SOFTWARE APPLICATION BOUNDARIES	SSL
NETWORK MAPPING PENETRATION TESTING - PING	NS	NIST - GUIDANCE ON SYSTEM CATEGORIZATION - LIFE-CYCLE PHASES	RMG
NETWORK MAPPING PENETRATION TESTING - SOLARWINDS	NS	NIST - IMPACT OF TECHNOLOGICAL CHANGES ON SYSTEM BOUNDARIES	SSL
NETWORK MAPPING PENETRATION TESTING - SUPERSCAN	NS	NIST - INFORMATION SYSTEM DEFINITION	RMG
NETWORK MAPPING PENETRATION TESTING - TCP CONNECT SCAN	NS	NIST - INFORMATION SYSTEM DEFINITION - PURPOSE AND APPLICABILITY	RMG
NETWORK MAPPING PENETRATION TESTING - TCP FIN SCAN	NS	NIST - NIST SP 800-137	RMG
NETWORK MAPPING PENETRATION TESTING - TCP SYN SCAN	NS	NIST - OVERVIEW	RMG
NETWORK MAPPING PENETRATION TESTING - TCP XMAS SCAN	NS	NIST - RESPONSES TO RISK ASSESSMENT	RMG
NETWORK MAPPING PENETRATION TESTING - TELNET	NS	NIST - RISK MANAGEMENT GUIDANCE	RMG
NETWORK MAPPING PENETRATION TESTING - TRACEROUTE	NS	NIST - SUMMARY OF GUIDANCE	RMG
NETWORK MAPPING PENETRATION TESTING - UDP SCANS	NS	NIST - SYSTEM AUTHORIZATION ROLES AND RESPONSIBILITIES	RMG
NETWORK MAPPING PENETRATION TESTING - WHOIS	NS	NIST GUIDANCE ON - SECURITY CONTROLS	RMG
NETWORK MONITORING	MAT	NIST GUIDANCE ON - STATUS REPORTING AND DOCUMENTATION	RMG
NETWORK PERIMETER PROTECTION	NS	NIST GUIDANCE ON ASSESSING EFFECTIVENESS OF	SOIM
NETWORK PROTOCOLS	CPS	NIST GUIDANCE ON IMPLEMENTATION OF	SOIM
NETWORK PROTOCOLS AND VULNERABILITY	NS	NIST GUIDANCE ON IMPLEMENTATION OF - SP 800-37 REVISION 1 GUIDANCE ON ALLOCATION OF	RMG
NETWORK SECURITY	NS	NIST GUIDANCE ON SECURITY STATE OF - SECURITY CONTROL SELECTION	RMG
NETWORK SERVICE PROVIDER (NSP)	NS	NIST GUIDELINES	RMG
NETWORK SERVICES	NS	NIST PRINCIPLES	CI
NETWORK STANDARDS AND PROTOCOLS	NS	NIST RISK ASSESSMENT METHODOLOGY	RMG
NETWORK TRAFFIC	SOIM	NIST RISK ASSESSMENT METHODOLOGY - AS OPERATIONAL ACTIVITIES	SOIM
NETWORK VIRTUALIZATION	OSV	NIST RISK ASSESSMENT METHODOLOGY - IN RISK MANAGEMENT PROCESS	RMG
NETWORK-BASED	MAT	NIST RISK ASSESSMENT METHODOLOGY - PROBABILISTIC RISK ASSESSMENT (PRA)	RMG
NETWORK-BASED INTRUSION DETECTION (NID)	SOIM NS	NIST RISK ASSESSMENT METHODOLOGY - RESIDUAL RISK IN	RMG
NETWORKED-CONTROLLED SYSTEMS	CPS	NIST RISK ASSESSMENT METHODOLOGY - RISK ANALYSIS IN	RMG
NETWORKS	NS	NIST RISK ASSESSMENT METHODOLOGY - RISK IDENTIFICATION IN	RMG
NETWORKS - ACCESS CONTROL AND	OSV	NIST RISK ASSESSMENT METHODOLOGY - RISK OWNERSHIP AND ACCOUNTABILITY	RMG
NETWORKS - BASTION HOSTS	NS	NIST RISK ASSESSMENT METHODOLOGY - RISK RANKING	RMG
NETWORKS - CABLING	PLT	NIST RISK ASSESSMENT METHODOLOGY - SECURITY BASELINES IN	RMG
NETWORKS - CELLULAR COMMUNICATIONS	PLT	NIST RISK ASSESSMENT METHODOLOGY - THREATS IN	RMG
NETWORKS - CIFS (COMMON INTERNET FILE SYSTEM)	OSV	NIST RISK ASSESSMENT METHODOLOGY - TASK EVALUATION	RMG
NETWORKS - CIRCUIT-SWITCHED	NS	NIST RISK ASSESSMENT METHODOLOGY - TASK LIKELIHOOD AND IMPACT IN	RMG
NETWORKS - CLASSES	NS	NIST RISK ASSESSMENT METHODOLOGY - TASK REGISTER	RMG
NETWORKS - CSMA (CARRIER SENSE MULTIPLE ACCESS)	PLT	NIST RISK ASSESSMENT METHODOLOGY - TASK TREATMENT OPTIONS	RMG
NETWORKS - DMZ (DEMILITARIZED ZONE)	NS	NIST RISK ASSESSMENT METHODOLOGY - VULNERABILITIES IN	RMG
NETWORKS - DNS (DOMAIN NAME SYSTEMS)	NS	NIST SP 800-30	RMG
NETWORKS - ENDPOINT SECURITY	NS	NIST SP 800-30 DEFINITION OF - PROJECT PLANNING	RMG
NETWORKS - ETHERNET AND	NS	NIST SP 800-37 GUIDANCE ON SELECTION OF	RMG
NETWORKS - EXTRANET	NS	NIST SP 800-37 GUIDANCE ON SELECTION OF - RECOMMENDATIONS	RMG
NETWORKS - FDDI (FIBER DISTRIBUTED DATA INTERFACE)	NS	NIST SP 800-37 GUIDANCE ON SELECTION OF - SELECTION OF	SOIM
NETWORKS - HARDWARE	NS	NIST SP 800-37 GUIDANCE ON SELECTION OF - STYLE OF	SOIM
NETWORKS - IDPS	NS	NIST SP 800-37 GUIDANCE ON SELECTION OF - USE OF	RMG
NETWORKS - INTRANETS	NS	NIST SP 800-37 REVISION 1 GUIDANCE ON	RMG
NETWORKS - IPV6	NS	NIST SP 800-37 REVISION 1 GUIDANCE ON - SYSTEM INVENTORY PROCESS	RMG
NETWORKS - LANS (LOCAL AREA NETWORKS)	NS	NIST SP 800-37 Ri	SOIM RMG
NETWORKS - NETBIOS	OSV	NIST SP 800-53	SSL CPS RMG
NETWORKS - NFS (NETWORK FILE SYSTEM)	NS	NIST SP 800-53 - CERTIFICATION TESTING	SOIM
NETWORKS - PROTOCOLS - DHCP	NS	NIST SP 800-53 - SECURITY CONTROLS	POR
NETWORKS - PROTOCOLS - ESMTP	NS	NIST SP 800-53A - CONTINUOUS MONITORING OF SYSTEM CONTROLS	SOIM
NETWORKS - PROTOCOLS - FTP	NS	NIST SP 800-53A - CONTINUOUS MONITORING OF SYSTEM CONTROLS - MISSION CRITICAL SYSTEM	LR
NETWORKS - PROTOCOLS - HTTP	NS	NIST SP 800-53A - USE OF TO DEVELOP CERTIFICATION TEST PROCEDURES	SOIM
NETWORKS - PROTOCOLS - ICMP	NS	NIST-IR 762	CPS
NETWORKS - PROTOCOLS - IP	NS	NODE	NS
NETWORKS - PROTOCOLS - LDAP	AAA	NOISE	HF
NETWORKS - PROTOCOLS - MPLS	NS	NOISE AND PERTURBATION	AB
NETWORKS - PROTOCOLS - MULTI-LAYER	NS	NON-BLIND SPOOFING	NS
NETWORKS - PROTOCOLS - OPEN	NS	NON-COHERENT AND MODIFIED MESSAGE CONTENTS	PLT
NETWORKS - PROTOCOLS - PROTOCOLS	NS	NON-COHERENT BUT UNMODIFIED MESSAGE CONTENTS	PLT
NETWORKS - PROTOCOLS - SMTP	NS	NON-EXECUTABLE MEMORY	SS
NETWORKS - PROTOCOLS - TCP	NS	NON-INJECTIVE AGREEMENT	AAA
NETWORKS - PROTOCOLS - TFTP	NS	NON-REPUDIATION	C
NETWORKS - PROTOCOLS - UDP	NS	NONCOMPLIANCE	SOIM
NETWORKS - PVCS (PERMANENT VIRTUAL CIRCUITS)	NS	NONCOMPLIANCE ISSUES	SOIM
NETWORKS - ROUTING	NS	NONINTRUSIVE MONITORING	SOIM
NETWORKS - RPCS (REMOTE PROCEDURE CALLS)	NS	NONREPUDIATION	C
NETWORKS - SDN (SOFTWARE-DEFINED NETWORKS)	NS	NONREPUDIATION - ENCRYPTION	C
NETWORKS - SMB (SERVER MESSAGE BLOCK)	OSV	NONREPUDIATION	C
NETWORKS - SNFS (SECURE NFS)	OSV	NOTIFICATION PROCESS FOR INCIDENTS	SOIM
NETWORKS - SVCS (SWITCHED VIRTUAL CIRCUITS)	NS	NSTISSC	RMG
NETWORKS - TOKEN PASSING	NS	NTFS SPECIAL PERMISSIONS	OSV
NETWORKS - TOKEN RING	NS	NTP	NS
NETWORKS - TOPOGRAPHIES	NS	NULL SCANNING	NS
NETWORKS - TRACEROUTE EXPLOITATION	MAT	NUMBER AS RECOVERY TEST METRIC	F
NETWORKS - TRANSMISSIONS	NS	NVD (NATIONAL VULNERABILITY DATABASE)	SOIM
NETWORKS - VIRTUAL NETWORK TERMINAL SERVICES	NS		
NEW APPROACHES	HF		
NEW PROTOCOLS	SOIM		
NEWER PRINCIPLES	OSV		
NEXT GENERATION SECURE COMPUTING BASE (NGSCB)	OSV		
NEXUS COMPUTING AGENT (NCA)	OSV		
NFC	PLT		
NFS (NETWORK FILE SYSTEM)	NS		
NFS (NETWORK FILE SYSTEM) - SNFS (SECURE NFS)	OSV		
NIACAP	RMG		
NIACAP - LIFE-CYCLE PHASES	LR		
NIACAP - NATIONAL SECURITY INFORMATION	SOIM		
NIDS (NETWORK-BASED IDS)	NS		
NIS	RMG		
NIS DIRECTIVE	LR		
NIS/NIS+ (NETWORK INFORMATION SERVICE)	NS		
NIST	F		
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)	SSL		
NIST - DEFINITION OF RISK	RMG		
NIST - GUIDANCE ON APPLYING RMF	RMG		
NIST - GUIDANCE ON ASSESSMENT OF SECURITY CONTROL EFFECTIVENESS	SOIM		

O

OAUTH WAM
 OAUTH 2 AAA
 OBFUSCATION MAT
 OBFUSCATION-BASED INFERENCE CONTROL POR
 OBJECT AAA
 OBJECT - SIGNING C
 OBJECT CODE OSV
 OBJECT STORAGE ENCRYPTION C
 OBJECT-CAPABILITY SYSTEMS SS
 OBJECT-ORIENTED (OO) - SECURITY SS
 OBJECTIVES HS
 OBJECTIVES OF CYBER SECURITY CI
 OBJECTS - ABAC AAA
 OBJECTS - ACCESS CONTROLS AAA
 OBJECTS - BELL-LAPADULA MODEL AAA
 OBLIGATIONS OWED TO A CLIENT LR
 OBLIVIOUS TRANSFER C POR
 OCSP (ONLINE CERTIFICATE STATUS PROTOCOL) C
 OCTAVE RMG
 OCTAVE (OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION) RMG
 OCTAVE - IN RISK ASSESSMENT RMG
 OCTAVE - QUALITATIVE ANALYSIS RMG
 OCTAVE - QUANTITATIVE ANALYSIS RMG
 OCTAVE - SEMIQUANTITATIVE ANALYSIS RMG
 OCTAVE - VALUE AT RISK RMG
 OCTAVE ALLEGRO RMG
 OCTAVEÁ® RMG
 OFB C
 OFF-SITE STORAGE FOR BACKUPS SOIM
 OFFLINE CONCOLIC EXECUTION MAT
 OFFSITE FACILITY SOIM
 OFFSITE STORAGE SOIM
 OFFSITE STORAGE TEAM SOIM
 OLDER CITIZENS HF
 ON-DEMAND COMPUTING (ODC) DSS
 ON-DEMAND SELF-SERVICE DSS
 ONCE IN-UNLIMITED ACCESS AAA
 ONE-TIME PAD C
 ONE-TIME PADS C
 ONE-TIME PASSWORDS HF
 ONE-WAY C
 ONE-WAY HASH C
 ONE-WAY TRUST AAA
 ONLINE - CERTIFICATE STATUS PROTOCOL (OCSP) AAA
 ONLINE - TRANSACTION PROCESSING (OLTP) SS
 ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) AAA
 ONLINE CONCOLIC EXECUTION MAT
 ONLINE CONTRACTS LR
 ONLINE GAMING SYSTEMS DSS
 ONLY THE FIRST STEP HF
 OPEN - MAIL RELAY - SERVERS NS
 OPEN - PROXY SERVERS WAM
 OPEN - SHORTEST PATH FIRST (OSPF) NS
 OPEN - SYSTEM - AUTHENTICATION NS
 OPEN - SYSTEM INTERCONNECT (OSI) NS
 OPEN - SYSTEMS INTERCONNECTION (OSI) MODEL NS
 OPEN - WEB APPLICATION SECURITY PROJECT (OWASP) SS
 OPEN DESIGN CI
 OPEN SHORTEST PATH FIRST (OSPF) NS
 OPEN SOURCE SECURITY TESTING METHODOLOGY RMG
 OPEN SYSTEMS INTERCONNECTION (OSD) NS
 OPENBR FACE RECOGNITION POR
 OPERATING SYSTEM ANALYSIS F
 OPERATING SYSTEM HARDENING OSV
 OPERATING SYSTEMS OSV
 OPERATING SYSTEMS - GUEST OSV
 OPERATIONAL - BINDINGS MANAGEMENT PROTOCOL (DOP) DIRECTORY AAA
 OPERATIONAL - PLANNING SOIM
 OPERATIONAL ACTIVITIES SOIM
 OPERATIONAL ACTIVITIES - AUDITS SOIM
 OPERATIONAL ACTIVITIES - CLOUD COMPUTING DSS
 OPERATIONAL ACTIVITIES - COMPLIANCE MONITORING AND ENFORCEMENT SOIM
 OPERATIONAL ACTIVITIES - DUE DILIGENCE IN SOIM
 OPERATIONAL ACTIVITIES - INCIDENT RESPONSE SOIM
 OPERATIONAL ACTIVITIES - SECURITY REVIEWS RMG
 OPERATIONAL ACTIVITIES - SECURITY TECHNOLOGY MANAGEMENT SOIM
 OPERATIONAL ACTIVITIES - TASK AND IMPACT ASSESSMENT SOIM
 OPERATIONAL ATTRIBUTES DSS
 OPERATIONAL COMPONENTS FOR INFORMATION SECURITY FRAMEWORK SOIM
 OPERATIONAL CONTROLS SSL
 OPERATIONAL METRICS SOIM
 OPERATIONAL RISK CATEGORIES SOIM
 OPERATIONAL RISK MANAGEMENT RMG
 OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION RMG
 OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION (OCTAVE) RMG
 OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION (OCTAVEÁ®) RMG
 OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION - IN SECURITY PROGRAM MANAGEMENT RMG
 OPERATIONALLY CRITICAL THREAT ASSET AND VULNERABILITY EVALUATION - RISK RMG
 OPERATIONS ABAC AAA
 OPERATIONS MANAGER SOIM
 OPERATIONS/MAINTENANCE PHASE SOIM
 OPTICAL SCANNER HS

OPTICAL-FAULT ATTACKS HS
 ORANGE BOOK SOIM
 ORDERS TO IN-STATE PERSONS DIRECTING PRODUCTION OF DATA UNDER THEIR CONTROL WHETHER HELD ON DOMESTIC OR FOREIGN IT SYSTEMS LR
 ORGANIZATION DESIGN AND STRATEGY RMG
 ORGANIZATION LEVEL (TIER 1) RISK MANAGEMENT FOR RMG
 ORGANIZATIONAL - ANALYSIS SOIM
 ORGANIZATIONAL - SECURITY EFFORTS SOIM
 ORGANIZATIONAL AWARENESS HF
 ORGANIZATIONAL STRUCTURE - IN INCIDENT MANAGEMENT SOIM
 ORGANIZATIONAL SUPPORT - IN RISK MANAGEMENT RMG
 ORIGIN-BASED POLICIES AAA
 ORTHOGONAL BLINDING PLT
 OS AVAILABILITY OSV
 OS SECURITY PRINCIPLES OSV
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - APPLICATION LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - DATA LINK LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - LAYERS NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - NETWORK LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - PHYSICAL LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - PRESENTATION LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - SESSION LAYER NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - TCP/IP MODEL NS
 OSI (OPEN SYSTEM INTERCONNECT) MODEL - TRANSPORT LAYER NS
 OSINT (OPEN SOURCE INTELLIGENCE) QUERIES AB
 OSPF (OPEN SHORTEST PATH FIRST) NS
 OSPF (OPEN SHORTEST POST FIRST) NS
 OT RMG
 OT NETWORKS CPS
 OTHER MODELS AB
 OTHER REGULATORY MATTERS LR
 OTP (ONE-TIME PASSWORD) AAA
 OTR POR
 OUT-OF-BAND DETECTION CPS
 OUT-OF-BAND VERIFICATION AAA
 OUT-OF-BAND VERIFICATION - VULNERABILITIES AND SS
 OUT-SPECIFICATION PLT
 OUTCOMES - OF INCIDENT MANAGEMENT SOIM
 OUTCOMES - OF INFORMATION SECURITY GOVERNANCE RMG
 OUTCOMES - OF RISK MANAGEMENT RMG
 OUTCOMES - OF SECURITY PROGRAM MANAGEMENT SOIM
 OUTDATED THIRD PARTY LIBRARIES WAM
 OUTGOING ECLIPSE ATTACKS DSS
 OUTPUT SECURE F
 OUTSOURCED DATABASES OSV
 OUTSOURCED IRT SOIM
 OUTSOURCING POR
 OVE/UNDER VOLTAGE CPS
 OVERCURRENT PROTECTION CPS
 OVERSIGHT RMG
 OVERSIGHT - PERSONALLY IDENTIFIABLE INFORMATION (PII) POR
 OVERSIGHT COMMITTEE RMG
 OVERWRITING DATA SOIM
 OWASP (OPEN WEB APPLICATION SECURITY PROJECT) SSL
 OWASP ASVS SSL
 OWASP MOBILE APPLICATION SECURITY VERIFICATION STANDARD SSL
 OWNERSHIP SS RMG
 OWNERSHIP (AUTHENTICATION) - PASSWORDS DYNAMIC AAA
 OWNERSHIP (AUTHENTICATION) - RFID HS
 OWNERSHIP (AUTHENTICATION) - SMART CARDS HS
 OWNERSHIP (AUTHENTICATION) - TOKENS AAA

P

P2P DSS
 P2P (PEER-TO-PEER) APPLICATIONS NS
 P2P DATA STRUCTURES DSS
 P2P NETWORKS ATTACKS MAT
 P2P OPERATIONS DSS
 P2P TAKEDOWN MAT
 P3P POR
 PAAS F DSS
 PAAS (PLATFORM AS A SERVICE) DSS
 PACKET NS
 PACKET FILTERING NS
 PACKET FILTERS NS
 PACKET LOSS NS
 PACKET SIZE SOIM
 PACKET SNIFFER NS
 PACKET SNIFFING NS
 PACKET SWITCHED NETWORK NS
 PACKET SWITCHING NS
 PACKET-SWITCHED NS
 PACKET-SWITCHED NETWORKS NS
 PACKING MAT
 PAGE COLOURING OSV
 PAGING OSV
 PAP (PASSWORD AUTHENTICATION PROTOCOL) NS
 PAPER TEST SOIM
 PAPERWORK SOIM RMG
 PARALLEL - DATA SYSTEMS DSS
 PARALLEL - TEST SOIM
 PARALLEL CHANGEOVER SOIM
 PARALLEL TEST SOIM
 PARALLEL TESTING SOIM

PARAMETER VALIDATION	SS	GOVERNANCE	RMG
PARKING LOT ATTACK	AB	PERFORMANCE MEASUREMENT - IN INCIDENT MANAGEMENT	SOIM
PARTIAL REPLICATION	F	PERFORMANCE METRICS	SOIM
PARTIALLY ORDERED	CI	PERFORMANCE TESTING	SSL
PARTIALLY SYNCHRONOUS	DSS	PERFORMANCE WEB-BASED ATTACKS AND	SOIM F
PARTITION	DSS	PERFORM STATIC ANALYSIS SECURITY TESTING	SSL
PARTITIONING	OSV	PERIMETER-BASED WEB PORTAL ACCES	AAA
PARTITIONING MICRO-ARCHITECTURAL STATES	OSV	PERIODIC AUTHENTICATION	AAA
PARTITIONS	F	PERIPHERAL DEVICE RECOGNITION	AAA
PASSIVE ATTACK	C MAT	PERIPHERALS	HS
PASSIVE ATTACKS	AB	PERMANENT VIRTUAL CIRCUITS (PVCS)	NS
PASSIVE SIDE CHANNEL ATTACKS	HS	PERMANENCE	PLT
PASSWORD	C	PERMISSION DIALOG BASED ACCESS CONTROL	WAM
PASSWORD - AUTHENTICATION PROTOCOL (PAP)	AAA	PERMISSIONS	AAA
PASSWORD - PROTECTION TECHNIQUES	AAA	PERSISTENT OR TRANSIENT	MAT
PASSWORD LEAKS	WAM	PERSISTENT-MODE ROOTKITS	MAT
PASSWORD MANAGERS	WAM	PERSONAL DATA	POR
PASSWORD POLICIES	WAM	PERSONAL DATA BREACH NOTIFICATION	LR
PASSWORD STRENGTH METERS	WAM	PERSONAL FIREWALL	WAM
PASSWORDS	AAA HF	PERSONALLY IDENTIFIABLE INFORMATION (PI1)	POR
PASSWORDS - ASYNCHRONOUS	AAA	PERSONALLY IDENTIFIABLE INFORMATION (PII)	POR
PASSWORDS - COGNITIVE PASSWORDS	C	PERSONNEL - IN INCIDENT MANAGEMENT	SOIM
PASSWORDS - DYNAMIC	AAA	PERSONNEL - PHARMING	AB OSV
PASSWORDS - DYNAMIC - SYNCHRONOUS	AAA	PERSONNEL - PHISHING	AB
PASSWORDS - STATIC	AAA	PERTURBATION	POR
PASSWORDS AND ALTERNATIVES	WAM	PESTUDIO	MAT
PASSWORK CRACKER	MAT	PGP (PRETTY GOOD PRIVACY) CRYPTOSYSTEM	C
PAST DECISIONS ABOUT A SYSTEM	CI	PHARMING	AB
PAT (PORT ADDRESS TRANSLATION)	NS	PHASED CHANGEOVER	SOIM
PATCH MANAGEMENT	SOIM	PHISHING	WAM AB
PATCH PANELS	NS	PHISHING - BOTNETS	MAT
PATCHING CAN INTRODUCE VULNERABILITIES	SSL	PHISHING - DISTRIBUTION	AB
PATENT	LR	PHISHING - E-MAIL	WAM AB
PATENTS	LR	PHISHING - FACIAL RECOGNITION	AAA
PATH EXPLORATION	MAT	PHISHING - FINGERPRINT VERIFICATION	AAA
PATH SANITISATION	WAM	PHISHING - GEOMETRY RECOGNITION	AAA
PATHS OF LOGICAL ACCESS	AAA	PHISHING - HAND GEOMETRY	AAA
PATTERN THEORY OF CRIME	AB	PHISHING - IRIS SCAN	AAA
PATTERNS FOR ENTITY AUTHENTICATION	AAA	PHISHING - RETINAL SCAN	AAA
PAX TEAM	OSV	PHISHING - VASCULAR PATTERNS	AAA
PAXOS	DSS	PHISHING - VISHING	PLT
PAY-PER-INSTALL SERVICES	AB	PHREAKERS	PLT
PAYLOAD MALCODE	MAT	PHYSICAL ACCESS AND SECURE DELETION	OSV
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)	WAM	PHYSICAL ATTACKS	WAM
PAYMENT METHODS	AB	PHYSICAL CHARACTERISTICS	HF
PAYPAL	AB	PHYSICAL DATA ACQUISITION	F
PBX (PRIVATE BRANCH EXCHANGE)	PLT	PHYSICAL DOMAIN	HS
PCAP	SOIM	PHYSICAL FAULT-INJECTION	SS
PCI DSS	SSL	PHYSICAL LAYER	PLT
PCRS	OSV	PHYSICAL LAYER (OSI)	NS
PDCA (PLAN-DO-CHECK-ACT)	SOIM	PHYSICAL LAYER ATTACKS ON SECURE DISTANCE MEASUREMENT	PLT
PEER RESOURCES AT THE NETWORK'S EDGE	DSS	PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATION TECHNOLOGIES	PLT
PEER-TO-PEER APPLICATIONS	DSS	PHYSICAL MEDIA	F
PENETRATION TEST METHODOLOGY	SOIM	PHYSICAL MODELS	HF
PENETRATION TESTING	SOIM SSL	PHYSICAL PARTITIONS	HS
PENETRATION TESTING - ACTIVE PENETRATION	SOIM	PHYSICAL SPACE ACCESS CONTROL AND	OSV
PENETRATION TESTING - BLACK BOX	SOIM	PHYSICAL-LAW ANOMALIES	CPS
PENETRATION TESTING - DNS ZONE TRANSFER	NS	PHYSICALLY UNCLONABLE FUNCTIONS (PUFS)	HS
PENETRATION TESTING - DNS ZONE TRANSFER - LOW-TECH	NS	PHYSICS-BASED ATTACK DETECTION	CPS
PENETRATION TESTING - DNS ZONE TRANSFER - MID-TECH	NS	PICASA FACE RECOGNITION AND	POR
PENETRATION TESTING - DNS ZONE TRANSFER - SOCIAL ENGINEERING	AB	PII (PERSONALLY IDENTIFIABLE INFORMATION)	POR
PENETRATION TESTING - GREY BOX	SOIM	PING	NS
PENETRATION TESTING - HIGH-LEVEL STEPS	SOIM	PING - SCANNING	NS
PENETRATION TESTING - INFORMATION EVALUATION	SOIM	PING OF DEATH	NS MAT
PENETRATION TESTING - INHERITANCE	SOIM	PKCS	C
PENETRATION TESTING - NETWORK MAPPING	SOIM	PKI	C
PENETRATION TESTING - NETWORK MAPPING - FINGERPRINTING	SS	PKI (PUBLIC KEY INFRASTRUCTURE)	C
PENETRATION TESTING - NETWORK MAPPING - FIREWALKING	NS	PLAIN OLD TELEPHONE SERVICE (POTS)	PLT
PENETRATION TESTING - NETWORK MAPPING - ICMP ECHO REQUESTS	NS	PLAINTEXT	C
PENETRATION TESTING - NETWORK MAPPING - IMAP	WAM	PLAINTEXT - ATTACKS	C
PENETRATION TESTING - NETWORK MAPPING - LANSPIY	NS	PLAINTEXT - CHOSEN	C
PENETRATION TESTING - NETWORK MAPPING - NMAP	NS	PLAINTEXT - KNOWN	C
PENETRATION TESTING - NETWORK MAPPING - PING	NS	PLAINTEXT - XOR	C
PENETRATION TESTING - NETWORK MAPPING - RECONNAISSANCE	SOIM	PLAN AND PREPARE	RMG
PENETRATION TESTING - NETWORK MAPPING - SOLARWINDS	NS	PLAN-DO-CHECK-ACT (PDCA)	SOIM RMG
PENETRATION TESTING - NETWORK MAPPING - SUPERSCAN	NS	PLAN: SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
PENETRATION TESTING - NETWORK MAPPING - TCP CONNECT SCAN	NS	PLANNING ESTIMATES	SOIM RMG
PENETRATION TESTING - NETWORK MAPPING - TCP FIN SCAN	NS	PLANNING IN RISK MANAGEMENT FRAMEWORK	RMG
PENETRATION TESTING - NETWORK MAPPING - TCP SYN SCAN	NS	PLANNING THE IMPLEMENTATION AND DEPLOYMENT OF SECURE DEVELOPMENT	SSL
PENETRATION TESTING - NETWORK MAPPING - TCP XMAS SCAN	NS	PLATFORM AS A SERVICE (PAAS)	DSS
PENETRATION TESTING - NETWORK MAPPING - TELNET	NS	PLC (PROGRAMMABLE LOGIC CONTROLLER)	CPS
PENETRATION TESTING - NETWORK MAPPING - TRACEROUTE	NS	PLCS	CPS
PENETRATION TESTING - NETWORK MAPPING - UDP SCANS	NS	PM (PRIVACY MODULE)	OSV
PENETRATION TESTING - NETWORK MAPPING - WHOIS	NS	PMB (PICTURE MOTION BROWSER) - RECOGNITION AND	POR
PENETRATION TESTING - REPORTING	SOIM	POC (PROOF OF CONCEPT)	MAT
PENETRATION TESTING - RESULTS ANALYSIS	SOIM	POINT-OF-SALE (POS)	AB
PENETRATION TESTING - RISK ANALYSIS	RMG	POINT-TO-POINT - TUNNELING PROTOCOL (PPTP)	NS
PENETRATION TESTING - SETTINGS	SOIM	POINT-TO-POINT PROTOCOL (PPP)	NS
PENETRATION TESTING - SOFTWARE TOOLS	SOIM	POINTER AUTHENTICATION	HS OSV
PENETRATION TESTING - SPECIAL	SOIM	POINTS	AAA
PENETRATION TESTING - STANDARD	SOIM	POLICIES	RMG
PENETRATION TESTING - WHITE BOX	SOIM	POLICIES - COMPLIANCE WITH	SOIM
PENETRATION TESTING - WINDOWS	SOIM	POLICIES - FOR INCIDENT MANAGEMENT	SOIM
PEOPLE ARE NOT THE WEAKEST LINK	HF	POLICIES - IN RISK MANAGEMENT FRAMEWORK	RMG
PERCENTAGE AS RECOVERY TEST METRIC	F	POLICIES DOCUMENTATION OF	RMG
PERFORM DYNAMIC ANALYSIS SECURITY TESTING	SSL	POLICY ADMINISTRATION POINTS	AAA
PERFORM PENETRATION TESTING	SSL	POLICY AND POLITICAL ASPECTS	CPS
PERFORM THREAT MODELLING	SSL	POLICY DECISION POINTS	AAA
PERFORMANCE INDICATORS	RMG	POLICY DEVELOPMENT FOR ACTION PLAN	RMG
PERFORMANCE MANAGEMENT	SOIM	POLICY ENFORCEMENT POINTS	AAA
PERFORMANCE MEASUREMENT - AS RESULT OF INFORMATION SECURITY		POLICY INFORMATION POINTS	AAA

POLLING	NS	PROBABILISTIC SIGNATURE SCHEMES	C
POLLUTION	HF	PROBABLE DISRUPTIONS	SOIM
POLLUTION ATTACKS	DSS	PROBLEM ESCALATION	SOIM
POLYINSTANTIATION	AAA SS	PROBLEM FORECASTING	SOIM
POLYMORPHIC VIRUSES	MAT	PROCEDURES	SOIM RMG
POLYMORPHISM	MAT	PROCEDURES - ACCESS TO	SOIM
POP (POST OFFICE PROTOCOL)	WAM	PROCEDURES - CERTIFICATION TESTING	SOIM
POP-UPS	WAM	PROCEDURES - DEVELOPMENT PROCESS	SOIM
POROUS DEFENSES	SS	PROCEDURES - ESTABLISHING AS POSTINCIDENT ACTIVITY	F
PORT ADDRESS TRANSLATION (PAT)	NS	PROCEDURES - FOR INCIDENT MANAGEMENT	SOIM
PORT SCANNING	NS	PROCEDURES - FOR INCIDENT RESPONSE	SOIM
PORTS	NS	PROCEDURES - STYLE OF	SOIM
POSITION SENSITIVITY DESIGNATIONS	SOIM	PROCESS INFORMATION	F
POSITIVE SECURITY	HF	PROCESSES - AH (AUTHENTICATION HEADER)	NS
POST-QUANTUM CRYPTOGRAPHY	C	PROCESSES - APPLICATION-LEVEL	NS
POSTINCIDENT ACTIVITIES	SOIM	PROCESSES - BGP (BORDER GATEWAY PROTOCOL)	NS
POTENTIALLY UNWANTED PROGRAMS	MAT	PROCESSES - CIRCUIT-LEVEL	NS
POTS (PLAIN OLD TELEPHONE SERVICE)	PLT	PROCESSES - DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)	NS
POWER CONSUMPTION	HS	PROCESSES - ESMT (ENHANCED SIMPLE MAIL TRANSFER PROTOCOL)	NS
PPTP (POINT-TO-POINT TUNNELING PROTOCOL)	NS	PROCESSES - ESP (ENCAPSULATING SECURITY PAYLOAD)	NS
PRA (PROBABILISTIC RISK ASSESSMENT)	RMG	PROCESSES - FCP (FIBER CHANNEL PROTOCOL)	NS
PRANKS	MAT	PROCESSES - FTP (FILE TRANSFER PROTOCOL)	NS
PRE-/POST-CONDITIONS	SS	PROCESSES - H.245 (CALL CONTROL PROTOCOL FOR MULTIMEDIA COMMUNICATION)	NS
PRECAUTIONARY PRINCIPLE	CI	PROCESSES - HAIP (HIGH ASSURANCE INTERNET PROTOCOL ENCRYPTOR)	NS
PREPARATION IN INCIDENT MANAGEMENT PROCESSES	SOIM	PROCESSES - HTTP (HYPERTEXT TRANSFER PROTOCOL)	NS
PREPARATION IN INCIDENT RESPONSE PLAN	SOIM	PROCESSES - ICMP (INTERNET CONTROL MESSAGE PROTOCOL)	NS
PREPARE	RMG	PROCESSES - IKE (INTERNET KEY EXCHANGE)	C
PREPARE: INCIDENT MANAGEMENT PLANNING	SOIM	PROCESSES - IN BUSINESS MODEL FOR INFORMATION SECURITY	RMG
PREPARED STATEMENTS	WAM	PROCESSES - IP (INTERNET PROTOCOL)	NS
PREPAREDNESS TEST	SOIM	PROCESSES - IPSEC AND	NS
PRESCRIPTIVE JURISDICTION	LR	PROCESSES - ISAKMP (INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL)	WAM
PRESCRIPTIVE JURISDICTION AND DATA PROTECTION	LR	PROCESSES - ISNS (INTERNET STORAGE NAME SERVICE)	NS
PRESCRIPTIVE JURISDICTION OVER COMPUTER CRIME	LR	PROCESSES - ISOLATION	OSV
PRESCRIPTIVE JURISDICTION OVER ONLINE CONTENT	LR	PROCESSES - KIMP (KEY MANAGEMENT INTEROPERABILITY PROTOCOL)	C
PRESCRIPTIVE PROCESSES	SSL	PROCESSES - L2TP (LAYER 2 TUNNELING PROTOCOL)	NS
PRESENCE OF VULNERABILITIES	CI	PROCESSES - LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)	AAA
PRESENTATION LAYER (OSI)	NS	PROCESSES - LINK-STATE ROUTING	NS
PRESENTATION OF RISK ASSESSMENT INFORMATION	RMG	PROCESSES - MPLS (MULTIPROTOCOL LABEL SWITCHING)	NS
PRESERVING THE EVIDENCE	AAA	PROCESSES - MULTI-LAYER	NS
PRETTY GOOD PRIVACY (PGP) CRYPTOSYSTEM	C	PROCESSES - MULTI-LAYER - FIELDBUS PROTOCOL	CPS
PREVENTING ATTACKS	CPS	PROCESSES - MULTI-LAYER - MODBUS PROTOCOL	CPS
PREVENTING TRANSDUCTION ATTACKS	CPS	PROCESSES - MULTI-LAYER - SCADA	CPS
PREVENTION OF VULNERABILITIES	SS	PROCESSES - PAP (PASSWORD AUTHENTICATION PROTOCOL)	NS
PREVENTIVE CONTROL	SOIM	PROCESSES - PPTP (POINT-TO-POINT TUNNELING PROTOCOL)	NS
PRIMARY KEYS	C	PROCESSES - PROTOCOLS	NS
PRIMITIVES FOR ISOLATION AND MEDIATION	OSV	PROCESSES - RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)	AAA
PRINCIPAL	AAA	PROCESSES - RDP (RELIABLE DATAGRAM PROTOCOL)	NS
PRINCIPLE OF COMPLETE MEDIATION	OSV CI	PROCESSES - REDIRECT ATTACKS	NS
PRINCIPLE OF ECONOMY OF MECHANISM	OSV CI	PROCESSES - RPC (REMOTE PROCEDURE CALL)	NS
PRINCIPLE OF FAIL-SAFE DEFAULTS	OSV CI	PROCESSES - RTCP (REAL-TIME TRANSPORT CONTROL PROTOCOL)	NS
PRINCIPLE OF INTENTIONAL USE	OSV CI	PROCESSES - S/MIME (SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS)	WAM
PRINCIPLE OF LEAST AUTHORITY	OSV CI	PROCESSES - SA (SECURITY ASSOCIATIONS)	NS
PRINCIPLE OF LEAST COMMON MECHANISM	OSV CI	PROCESSES - SCTP (STREAM CONTROL TRANSMISSION PROTOCOL)	NS
PRINCIPLE OF LEAST PRIVILEGE	SS CI	PROCESSES - SMPP (SHORT MESSAGE PEER-TO-PEER)	NS
PRINCIPLE OF MINIMIZING THE TRUSTED COMPUTING BASE	OSV CI	PROCESSES - SMTP (SIMPLE MAIL TRANSFER PROTOCOL)	NS
PRINCIPLE OF OPEN DESIGN	OSV CI	PROCESSES - SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)	NS
PRINCIPLE OF PSYCHOLOGICAL ACCEPTABILITY	OSV CI	PROCESSES - SPX (SEQUENCED PACKET EXCHANGE)	NS
PRINCIPLE OF SEPARATION OF PRIVILEGE	OSV CI	PROCESSES - SSL/TLS (SECURE SOCKET LAYER/TRANSPORT LAYER SECURITY)	NS
PRINCIPLES	DSS	PROCESSES - SST (STRUCTURED STREAM TRANSPORT)	NS
PRINCIPLES	CI	PROCESSES - STP (SPANNING TREE PROTOCOL)	NS
PRIORITY-BASED FLOW CONTROL (PFC)	NS	PROCESSES - TCP (TRANSMISSION CONTROL PROTOCOL)	NS
PRISM	FMS	PROCESSES - TFTP (TRIVIAL FILE TRANSFER PROTOCOL)	NS
PRIVACY	POR	PROCESSES - TRANSPORT MODE	NS
PRIVACY - PROTECTION	POR	PROCESSES - TUNNEL MODE	NS
PRIVACY - REQUIREMENTS COMPLIANCE	LR	PROCESSES - UDP (USER DATAGRAM PROTOCOL)	NS
PRIVACY AND ACCOUNTABILITY	AAA	PROCESSES - VOIP (VOICE OVER INTERNET PROTOCOL)	WAM
PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS	AB	PROCESSING	LR
PRIVACY BY DESIGN	AAA	PROCESSOR	HS
PRIVACY CONCERNS OF DRONES	CPS	PROCESSORS	HS
PRIVACY DATA	POR	PROCNETMONITOR	OSV
PRIVACY ENGINEERING	POR	PRODUCTION AND ENABLING TASKS	HF
PRIVACY EVALUATION	POR	PROFESSIONAL LIABILITY (INSURANCE COVERAGE)	SOIM
PRIVACY IMPACT ASSESSMENT (PIA)	POR	PROFILE MANAGEMENT	AAA
PRIVACY INFORMATION OMB DEFINITION OF	POR	PROFINET	CPS
PRIVACY INVASIONS	CPS	PROFINET IRT	SOIM
PRIVACY LAWS IN GENERAL AND ELECTRONIC INTERCEPTION	LR	PROGRAM - PROGRAMMABLE LOGIC CONTROLLER (PLC)	CPS
PRIVACY MIRRORS	POR	PROGRAM ACTIVITIES MANAGING	SOIM
PRIVACY NUDGES	POR	PROGRAM AND PROJECT MANAGEMENT	SSL
PRIVACY POLICY INTERPRETABILITY	POR	PROGRAM AWARENESS	HF
PRIVACY POLICY NEGOTIATION	POR	PROGRAM CHANGES	SSL
PRIVACY SETTINGS CONFIGURATION	POR	PROGRAM CORRECTNESS	FMS
PRIVACY TECHNOLOGIES AND DEMOCRATIC VALUES	POR	PROGRAM DRIVERS EXTERNAL	LR
PRIVACY TECHNOLOGIES AS SUPPORT FO DEMOCRATIC POLITICAL SYSTEMS	POR	PROGRAM EVALUATION REVIEW TECHNIQUE (PERT)	SSL
PRIVATE	DSS	PROGRAM INTEGRATION	RMG
PRIVATE - BRANCH EXCHANGE (PBX)	PLT	PROGRAM INTEGRATION - RAM MANAGER - MANAGING PROGRAM ACTIVITIES	SOIM
PRIVATE AUTHENTICATION	POR	PROGRAM INTEGRATION - RAM MANAGER - RESPONDING TO CHANGES	RMG
PRIVATE BRANCH EXCHANGE	PLT	PROGRAM LOGIC	SS
PRIVATE BRANCH EXCHANGE (PBX)	PLT	PROGRAM MANAGEMENT INCONSISTENCY IN	SOIM RMG
PRIVATE COMPUTATION - INPUT VERIFICATION	POR	PROGRAM OVERSIGHT	RMG
PRIVATE INFORMATION RETRIEVAL	POR	PROGRAM SCOPE	SOIM
PRIVATE KEY	C	PROGRAM VERIFICATION	SS
PRIVATE PAYMENTS	POR	PROGRAMMING - LANGUAGE(S) - SECURITY ISSUES	SS
PRIVATE SUBDOMAINS	AAA	PROGRAMMING - LANGUAGE(S) - SUPPORT	SS
PRIVILEGE ATTRIBUTES	OSV	PROGRAMMING IDIOMS	SS
PRIVILEGE MANAGEMENT	OSV	PROGRAMMING LANGUAGES	SS
PRIVILEGED ACCOUNTS	OSV	PROGRAMMING SKILLS	SS
PRIVILEGED ACCOUNTS - ADMINISTRATOR ACCOUNTS	OSV	PROJECT - INITIATIVES	RMG
PRIVILEGED ACCOUNTS - POWER USERS	OSV	PROJECT - PLANNING	SOIM
PRIVILEGED ACCOUNTS - ROOT OR BUILT-IN ADMINISTRATOR ACCOUNTS	OSV	PROJECT AGREEMENT OUTLINE	RMG
PRIVILEGED ACCOUNTS - SERVICE ACCOUNTS	OSV		
PROBABILISTIC RISK ASSESSMENT (PRA)	RMG		

R

PROJECT MANAGEMENT RMG
 PROJECT MANAGEMENT OFFICE RMG
 PROJECT MANAGEMENT STRUCTURE RMG
 PROJECT MANAGEMENT TECHNIQUES RMG
 PROJECT MANAGER RMG
 PROJECT MANAGER ADMINISTRATIVE REQUIREMENTS RMG
 PROJECT MANAGER ADMINISTRATIVE REQUIREMENTS - DEALING WITH PEOPLE RMG
 PROJECT MANAGER ADMINISTRATIVE REQUIREMENTS - DEALING WITH PEOPLE - RESPONSIBILITIES OF RMG
 PROJECT PLANNING RMG
 PROJECT PLANNING - ADMINISTRATIVE REQUIREMENTS RMG
 PROJECT PLANNING - ASSUMPTIONS RMG
 PROJECT PLANNING - DEALING WITH PEOPLE RMG
 PROJECT PLANNING - RISKS RMG
 PROJECT RISK SSL
 PROJECTIVE TECHNIQUES HF
 PROOF OF IDENTITY SOIM
 PROOF OF WORK DSS
 PROOFING AAA
 PROOFING DSS
 PROPERTIES PLT
 PROPERTY OF ELECTRONIC VOTING SYSTEMS POR
 PROTECT (INCIDENT MANAGEMENT PROCESSES) SOIM
 PROTECTED MODULE ARCHITECTURES HS
 PROTECTING DATA DURING PROCESSING POR
 PROTECTING DATA IN TRANSIT POR
 PROTECTING DATA INTEGRITY PLT
 PROTECTION CPS
 PROTECTION OF DATA CI
 PROTECTION OF GENERATORS CPS
 PROTECTION OF INFORMATION SYSTEMS CI
 PROTECTION OF SERVICE CI
 PROTECTION PROFILE OSV
 PROTECTION RINGS OSV
 PROTECTIONS AGAINST NATURAL EVENTS AND ACCIDENTS CPS
 PROTOCOL SOIM
 PROTOCOL AUGMENTATION PLT
 PROTOCOL CONVERTERS NS
 PROTOCOL FORMAT WAM
 PROVERIF FMS
 PROVIDE TRAINING SSL
 PROXIES - APPLICATION-LEVEL PROXY WAM
 PROXIES - CIRCUIT-LEVEL PROXY WAM
 PROXIMITY RMG
 PROXY SERVER POR
 PSEUDO RANDOM NUMBER GENERATION (PRNG) HS
 PSEUDO-RANDOM FUNCTIONS C
 PSEUDO-RANDOM PERMUTATIONS C
 PSTTN (PUBLIC SWITCHED TELEPHONE NETWORKS) PLT
 PUBLIC DSS
 PUBLIC - KEY C
 PUBLIC - KEY CRYPTOGRAPHY C
 PUBLIC - KEY ENCRYPTION C
 PUBLIC - KEY INFRASTRUCTURE (PKI) C
 PUBLIC DATA POR
 PUBLIC DATA NETWORKS (PDNS) NS
 PUBLIC DATA SENSITIVITY POR
 PUBLIC INTERNATIONAL LAW LR
 PUBLIC KEY C
 PUBLIC KEY ALGORITHMS HS
 PUBLIC KEY CRYPTOGRAPHY C
 PUBLIC KEY CRYPTOSYSTEM C
 PUBLIC KEY ENCRYPTION C
 PUBLIC KEY INFRASTRUCTURE NS
 PUBLIC KEY INFRASTRUCTURE (PK) C
 PUBLIC KEY SIGNATURES C
 PUBLIC MULTISCANNERS MALWARE NAMING MAT
 PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES C
 PUBLIC-SWITCHED TELEPHONE NETWORK (PSTN) PLT
 PURGING SOIM
 PURPOSE-BASED ACCESS CONTROL POR
 PVCS (PERMANENT VIRTUAL CIRCUITS) NS

RA (REGISTRATION AUTHORITY) C
 RACE (RESEARCH AND DEVELOPMENT IN ADVANCED COMMUNICATIONS TECHNOLOGIES IN EUROPE) C
 RACE CONDITION MITIGATIONS SS
 RACE CONDITION VULNERABILITIES SS
 RACE CONDITIONS SS
 RACI CHART RMG
 RADIO FREQUENCY IDENTIFICATION (RFID) PLT
 RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) AAA
 RAID DATA RECOVERY F
 RAIL FENCE C
 RAINBOW TABLES C
 RANDOM NUMBER GENERATION HS
 RANDOM NUMBER GENERATOR C
 RANDOM ORACLE MODEL C
 RANDOM-ACCESS MEMORY (RAM) OSV
 RANDOMISATION HS
 RANGE CHECK SS
 RANKING CRITICALITY SOIM
 RANKING DATA SENSITIVITY RMG
 RANSOMWARE SOIM
 RANSOMWARE DETECTION AB
 RAPID APPLICATION DEVELOPMENT MAT
 RAPID APPLICATION DEVELOPMENT (RAD) SSL
 RATIONAL CHOICE THEORY SSL
 RATS (REMOTE ACCESS TROJANS) AB
 RC (ROLE COMPATIBILITY MODULE) MAT
 RC4 OSV
 RC5 C
 RC6 C
 RDN (RELATIVE DISTINGUISHED NAME) AAA
 RDP (RELIABLE DATAGRAM PROTOCOL) NS
 RE-EVALUATE F
 REACTIVATION SOIM
 REACTIVE PLT
 REACTIVE CONTROL COMPENSATION CPS
 READ AND EXTRACT F
 READ ATTRIBUTES PERMISSION OSV
 READ EXTENDED ATTRIBUTES PERMISSION OSV
 READ ONLY MEMORY (ROM) HS
 READ PERMISSIONS PERMISSION OSV
 READER COLLISION (RFID) HS
 REAL USER MONITORING (RUM) WAM
 REAL USER MONITORING (RUM) - DATABASE MONITORING WAM
 REAL USER MONITORING (RUM) - TCP PORT MONITORING WAM
 REAL USER MONITORING (RUM) - WEBSITE MONITORING WAM
 REAL-TIME ASSESSMENT - ONS FOR PROGRAM FAILURE SOIM
 REAL-TIME SYSTEMS CPS
 REAL-TIME TRANSPORT CONTROL PROTOCOL (RTCP) NS
 REAL-TIME TRANSPORT PROTOCOL (RTP) NS
 REALISTIC GOALS RMG
 REASONABLE ASSURANCE AAA
 RECERTIFICATION TRACKING SOIM
 RECIPROCAL AGREEMENT RMG
 RECOMMENDATIONS AAA
 RECONNAISSANCE AB
 RECOVERY MAT
 RECOVERY (INCIDENT RESPONSE PLAN) RMG
 RECOVERY - PHASE SOIM
 RECOVERY - POINT OBJECTIVE (RPO) SOIM
 RECOVERY - SITE STRATEGIES SOIM
 RECOVERY - SYSTEMS SOIM
 RECOVERY - TIME OBJECTIVE (RTO) SOIM
 RECOVERY ACTION SOIM
 RECOVERY ALTERNATIVES SOIM
 RECOVERY CONTROLS SSL
 RECOVERY INCIDENT RESPONSE SOIM
 RECOVERY INCIDENT RESPONSE AND - BACKUPS SOIM
 RECOVERY INCIDENT RESPONSE AND - CONTINUITY AND SOIM
 RECOVERY INCIDENT RESPONSE AND - DISASTER RECOVERY SOIM
 RECOVERY INCIDENT RESPONSE AND - PLAN TESTING SOIM
 RECOVERY OPERATIONS SOIM
 RECOVERY PLAN SOIM
 RECOVERY PLANNING SOIM
 RECOVERY PLANS UPDATING SOIM
 RECOVERY POINT OBJECTIVE (RPO) SOIM
 RECOVERY POINT OBJECTIVE - AND INCIDENT RESPONSE SOIM
 RECOVERY POINT OBJECTIVE - AS BASIS FOR RECOVERY SITE SELECTION SOIM
 RECOVERY POINT OBJECTIVE - DEFINED SOIM
 RECOVERY POINT OBJECTIVE - IN INCIDENT RESPONSE PLAN SOIM
 RECOVERY POINT OBJECTIVE - IN RISK MANAGEMENT RMG
 RECOVERY SITES SOIM
 RECOVERY STRATEGIES SOIM
 RECOVERY TIME OBJECTIVE (RTO) SOIM
 RECOVERY TIME OBJECTIVE - AND INCIDENT RESPONSE SOIM
 RECOVERY TIME OBJECTIVE - AS BASIS FOR RECOVERY SITE SELECTION SOIM
 RECOVERY TIME OBJECTIVE - DEFINED SOIM
 RECOVERY TIME OBJECTIVE - IN INCIDENT RESPONSE PLAN SOIM
 RECOVERY TIME OBJECTIVE - IN OPERATIONAL RISK MANAGEMENT SOIM
 RECTANGULAR SUBSTITUTION TABLES C
 RECURSION DNS NS
 RECURSIVE RESOLVER DNS NS
 RED HAT OSV
 RED PILL TECHNIQUES MAT
 REDUNDANCY SOIM
 REDUNDANCY IN NETWORK SERVICES HS
 REDUNDANT SITE SOIM

Q

QARMA HS
 QUALITATIVE RISK ANALYSIS RMG
 QUALITATIVE RISK ASSESSMENT RMG
 QUALITY ASSURANCE (QA) SSL
 QUALITY ASSURANCE TESTING SSL
 QUALITY ASSURANCE TESTING (QAT) SSL
 QUALITY OF SERVICE (QoS) NS
 QUANTISATION PLT
 QUANTITATIVE RISK ANALYSIS RMG
 QUANTITATIVE RISK ASSESSMENT RMG
 QUANTITATIVE VS QUALITATIVE APPROACHES RMG
 QUANTIZED CONGESTION NOTIFICATION (QCN) NS
 QUANTUM CRYPTOGRAPHY C
 QUANTUM RESISTANT ALGORITHMS HS
 QUBESOS OSV
 QUERIES DYNAMIC SS
 QUERY GENERATION SS
 QUERYING ENCRYPTED DATABASES OSV
 QUIC NS

REFERENCE MONITOR	AAA WAM OSV	RESOURCE MANAGEMENT	SOIM
REFINEMENT-BASED ANALYSIS	FMS	RESOURCE MANAGEMENT AND COORDINATION SERVICES	DSS
REFLECTED XSS ATTACKS	WAM	RESOURCE POOLING	DSS
REFORMATTING DATA	SOIM	RESOURCE PROTECTION	OSV
REFRACTION NETWORKING	POR	RESOURCES - CONTROLS AS STRATEGY IMPLEMENTATION	SOIM
REGISTER TRANSFER LEVEL (RTL)	HS	RESOURCES - DETERMINATION OF LEVEL OF	RMG
REGISTER TRANSFERS	HS	RESOURCES - FOR INCIDENT MANAGEMENT	SOIM
REGISTRATION AUTHORITY (RA)	C	RESOURCES - IN RISK MANAGEMENT FRAMEWORK	RMG
REGRESSION TESTING	SSL	RESOURCES - IN SECURITY PROGRAM MANAGEMENT	SOIM
REGULATED DATA SENSITIVITY	LR	RESOURCES - TRACKING	RMG
REGULATION	CPS	RESPONSE	RMG
REGULATION COMPLIANCE AUDITS	LR	RESPONSE (INCIDENT MANAGEMENT PROCESSES)	SOIM
REGULATIONS	LR	RESPONSE AND RECOVERY PLAN	SOIM
REGULATORY COMPLIANCE	RMG	RESPONSE STRATEGIES	SOIM
REGULATORY CONSTRAINTS FOR INFORMATION SECURITY STRATEGY	LR	RESPONSIBILITIES - IN EFFECTIVE INFORMATION RISK MANAGEMENT	RMG
REGULATORY CONTROL	CPS	RESPONSIBILITIES - IN INCIDENT MANAGEMENT	SOIM
RELATED AREAS	OSV	RESPONSIBILITIES - IN INFORMATION SECURITY	RMG
RELATIONAL	OSV	RESPONSIBILITIES - IN INFORMATION SECURITY GOVERNANCE	RMG
RELATIONSHIP BUILDING	RMG	RESPONSIBILITIES - IN RISK MANAGEMENT FOR INFORMATION SECURITY GOVERNANCE	RMG
RELATIONSHIPS - BUSINESS	RMG	RESPONSIBILITY	SOIM
RELEASE MANAGEMENT	SSL	RESPONSIBILITY LACK OF	SOIM RMG
RELEVENCE	F	RESTORATION	SOIM
RELIABILITY	CPS	RESTRICTED DATA	POR
RELIABLE AND SECURE GROUP COMMUNICATION	DSS	RESTRICTED INTERFACE	SS
RELIABLE TRANSFER SERVICE ELEMENT (RTSE)	NS	RESTRICTIONS ON EXPORTING SECURITY TECHNOLOGIES	LR
RELIANCE	SOIM	RESTRICTIVE DEVELOPMENT FRAMEWORKS	WAM
REMIEDIATION PLANNING	SOIM	RETENTION	SOIM
REMIEDIATION PLANS - APPLICABILITY OF	SOIM	RETENTION IN SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
REMIEDIATION PLANS - CONTENT OF	SOIM	RETINAL SCAN	AAA
REMIEDIATION PLANS - FORMAT OF	SOIM	RETURN ON INVESTMENT (ROD)	RMG
REMIEDIATION PLANS - RESPONSIBILITY FOR	SOIM	RETURN ON INVESTMENT (ROI)	RMG
REMIEDIATION PLANS - SCOPE OF	SOIM	RETURN ON SECURITY INVESTMENT (ROSI)	RMG
REMIEDIATION PLANS - TIMING OF CREATION OF	SOIM	REVERSE AUTHENTICATION	AAA
REMIEDIATION PLANS - TIMING OF CREATION OF - USE OF	SOIM	REVERSE ENGINEERING	MAT LR
REMIEDIATION PLANS - UPDATING OF	SOIM	REVISION ACQUISITION	F
REMOTE - AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)	AAA	RFID - ANTI-COLLISION PROTOCOL	HS
REMOTE - COMPUTING RISKS	SOIM	RIDL	OSV
REMOTE - DATABASE ACCESS (RDA)	NS	RIJNDAEL	C
REMOTE - JOURNALING	SOIM	RIJNDAEL ALGORITHM	C
REMOTE - MEETING TECHNOLOGY	WAM	RIJNDAEL ALGORITHM - ADD ROUND KEY	C
REMOTE - OPERATION SERVICE ELEMENT (ROSE)	NS	RIJNDAEL ALGORITHM - MIX COLUMN TRANSFORMATION	C
REMOTE - PROCEDURE CALLS (RPCS)	DSS	RIJNDAEL ALGORITHM - SHIFT ROW TRANSFORMATION	C
REMOTE - TERMINAL UNIT (RTU)	CPS	RIJNDAEL ALGORITHM - SUBSTITUTE BYTES	C
REMOTE ACCESS	AAA	RING-1	OSV
REMOTE ACCESS - TELECOMMUTING	NS	RING-2	OSV
REMOTE ACCESS - TELNET	NS	RING-3 / INTEL ME	OSV
REMOTE ACCESS - TUNNELING - L2TP	NS	RING 0	OSV
REMOTE ACCESS - TUNNELING - PPTP	NS	RING SIGNATURES	C
REMOTE ACCESS - TUNNELING - RADIUS	AAA	RING TOPOLOGY	NS
REMOTE ACCESS - TUNNELING - SNMP	NS	RINGS	OSV
REMOTE ACCESS - VIRTUAL NETWORK TERMINAL SERVICES	NS	RIP (ROUTING INFORMATION PROTOCOL)	NS
REMOTE ACCESS - VPN (VIRTUAL PRIVATE NETWORK)	NS	RIPEND-160	C
REMOTE ATTESTATION	CPS	RISK	RMG
REMOTE JOURNALING	SOIM	RISK - ACCEPTANCE	SOIM
REMOTE PROCEDURE CALLS (RPC)	SOIM	RISK - ASSESSMENTS	RMG
REMOTE-ACCESS - SERVICES	OSV	RISK - ASSESSMENTS - METHODOLOGIES	RMG
REMOTE-ACCESS - TROJANS (RA.TS)	MAT	RISK - ASSESSMENTS - TOOLS AND TECHNIQUES	RMG
REPEAT VICTIMS	AB	RISK - ASSIGNMENT	SOIM
REPEATERS	NS	RISK - AVOIDANCE	SOIM
REPLAY ATTACK	C	RISK - CATEGORIZATION	RMG
REPLICATION	SOIM	RISK - CURRENT	RMG
REPLICATION AND COORDINATION	DSS	RISK - DEFINED	RMG
REPLICATION MANAGEMENT AND COORDINATION SCHEMA	DSS	RISK - ELEMENTS OF	RMG
REPORT	RMG	RISK - IN RISK MANAGEMENT	RMG
REPORTING	AAA	RISK - INHERENT	RMG
REPORTING - ADMINISTRATIVE SERVICES DEPARTMENT	RMG	RISK - IT-RELATED	RMG
REPORTING - CEO	RMG	RISK - LIKELIHOOD IMPACT AND	RMG
REPORTING - CORPORATE SECURITY	RMG	RISK - MANAGEMENT - COMPONENTS	RMG
REPORTING - IN INFORMATION RISK MANAGEMENT PROGRAM	RMG	RISK - MANAGEMENT - COMPONENTS - COMMUNICATION	RMG
REPORTING - IN RISK MONITORING	RMG	RISK - MANAGEMENT - COMPONENTS - CONTROL ACTIVITIES	RMG
REPORTING - INFORMATION TECHNOLOGY (IT) DEPARTMENT	RMG	RISK - MANAGEMENT - COMPONENTS - EVENT IDENTIFICATION	RMG
REPORTING - INSURANCE	RMG	RISK - MANAGEMENT - COMPONENTS - INTERNAL ENVIRONMENT	RMG
REPORTING - INTERNAL AUDIT DEPARTMENT	RMG	RISK - MANAGEMENT - COMPONENTS - MONITORING	RMG
REPORTING - LEGAL DEPARTMENT	RMG	RISK - MANAGEMENT - COMPONENTS - OBJECTIVE SETTING	RMG
REPORTING - MODEL	RMG	RISK - MANAGEMENT - COMPONENTS - RISK ASSESSMENT	RMG
REPORTING - OF VULNERABILITIES	SOIM	RISK - MANAGEMENT - COMPONENTS - RISK RESPONSE	RMG
REPORTING - PENETRATION TESTING	SOIM	RISK - MANAGEMENT - CONCEPTS	RMG
REPORTING - RISK MANAGEMENT DEPARTMENT	RMG	RISK - MEASURING	RMG
REPORTING CHANNELS	SOIM	RISK - MITIGATION	SOIM
REPOSITORY	SSL	RISK - RESIDUAL	RMG
REPRESENTATIONAL STATE TRANSFER (REST)	WAM	RISK - TRANSFER	SOIM
REPUTATION SCORING	MAT	RISK ACCEPTANCE	RMG
REQUIREMENTS - FUNCTIONAL	SSL	RISK ACCEPTANCE - AND INCIDENT RESPONSE	SOIM
REQUIREMENTS - NONFUNCTIONAL	SSL	RISK ACCEPTANCE - AS INFORMATION SECURITY STRATEGY CONSTRAINT	RMG
REQUIREMENTS DEFINITION	SSL	RISK ACCEPTANCE - AS RISK TREATMENT	RMG
REQUIREMENTS OF FORM AND THE THREAT OF UNENFORCEABILITY	LR	RISK ACCEPTANCE FRAMEWORK	RMG
RESEARCH AND DEVELOPMENT ACTIVITIES CONDUCTED BY NON-STATE PERSONS	LR	RISK ACTION PLAN	RMG
RESHIPPING MULES	AB	RISK ANALYSIS	RMG CI
RESIDUAL RISK	RMG	RISK ANALYSIS - PENETRATION TESTING	RMG
RESIDUAL RISK - DEFINED	SOIM	RISK ANALYSIS - QUALITATIVE	RMG
RESIDUAL RISK - IN RISK ASSESSMENT	RMG	RISK ANALYSIS - QUANTITATIVE	RMG
RESIDUAL RISK - IN RISK MANAGEMENT PROCESS	RMG	RISK ANALYSIS ANNUAL LOSS EXPECTANCY	RMG
RESILIENCE	DSS	RISK ANALYST RESPONSIBILITIES OF	RMG
RESILIENCE TO PERTURBATIONS	DSS	RISK APPETITE	RMG
RESILIENT CONTROL SYSTEMS	CPS	RISK APPETITE - DETERMINING	RMG
RESILIENT ESTIMATION	CPS	RISK APPETITE - IN RISK MANAGEMENT PROGRAM DEVELOPMENT	RMG
RESOLVERS	NS	RISK ASSESSMENT	RMG
RESOURCE ACQUISITION IS INITIALISATION	SS	RISK ASSESSMENT - AGEREGATED RISK	RMG
RESOURCE COORDINATION CLASS	DSS	RISK ASSESSMENT - APPROACHES TO	RMG
RESOURCE DEPENDENCY ANALYSIS	RMG	RISK ASSESSMENT - ASSET IDENTIFICATION IN	RMG
RESOURCE DEPLETION (DOS)	OSV		

RISK ASSESSMENT - ASSET VALUATION	RMG	RISK MONITORING	SOIM RMG
RISK ASSESSMENT - CASCADING RISK	RMG	RISK OBJECTIVES	RMG
RISK ASSESSMENT - CONDUCTING	RMG	RISK OWNERSHIP	RMG
RISK ASSESSMENT - CONDUCTING - OBSERVATIONS	RMG	RISK PERCEPTION FACTORS	RMG
RISK ASSESSMENT - CONTROLS IN	RMG	RISK PROFILE	RMG
RISK ASSESSMENT - COSTS AND BENEFITS OF	RMG	RISK RANKING	RMG
RISK ASSESSMENT - DEFINED	RMG	RISK REGISTER	RMG
RISK ASSESSMENT - DOCUMENTATION OF RESULTS	RMG	RISK REGISTER - ELEMENTS OF	RMG
RISK ASSESSMENT - FACTOR ANALYSIS OF INFORMATION RISK (FAIR)	RMG	RISK REGISTER - UPDATING	RMG
RISK ASSESSMENT - IMPACT IN	RMG	RISK RELATED TO BUSINESS PROCESSES	RMG
RISK ASSESSMENT - IN INFORMATION SECURITY STRATEGY	RMG	RISK RELATED TO DATA MANAGEMENT	RMG
RISK ASSESSMENT - PROCESS	RMG	RISK REMEDIATION PLAN - APPLICABILITY OF	SOIM
RISK ASSESSMENT - RISK REMEDIATION	SOIM RMG	RISK REMEDIATION PLAN - CONTENT OF - OBSERVATIONS	SOIM RMG
RISK ASSESSMENT - SAMPLE OUTLINE	RMG	RISK REMEDIATION PLAN - FORMAT OF	SOIM
RISK ASSESSMENT - SECURITY PLANS	SOIM RMG	RISK REMEDIATION PLAN - RESPONSIBILITY FOR	SOIM
RISK ASSESSMENT - SECURITY PROCEDURES	SOIM RMG	RISK REMEDIATION PLAN - SCOPE OF	SOIM
RISK ASSESSMENT - SUMMARY OF TASKS PER NIST 800-30 REVISION 1	RMG	RISK REMEDIATION PLAN - TIMING OF CREATION OF	SOIM
RISK ASSESSMENT - SYSTEM AUTHORIZATION AND	RMG	RISK REMEDIATION PLAN - USE OF	SOIM
RISK ASSESSMENT - SYSTEM INVENTORY	RMG	RISK REPORTING	RMG
RISK ASSESSMENT - USE OF	RMG	RISK RESPONSE	SOIM RMG
RISK ASSESSMENT AND MANAGEMENT IN CYBER-PHYSICAL SYSTEMS	RMG	RISK SCENARIO	RMG
RISK ASSESSMENT AND MANAGEMENT METHODS	RMG	RISK SCENARIO - ANALYZING	RMG
RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG	RISK SCENARIO - BENEFITS	RMG
RISK ASSESSMENT MODEL	RMG	RISK SCENARIO - DEVELOPMENT	RMG
RISK ASSESSMENT TECHNIQUES	RMG	RISK SCENARIO TECHNIQUE	RMG
RISK AVOIDANCE	RMG	RISK SHARING/RISK TRANSFER	RMG
RISK AWARENESS	HF RMG	RISK TOLERANCE	RMG
RISK AWARENESS PROGRAM	RMG	RISK TOLERANCE - AND INCIDENT RESPONSE	SOIM
RISK CAPACITY	RMG	RISK TOLERANCE - AS INFORMATION SECURITY STRATEGY CONSTRAINT	RMG
RISK COMMUNICATION	RMG	RISK TOLERANCE - DEFINED	RMG
RISK COMMUNICATION PLAN	RMG	RISK TOLERANCE - IN RISK MANAGEMENT PROGRAM DEVELOPMENT	RMG
RISK COMMUNICATION PRINCIPLES	RMG	RISK TRANSFER	RMG
RISK COMPONENTS	RMG	RISK TREATMENT (RESPONSE)	RMG
RISK CULTURE	HF	RISK-BASED AUDIT APPROACH	RMG
RISK DEFINITION	RMG	RISK-BASED AUTHENTICATION	AAA
RISK DETERMINATION	RMG	RISK-BASED CONTROLS	SSL
RISK EVALUATION	RMG	RISK-BASED SECURITY TESTING	SSL
RISK EVENT	RMG	RISKS MONITORING	SOIM
RISK EXECUTIVE RESPONSIBILITIES OF	RMG	RISKWATCH	RMG
RISK FACTORS	RMG	RME - ACCREDITATION	SOIM
RISK GOVERNANCE	RMG	RME - APPLICATION OF TO FEDERAL INFORMATION SYSTEMS	RMG
RISK GOVERNANCE OBJECTIVES	RMG	RME - APPLICATION OF TO FEDERAL INFORMATION SYSTEMS - SP 800-37 REVISION 1	RMG
RISK HANDLING	RMG	GUIDANCE ON APPLYING	RMG
RISK HIERARCHY	RMG	RME - OVERVIEW OF	RMG
RISK IDENTIFICATION	RMG	RME - RISK MITIGATION PLANNING	RMG
RISK LIMITATION	RMG	RME - SECURITY CONTROL MONITORING	SOIM
RISK MANAGEMENT	RMG	RME - SECURITY CONTROLS IMPLEMENTATION	SOIM
RISK MANAGEMENT - AS OUTCOME OF SECURITY PROGRAMS	SOIM	ROAD MAP - FOR SECURITY PROGRAMS	RMG
RISK MANAGEMENT - AS RESULT OF INFORMATION SECURITY GOVERNANCE	RMG	ROAD MAP - IN INFORMATION SECURITY STRATEGY DEVELOPMENT	RMG
RISK MANAGEMENT - ASSESSMENTS	RMG	ROAD MAP - PROVIDED BY ARCHITECTURE	SOIM
RISK MANAGEMENT - ASSET	RMG	ROAD VEHICLES	SSL
RISK MANAGEMENT - CONCEPTS FOR	RMG	ROBOTICS AND ADVANCED MANUFACTURING	CPS
RISK MANAGEMENT - DEFINITION OF	RMG	ROBUST CONTROL	CPS
RISK MANAGEMENT - DOCUMENTATION FOR	HF	ROBUSTNESS	SOIM PLT
RISK MANAGEMENT - EFFECTIVE	RMG	ROGUE PRODUCTS ATTACKS	AB
RISK MANAGEMENT - FUNDAMENTAL CONCEPTS OF	RMG	ROGUES CERTIFICATE AUTHORITIES AND CERTIFICATE TRANSPARENCY	WAM
RISK MANAGEMENT - GUIDANCE ON IN THE SYSTEM DEVELOPMENT LIFE CYCLE	RMG	ROI (RETURN ON INVESTMENT)	RMG
RISK MANAGEMENT - GUIDANCE ON IN THE SYSTEM DEVELOPMENT LIFE CYCLE - INFORMATION SYSTEM LEVEL (TIER 3)	SSL RMG	ROLE OF OPERATING SYSTEMS	OSV
RISK MANAGEMENT - GUIDANCE ON IN THE SYSTEM DEVELOPMENT LIFE CYCLE - MISSION/BUSINESS PROCESS LEVEL (TIER 2)	SSL RMG	ROLE-BASED ACCESS CONTROL (RBAC)	AAA
RISK MANAGEMENT - GUIDANCE ON IN THE SYSTEM DEVELOPMENT LIFE CYCLE - ORGANIZATION LEVEL (TIER 1)	RMG	ROLE-BASED ACCESS CONTROL (RBAC) - RBAC ARCHITECTURES	AAA
RISK MANAGEMENT - GUIDANCE ON IN THE SYSTEM DEVELOPMENT LIFE CYCLE - ORGANIZATION-WIDE	SSL RMG	ROLE-BASED ACCESS CONTROL (RBAC) - RBAC ARCHITECTURES - FULL RBAC	AAA
RISK MANAGEMENT - IMPACT	RMG	ROLE-BASED ACCESS CONTROL (RBAC) - RBAC ARCHITECTURES - HYBRID RBAC	AAA
RISK MANAGEMENT - IMPLEMENTATION OF	RMG	ROLE-BASED ACCESS CONTROL (RBAC) - RBAC ARCHITECTURES - LIMITED RBAC	AAA
RISK MANAGEMENT - IN GOVERNANCE RISK MANAGEMENT AND COMPLIANCE	RMG	ROLE-BASED ACCESS CONTROL (RBAC) - RBAC ARCHITECTURES - NON-RBAC	AAA
RISK MANAGEMENT - IN INCIDENT MANAGEMENT	SOIM	ROLE-BASED ACCESS CONTROLS - CBAC (CONTEXT-BASED ACCESS CONTROL)	AAA
RISK MANAGEMENT - IN INFORMATION SECURITY GOVERNANCE	RMG	ROLE-BASED ACCESS CONTROLS - CDAC (CONTENT-DEPENDENT ACCESS CONTROL)	AAA
RISK MANAGEMENT - IN INFORMATION SECURITY STRATEGY	RMG	ROLE-BASED ACCESS CONTROLS - TRBAC (TEMPORAL ROLE-BASED ACCESS CONTROL)	AAA
RISK MANAGEMENT - IN SECURITY PROGRAM MANAGEMENT	RMG	ROLES	RMG
RISK MANAGEMENT - INFORMATION ASSET CLASSIFICATION	RMG	ROLES - IN EFFECTIVE INFORMATION RISK MANAGEMENT	RMG
RISK MANAGEMENT - LIKELIHOOD	RMG	ROLES - IN INFORMATION SECURITY	RMG
RISK MANAGEMENT - OPERATIONAL	SOIM	ROLES - IN INFORMATION SECURITY GOVERNANCE	RMG
RISK MANAGEMENT - OVERVIEW OF	RMG	ROLES - IN RISK MANAGEMENT FOR INFORMATION SECURITY GOVERNANCE	RMG
RISK MANAGEMENT - PROCESS	RMG	ROLES AND RESPONSIBILITIES - DOCUMENTING	RMG
RISK MANAGEMENT - REPORTING	SOIM	ROLES AND RESPONSIBILITIES - POSITION SENSITIVITY DESIGNATIONS	SOIM
RISK MANAGEMENT - RISK ACCEPTANCE	RMG	ROLLBACK	SOIM
RISK MANAGEMENT - RISK ASSESSMENT AND ANALYSIS METHODOLOGIES	RMG	ROOT CAUSE ANALYSIS	SOIM
RISK MANAGEMENT - RISK AVOIDANCE	RMG	ROOT OF TRUST	HS
RISK MANAGEMENT - RISK DEFINITION	RMG	ROOT OF TRUST FOR MEASUREMENT	HS
RISK MANAGEMENT - RISK MITIGATION	SOIM	ROOT OF TRUST FOR REPORTING	HS
RISK MANAGEMENT - RISK MONITORING AND COMMUNICATION	RMG	ROOT OF TRUST FOR STORAGE	HS
RISK MANAGEMENT - RISK TRANSFERENCE	RMG	ROOTKIT	MAT
RISK MANAGEMENT - RISK VISIBILITY	SOIM	ROOTKITS	MAT
RISK MANAGEMENT - SECURITY CONTROL BASELINES	RMG	ROS] (RETURN ON SECURITY INVESTMENT)	RMG
RISK MANAGEMENT - SELF-ASSESSMENT	RMG	ROTATION	SOIM
RISK MANAGEMENT - STRATEGY FOR	RMG	ROTATION OF DUTIES	F
RISK MANAGEMENT - THREAT	RMG	ROUND KEY	C
RISK MANAGEMENT - THREAT SOURCE	RMG	ROUTER	NS
RISK MANAGEMENT - TASK ASSESSMENT	RMG	ROUTINE ACTIVITY THEORY	AB
RISK MANAGEMENT - TRAINING AND AWARENESS OF	HF	ROUTING	SOIM
RISK MANAGEMENT - VULNERABILITY	RMG	ROUTING - BOUNDARY ROUTERS	NS
RISK MANAGEMENT CAPABILITY	RMG	ROUTING - DETERMINISTIC	NS
RISK MANAGEMENT FRAMEWORK	RMG	ROUTING - SECURE	NS
RISK MANAGEMENT PROCESS	RMG	ROUTING ATTACKS	DSS
RISK MANAGEMENT PROGRAM	RMG	ROUTING INFORMATION PROTOCOL (RIP)	NS
RISK MATRIX EXAMPLE	RMG	ROUTING PROTOCOL SECURITY	NS
RISK MITIGATION	SOIM RMG	ROUTING TABLE POISONING	DSS
RISK MITIGATION MEETINGS	RMG	ROUTING TABLES	NS
		ROUTING TABLES	NS
		ROWHAMMER	SS HS
		RPC (REMOTE PROCEDURE CALL PROTOCOL)	NS

RPO (RECOVERY POINT OBJECTIVE)	SOIM
RR (RESOURCE RECORD)	NS
RSA	C
RSA-KEM	C
RSA-OAEP	C
RSBAC (RULE SET-BASED ACCESS CONTROLS)	AAA
RSN	NS
RSI-BASED DISTANCE ESTIMATION ATTACKS	PLT
RTCP (REAL-TIME TRANSPORT CONTROL PROTOCOL)	NS
RTOS (RECOVERY TIME OBJECTIVES)	SOIM
RTU (REMOTE TERMINAL UNIT)	CPS
RTUS	CPS
RULE COMBINING ALGORITHMS	AAA
RULE-BASED ACCESS	AAA
RUNNING KEY CIPHER	C
RUNTIME DETECTION	MAT
RUNTIME DETECTION OF ATTACKS	SS

S

S/MIME (SECURE MIME)	WAM
SA (SECURITY ASSOCIATIONS)	NS
SAAS	F
SAAS FORENSICS	F
SABOTAGE	AB
SABSA	RMG
SAFE CONTROL ACTIONS	CPS
SAFE LANGUAGES	SS
SAFECODE	SSL
SAFETY	CPS
SAFETY AND LIVE-ENVIRONMENT REQUIREMENTS	MAT
SAFETY PROBLEMS	CPS
SAFETY VS SECURITY	CPS
SAFETY-CRITICAL SYSTEMS DOMAIN	CI
SALAMI TECHNIQUE	AB
SALTING	C
SALTZER AND SCHROEDER'S PRINCIPLES	OSV CI
SALTZER SCHROEDER PRINCIPLES	SSL
SAME ORIGIN POLICY (SOP)	WAM
SAME-ORIGIN POLICIES	WAM
SAML	AAA
SAML (SECURITY ASSERTION MARKUP LANGUAGE)	AAA
SAMM	SSL
SAMPLING	SOIM
SAN (STORAGE AREA NETWORK)	C OSV
SANDBOX	OSV
SANDBOX - MALCODE COUNTERMEASURES	MAT
SANDBOXING	WAM SS
SATISFACTION	HF
SCADA	CPS RMG
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - ATTACKS	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - CONTROL SERVER	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - DATA HISTORIAN	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - HMI (HUMAN-MACHINE INTERFACE)	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - IED (INTELLIGENT ELECTRONIC DEVICES)	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - IO (INPUT/OUTPUT) SERVER	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - PLC (PROGRAMMABLE LOGIC CONTROLLER)	CPS
SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) - RTU (REMOTE TERMINAL UNIT)	CPS
SCALABILITY	DSS
SCANNERS	SOIM
SCANNERS - NESSUS	SOIM
SCANNERS - NMAP	SOIM
SCANNING	AB
SCANNING - COMPLIANCE	SOIM
SCANNING - DISCOVERY	SOIM
SCANNING - SYN	NS
SCANNING - TECHNIQUES	NS
SCANNING - TECHNIQUES - FIN SCANNING	NS
SCANNING - TECHNIQUES - NULL SCANNING	NS
SCANNING - TECHNIQUES - PORT SCANNING	NS
SCANNING - TECHNIQUES - XMAS SCANNING	NS
SCHEDULE LIMITATIONS	SOIM
SCHEMA	SOIM F OSV
SCHEMAS	SOIM
SCHEMATIZE	F
SCHEMES	C
SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
SCHNORR SIGNATURES	C
SCM (SOFTWARE CONFIGURATION MANAGEMENT)	SSL
SCOPE AND CHARTER - OF EFFECTIVE INFORMATION RISK MANAGEMENT PROGRAM	RMG
SCOPE AND CHARTER - OF EFFECTIVE INFORMATION SECURITY GOVERNANCE	RMG
SCOPE AND CHARTER - OF SECURITY PROGRAM(S)	SOIM
SCOPE CREEP	RMG
SCOPING	SSL
SCREEN SCRAPERS	WAM
SCREENED - HOST	NS
SCREENED - SUBNET ARCHITECTURE	NS
SCREENED HOSTS	NS
SCREENED SUBNET ARCHITECTURE	NS

SCREENING ROUTERS	NS
SCREENSAVERS	HF
SCRIPT INJECTION VULNERABILITIES (XSS)	SS
SCRIPT PROCESSING	WAM
SCRIPTING	SS
SCTP (STREAM CONTROL TRANSMISSION PROTOCOL)	NS
SCYTALE CIPHER	C
SDLC	SSL
SDLC (SYSTEM DEVELOPMENT LIFE CYCLE)	SSL
SDLC - ACQUISITION/DEVELOPMENT PHASE	SSL
SDLC - CHALLENGES TO IMPLEMENTATION	SSL
SDLC - CHALLENGES TO IMPLEMENTATION - GUIDANCE ON RISK MANAGEMENT IN	SSL
SDLC - DISPOSITION PHASE	SSL
SDLC - IMPLEMENTATION PHASE	SSL
SDLC - INITIATION PHASE	SSL
SDLC - OPERATIONS/MAINTENANCE PHASE	SSL
SDN (SOFTWARE-DEFINED NETWORKS)	NS
SDN - APPLICATION (SDN APP)	NS
SDN - CONTROL TO DATA-PLANE INTERFACE (CDPI)	NS
SDN - NORTHBOUND INTERFACES (NBI)	NS
SEALED STORAGE	HS
SEARCH AND FILTER	F
SEARCH FOR EVIDENCE	F
SEARCH FOR INFORMATION	F
SEARCH FOR RELATIONS	F
SEARCH FOR SUPPORT	F
SECAAS (SECURITY AS A SERVICE)	DSS
SECOND ORDER ATTACKS	WAM
SECREC CAPACITY	PLT
SECRET KEY	C
SECRET KEY ALGORITHMS	HS
SECRET KEY LIGHT-WEIGHT ALGORITHMS	HS
SECRET SHARING	C
SECURE - AND FAST ENCRYPTION ROUTINE (SAFER)	C
SECURE - COMMUNICATION CHANNELS	C
SECURE - ELECTRONIC TRANSACTION (SET)	WAM
SECURE - FILE TRANSFER PROTOCOL (SFTP)	NS
SECURE - HASH ALGORITHM (SHA)	C
SECURE - HASH ALGORITHM (SHA) - SHA-1	C
SECURE - HASH ALGORITHM (SHA) - SHA-3	C
SECURE - MIME (S/MIME)	WAM
SECURE - MULTIPURPOSE INTERNET MAIL EXTENSION (S/MIME)	WAM
SECURE - REAL-TIME TRANSPORT PROTOCOL (SRTP)	NS
SECURE - SHELL (SSH)	NS
SECURE - SOCKETS LAYER (SSL)	NS
SECURE - SOCKETS LAYER (SSL) - PROTOCOL	C
SECURE CODING PRACTICES	SSL
SECURE DESIGN PRINCIPLES	SSL
SECURE ELEMENT AND SMARTCARD	HS
SECURE FAILURE	SOIM
SECURE HASH ALGORITHM (SHA)	C
SECURE HYPertext TRANSFER PROTOCOL (HTTPS)	WAM
SECURE MICROKERNELS	CPS
SECURE MULTI-PARTY COMPUTATION	C
SECURE MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)	WAM
SECURE PLATFORMS	HS
SECURE POSITIONING	PLT
SECURE POSITIONING BASED ON HIDDEN STATIONS	PLT
SECURE SHELL (SSH)	NS
SECURE SOCKETS LAYER (SSL)	NS
SECURE SOFTWARE LIFECYCLE	CI SSL
SECURING LEGACY SYSTEMS	CPS
SECURITY - ACCESS CONTROLS AND	AAA
SECURITY - ACCOUNTS MANAGER (SAM)	OSV
SECURITY - ADMINISTRATOR	RMG
SECURITY - ARCHITECTURE	SOIM CI
SECURITY - ARCHITECTURE - COMPONENT	SSL
SECURITY - ARCHITECTURE - CONCEPTUAL	SSL
SECURITY - ARCHITECTURE - CONTEXTUAL	SSL
SECURITY - ARCHITECTURE - LOGICAL	SSL
SECURITY - ARCHITECTURE - OPERATIONAL	SSL
SECURITY - ARCHITECTURE - PHYSICAL	SSL
SECURITY - ARCHITECTURE - VULNERABILITIES	SS
SECURITY - ASSERTION MARKUP LANGUAGE (SAML)	AAA
SECURITY - ASSURANCE REQUIREMENTS	SSL
SECURITY - AWARENESS	HF
SECURITY - AWARENESS TRAINING	HF
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP)	SOIM
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP) - ENUMERATIONS	SOIM
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP) - INTEGRITY	SOIM
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP) - LANGUAGES	SOIM
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP) - MEASUREMENT AND SCORING SYSTEMS	SOIM
SECURITY - CONTENT AUTOMATION PROTOCOL (SCAP) - REPORTING FORMATS	SOIM
SECURITY - COUNCIL	RMG
SECURITY - DOMAIN	SSL
SECURITY - EDUCATION	HF
SECURITY - ENGINEERING	SSL
SECURITY - EVENT MANAGEMENT (SEM)	SOIM
SECURITY - EXTERNAL PROGRAM DRIVERS FOR	LR
SECURITY - FOUNDATION	SSL
SECURITY - FUNCTIONAL REQUIREMENTS	SSL
SECURITY - IDSES (INTRUSION DETECTION SYSTEMS) - MOTION ACTIVATED CAMERAS	SOIM
SECURITY - IMPACT ASSESSMENT	SOIM
SECURITY - KERNEL	OSV
SECURITY - MEASUREMENTS	SOIM
SECURITY - MODELS	SOIM
SECURITY - MODELS - BELL-LAPADULA CONFIDENTIALITY MODEL	AAA
SECURITY - MODELS - BIBA INTEGRITY MODEL	AAA
SECURITY - MODELS - BREWER-NASH (THE CHINESE WALL) MODEL	AAA

SECURITY - MODELS - CLARK-WILSON INTEGRITY MODEL	AAA	SECURITY DEVICES - PROXIES - APPLICATION-LEVEL	WAM
SECURITY - MODELS - GRAHAM-DENNING MODEL	AAA	SECURITY DEVICES - PROXIES - CIRCUIT-LEVEL	NS
SECURITY - MODELS - HARRISON-RUZZO-ULLMAN MODEL	AAA	SECURITY DOCUMENTATION REVIEWING	SOIM
SECURITY - MODELS - INFORMATION FLOW MODELS	AAA	SECURITY DOMAIN	SSL
SECURITY - MODELS - LIPNER MODEL	AAA	SECURITY DOMAINS	OSV
SECURITY - MODELS - MATRIX-BASED MODELS	AAA	SECURITY ECONOMICS	CI
SECURITY - MODELS - MULTILEVEL LATTICE MODELS	AAA	SECURITY FAILURES	CI
SECURITY - MODELS - NONINTERFERENCE MODELS	AAA	SECURITY FATIGUE	HF
SECURITY - MODELS - STATE MACHINE MODEL	AAA	SECURITY GAMES	C
SECURITY - OFFICERS MANAGEMENT AND ANALYSIS PROJECT (SOMAP)	SOIM	SECURITY HUBS	CPS
SECURITY - ORGANIZATIONAL STRUCTURE	RMG	SECURITY HYGIENE	HF
SECURITY - PERIMETER	SSL	SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)	SOIM
SECURITY - POLICY	SOIM	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	SOIM
SECURITY - POLICY - DEVELOP AND IMPLEMENT	SOIM	SECURITY KERNEL	OSV
SECURITY - PROGRAM	SOIM	SECURITY METRICS	SOIM RMG
SECURITY - PROGRAM - OVERSIGHT	SOIM	SECURITY MODELS	OSV FMS
SECURITY - SERVICES	SOIM	SECURITY OBJECTIVES	NS
SECURITY - SERVICES - ACCESS CONTROL SERVICES	AAA	SECURITY OPERATIONS	SSL
SECURITY - SERVICES - AUDIT AND MONITORING SERVICES	AAA	SECURITY OPERATIONS AND BENCHMARKING	SOIM
SECURITY - SERVICES - BOUNDARY CONTROL SERVICES	AAA	SECURITY OPERATIONS AND INCIDENTS	CI SOIM
SECURITY - SERVICES - CRYPTOGRAPHIC SERVICES	C	SECURITY OPERATIONS MANAGEMENT	SOIM
SECURITY - SERVICES - INTEGRITY SERVICES	AAA	SECURITY ORCHESTRATION ANALYTICS AND REPORTING (SOAR)	SOIM
SECURITY - SURVEY	SOIM	SECURITY OVERSIGHT COMMITTEE	RMG
SECURITY - SYSTEM-LEVEL	SOIM	SECURITY PARAMETER INDEX (SPI)	RMG
SECURITY - TARGET	SOIM	SECURITY PERIMETER	NS
SECURITY - THROUGH OBSCURITY	C	SECURITY PLANS APPLICABILITY OF	SOIM
SECURITY - TRAINING	HF	SECURITY PLANS APPLICABILITY OF - APPROVAL OF	SOIM
SECURITY - ZONES	NS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - CONTENTS OF	SOIM
SECURITY ADMINISTRATION	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - DEVELOPMENT TOOLS	SOIM
SECURITY ANALYTICS	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - EXAMPLE OF WORK PLAN FOR	SOIM
SECURITY AND PRIVACY CONCERNS	CPS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - FORMAT	SOIM
SECURITY ARCHITECTURE AND LIFECYCLE	CI SSL	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - INCLUSION OF SECURITY	SOIM
SECURITY AS A SERVICE (SECAAS)	DSS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - INFORMATION SOURCES	SOIM
SECURITY ASSESSMENT - GATEWAY TESTING	NS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - INITIATION OF	SOIM
SECURITY ASSESSMENT - IPSS (INTRUSION PREVENTION SYSTEMS)	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - MAINTENANCE	SOIM
SECURITY ASSESSMENT - MONITORING TESTING	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - METRICS FOR	SOIM
SECURITY ASSESSMENT - VULNERABILITY SCANNING	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - MISCONCEPTIONS CONCERNING	SOIM
SECURITY ASSESSMENT - WAR DIALING	PLT	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - OBSERVATIONS	SOIM
SECURITY ASSESSMENT - WAR DRIVING	NS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - OBSERVATIONS -	SOIM
SECURITY ASSESSMENT - WIRELESS NETWORKING TESTING	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - OBSERVATIONS -	SOIM
SECURITY ASSESSMENT - WIRELESS NETWORKING TESTING - TOOLS	NS	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - RESISTANCE TO	SOIM
SECURITY ASSESSMENT PLAN	SOIM	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - SAMPLE DOCUMENTS	SOIM
SECURITY ASSESSMENT REPORT	RMG	SECURITY PLANS APPLICABILITY OF - APPROVAL OF - SECURITY OF	SOIM
SECURITY ASSOCIATION	NS	SECURITY POLICIES	AAA RMG
SECURITY ASSURANCE REQUIREMENTS	SSL	SECURITY POLICY	WAM RMG
SECURITY AUDITS	SOIM	SECURITY PRINCIPLES	WAM
SECURITY AUDITS - ANNUAL	SOIM	SECURITY PRINCIPLES IN INCIDENT MANAGEMENT	SOIM
SECURITY AUDITS - AUDITOR RESPONSIBILITY	SOIM	SECURITY PROCEDURES	SOIM
SECURITY AUDITS - CLOUD AND OUTSOURCED DOMAIN	SOIM	SECURITY PROCEDURES - ACCESS TO	SOIM
SECURITY AUDITS - DOCUMENTATION	SOIM	SECURITY PROCEDURES - COMMON	SOIM
SECURITY AUDITS - DOCUMENTATION - ACCEPTABLE USE	SOIM	SECURITY PROCEDURES - FORMATTING OF	SOIM
SECURITY AUDITS - DOCUMENTATION - BASELINE SECURITY CONFIGURATION	SOIM	SECURITY PROCEDURES - MAINTENANCE OF	SOIM
SECURITY AUDITS - DOCUMENTATION - BUSINESS FLOW	SOIM	SECURITY PROCEDURES - OBSERVATIONS	SOIM
SECURITY AUDITS - DOCUMENTATION - CHANGE MANAGEMENT	SOIM	SECURITY PROCEDURES - OBSERVATIONS - PURPOSE OF	SOIM
SECURITY AUDITS - DOCUMENTATION - DATA CLASSIFICATION	SOIM	SECURITY PROCEDURES - PROCESS FOR DEVELOPING	SOIM
SECURITY AUDITS - DOCUMENTATION - DISASTER/BUSINESS RECOVERY	SOIM	SECURITY PROCEDURES - RESPONSIBILITY FOR	SOIM
SECURITY AUDITS - DOCUMENTATION - HOST CONFIGURATION	SOIM	SECURITY PROCEDURES - STYLE OF	SOIM
SECURITY AUDITS - EVENT TRIGGERED	SOIM	SECURITY PROGRAM - ADMINISTRATIVE ACTIVITIES	SOIM
SECURITY AUDITS - EXIT INTERVIEW	SOIM	SECURITY PROGRAM - ARCHITECTURE IMPLEMENTATION	SOIM
SECURITY AUDITS - FINDINGS PRESENTATION	SOIM	SECURITY PROGRAM - CHALLENGES OF	SOIM
SECURITY AUDITS - LAN DOMAIN	SOIM	SECURITY PROGRAM - COMPONENTS OF	SOIM
SECURITY AUDITS - LAN-TO-WAN DOMAIN	SOIM	SECURITY PROGRAM - CONCEPTS FOR	SOIM
SECURITY AUDITS - MANAGEMENT RESPONSE	SOIM	SECURITY PROGRAM - CONTROLS AND COUNTERMEASURES	SOIM
SECURITY AUDITS - MERGER/ACQUISITION	SOIM	SECURITY PROGRAM - DEFINITION OF	SOIM
SECURITY AUDITS - METHODOLOGIES	SOIM	SECURITY PROGRAM - INFRASTRUCTURE AND ARCHITECTURE OF	SOIM
SECURITY AUDITS - ORDERED	SOIM	SECURITY PROGRAM - MANAGEMENT ACTIVITIES	SOIM
SECURITY AUDITS - REGULATION COMPLIANCE	SOIM	SECURITY PROGRAM - MANAGEMENT FRAMEWORK FOR	RMG
SECURITY AUDITS - REMOTE ACCESS DOMAIN	SOIM	SECURITY PROGRAM - METRICS FOR	SOIM
SECURITY AUDITS - SYSTEM/APPLICATION DOMAIN	SOIM	SECURITY PROGRAM - OBJECTIVES OF	SOIM
SECURITY AUDITS - USER DOMAIN	SOIM	SECURITY PROGRAM - OPERATIONAL ACTIVITIES	SOIM
SECURITY AUDITS - WAN DOMAIN	SOIM	SECURITY PROGRAM - OVERVIEW OF	SOIM
SECURITY AUDITS - WORKSTATION DOMAIN	SOIM	SECURITY PROGRAM - ROAD MAP FOR	RMG
SECURITY AWARENESS	HF	SECURITY PROGRAM - SCOPE AND CHARTER OF	SOIM
SECURITY AWARENESS GAMES	HF	SECURITY PROGRAM - SELF-ASSESSMENT	SOIM
SECURITY AWARENESS TRAINERS	HF	SECURITY PROGRAMS - ARCHITECTURE DESIGN	SSL
SECURITY AWARENESS TRAINING	HF	SECURITY PROGRAMS - ARCHITECTURE DESIGN - ACCOUNTABILITY	AAA
SECURITY CONTROL ASSESSOR - INDEPENDENCE OF	SOIM	SECURITY PROGRAMS - ARCHITECTURE DESIGN - AUTHORIZATION	AAA
SECURITY CONTROL ASSESSOR - INDEPENDENCE OF - RITY CONTROL BASELINE	SOIM	SECURITY PROGRAMS - ARCHITECTURE DESIGN - DOCUMENTATION	SSL
ESTABLISHING	RMG	SECURITY PROGRAMS - ARCHITECTURE DESIGN - LEAST PRIVILEGE	SSL
SECURITY CONTROL ASSESSOR - RESPONSIBILITIES OF	SOIM	SECURITY PROGRAMS - ARCHITECTURE DESIGN - RISK-BASED CONTROLS	SSL
SECURITY CONTROLS	SOIM	SECURITY PROGRAMS - ARCHITECTURE DESIGN - SEPARATION OF DUTIES	SSL
SECURITY CONTROLS - ASSESSMENT OF	SOIM	SECURITY PROGRAMS - AVAILABILITY	SOIM
SECURITY CONTROLS - COMMON	SOIM	SECURITY PROGRAMS - BEST PRACTICES	SSL
SECURITY CONTROLS - DEFINITION OF	POR	SECURITY PROGRAMS - CONFIDENTIALITY	SOIM
SECURITY CONTROLS - DEVELOPMENT OF CERTIFICATION TEST PLAN	SOIM	SECURITY PROGRAMS - INTEGRITY	SOIM
SECURITY CONTROLS - HYBRID	SOIM	SECURITY PROGRAMS - NON-REPUDIATION	C
SECURITY CONTROLS - IMPLEMENTATION OF	SOIM	SECURITY PROGRAMS - PRIVACY	POR
SECURITY CONTROLS - LEVELS OF	POR	SECURITY PROPERTIES	FMS
SECURITY CONTROLS - MONITORING OF	SOIM	SECURITY PROTOCOLS	FMS
SECURITY COST-EFFECTIVENESS	RMG	SECURITY REQUIREMENTS	SSL
SECURITY CULTURE	RMG	SECURITY REVIEWS	RMG
SECURITY DEVICES	NS	SECURITY RISK MANAGEMENT FUNDAMENTAL CONCEPTS OF	RMG
SECURITY DEVICES - FIREWALLS	NS	SECURITY SOFTWARE	MAT
SECURITY DEVICES - FIREWALLS - DYNAMIC PACKET FILTERING	WAM	SECURITY TARGET	SSL
SECURITY DEVICES - FIREWALLS - FILTERING	NS	SECURITY TECHNOLOGY MANAGEMENT	SOIM
SECURITY DEVICES - FIREWALLS - NAT	NS	SECURITY TESTING	SSL
SECURITY DEVICES - FIREWALLS - PAT	NS	SECURITY THROUGH OBSCURITY	C
SECURITY DEVICES - FIREWALLS - PERSONAL	WAM	SECURITY THROUGHOUT THE LIFECYCLE	CI
SECURITY DEVICES - FIREWALLS - STATEFUL INSPECTION	WAM		
SECURITY DEVICES - FIREWALLS - STATIC PACKET FILTERING	WAM		
SECURITY DEVICES - PROXIES	NS		

SECURITY/SUBJECT MATTER PROFESSIONALS	RMG	SIDE-CHANNEL VULNERABILITIES	SS
SEAMLESS TAKEOVER ATTACK	PLT	SIDE-LOADING	WAM
SEGMENT-BASED PROTECTION	OSV	SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)	SOIM
SEGMENTATION	OSV	SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) SOLUTIONS INCIDENT RESPONSE AND	SOIM
SEGMENTATION AND FRAGMENTATION	SOIM	SIEM PLATFORMS AND COUNTERMEASURES	SOIM
SEGREGATION OF DUTIES	C	SIGNAL ANIHILATION AND OVERSHADOWING	PLT
SEGREGATION/SEPARATION OF DUTIES (SOD)	SOIM	SIGNAL RE(P)LAY	PLT
SEIZURE AND FORFEITURE OF SERVERS DOMAIN NAMES AND REGISTRIES	LR	SIGNAL SPOOFING ATTACKS	PLT
SEL4	FMS	SIGNATURE DYNAMICS	AAA
SELF-ASSESSMENT - INCIDENT MANAGEMENT	SOIM	SIGNATURE-BASED IDS	NS
SELF-ASSESSMENT - INFORMATION SECURITY GOVERNANCE	RMG	SIGNATURES	SOIM
SELF-ASSESSMENT - RISK MANAGEMENT	RMG	SIGNING	WAM
SELF-ASSESSMENT - SECURITY PROGRAMS	SOIM	SIM (SECURITY INFORMATION MANAGEMENT)	SOIM
SELF-GARBLING VIRUS	MAT	SIM (SECURITY INFORMATION MODIFICATION MODULE)	OSV
SELF-HELP DISFAVoured: SOFTWARE LOCKS AND HACK-BACK	LR	SIM (SUBSCRIBER IDENTITY MODULE)	HS
SELINUX	AAA OSV	SIMPLE - MAIL TRANSFER PROTOCOL (SMTP)	NS
SEM (SECURITY EVENT MANAGEMENT)	SOIM	SIMPLE - NETWORK MANAGEMENT PROTOCOL (SNMP)	NS
SEMANTIC MATCHING	F	SIMPLE MAIL TRANSPORT PROTOCOL	WAM NS
SEMANTICS-BASED ANALYSIS	FMS	SIMPLE MAIL TRANSPORT PROTOCOL (SMTP)	WAM NS
SEMI-FORMAL DESIGN	SSL	SIMPLE NETWORK MANAGEMENT PROTOCOL	NS
SEMI-FORMAL VERIFIED DESIGN	SSL	SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	NS
SEMIQUANTITATIVE RISK ASSESSMENT	RMG	SIMPLE OBJECT ACCESS PROTOCOL	WAM
SENDER POLICY FRAMEWORK (SPF)	AAA	SIMPLE OBJECT ACCESS PROTOCOL (SOAP)	WAM
SENIOR INFORMATION SECURITY OFFICER - DEFINING	RMG	SIMPLE POWER ANALYSIS	HS
SENIOR INFORMATION SECURITY OFFICER - RESPONSIBILITIES OF	RMG	SIMS	HS
SENIOR INFORMATION SECURITY OFFICER - RESPONSIBILITIES OF - CHANGES IN	RMG	SIMULATION OF CRYPTOGRAPHIC OPERATIONS	C
SENIOR MANAGEMENT - COMMITMENT TO INCIDENT MANAGEMENT	SOIM	SIMULATION TEST	SOIM
SENIOR MANAGEMENT - INFORMATION SECURITY RESPONSIBILITIES OF	RMG	SIMULATION TEST - RECOVERY PLAN	SOIM
SENIOR MANAGEMENT - OBTAINING COMMITMENT OF	RMG	SIMULATION-BASED ANALYSIS	FMS
SENIOR MANAGEMENT - ON CURRENT INCIDENT RESPONSE CAPABILITIES	RMG	SINGLE - LOSS EXPECTANCY (SLE)	RMG
SENIOR MANAGEMENT - RISK MANAGEMENT RESPONSIBILITIES OF	RMG	SINGLE - POINT OF FAILURE (SPOF)	SOIM
SENSE-MAKING LOOP	F	SINGLE - SIGN-ON (SSO)	AAA
SENSITIVE INFORMATION	POR	SINGLE DOMAIN	OSV
SENSITIVITY	RMG	SINGLE SIGN-ON	AAA
SENSITIVITY ASSESSMENT PROCESS	SOIM	SINGLE SIGN-ON (SSO)	AAA
SENSITIVITY ASSESSMENT PROCESS - RESPONSIBILITY FOR	SOIM	SINGLE/MULTI-FACTOR AUTHENTICATION	AAA
SENSOR FUSION	CPS	SINGULATION PROTOCOL (RFID)	HS
SENSOR NETWORKS	CPS	SIP (SESSION INITIATION PROTOCOL)	NS
SENSORS	HS	SITE RELIABILITY ENGINEERING	SOIM
SEPARATION OF DUTIES	SOIM	SITUATIONAL CRIME PREVENTION	AB
SEPARATION OF DUTIES (SOD)	SSL	SITUATIONAL AWARENESS	SOIM
SEPARATION OF PRIVILEGE	CI	SIX SIGMA	RMG
SEQUENCE ERRORS	NS	SKA (SHARED KEY AUTHENTICATION)	NS
SEQUENTIAL CONSISTENCY	DSS	SKILLS - AND LIKELIHOOD OF RISK	RMG
SERVER - MESSAGE BLOCK (SMB)	NS	SKILLS - OF PERSONNEL IN INFORMATION SECURITY	HF
SERVER SIDE MISCONFIGURATIONS & VULNERABLE COMPONENTS	WAM	SKILLS - PROGRAMMING IN INCIDENT MANAGEMENT	SS
SERVER SIDE VULNERABILITIES AND MITIGATIONS	WAM	SLA (SERVICE LEVEL AGREEMENT)	SOIM
SERVER VIRTUALIZATION	OSV	SLACK SPACE	F
SERVER-BASED VULNERABILITIES	NS	SLAS (SERVICE LEVEL AGREEMENTS)	SOIM
SERVICE - LEVEL AGREEMENT (SLA)	SOIM	SLE (SINGLE LOSS EXPECTANCY)	RMG
SERVICE - LEVEL REPORT	SOIM	SMALL SYSTEMS SYSTEM INVENTORY PROCESS	SOIM
SERVICE - LEVEL REQUIREMENTS (SLR)	SOIM	SMALL TCB IMPLEMENTATIONS	HS
SERVICE - ORIENTED ARCHITECTURES (SOA)	DSS	SMART	HS
SERVICE DELIVERY OBJECTIVE - AND INCIDENT RESPONSE	SOIM	SMART (SPECIFIC MEASURABLE ATTAINABLE RELEVANT TIMELY) METRICS	RMG
SERVICE DELIVERY OBJECTIVE - AS BASIS FOR RECOVERY SITE SELECTION	SOIM	SMART GRIDS	CPS
SERVICE DELIVERY OBJECTIVE - DEFINED	SOIM	SMART POINTERS	SS
SERVICE DELIVERY OBJECTIVE - IN RISK MANAGEMENT	RMG	SMARTCARDS	NS
SERVICE LEVEL AGREEMENT (SLA)	SOIM	SMB (SERVER MESSAGE BLOCK)	OSV
SERVICE LEVEL AGREEMENTS (SLA)	SOIM	SMEP AND SMAP	OSV
SERVICE PROVIDERS - APPLICATION SERVICE PROVIDER	DSS	SMPP (SHORT MESSAGE PEER-TO-PEER)	NS
SERVICE PROVIDERS - CLOUD SERVICE PROVIDERS	DSS	SMTP (SIMPLE MAIL TRANSFER PROTOCOL)	NS
SERVICES	F	SMUDGE ATTACKS	WAM
SERVICES COORDINATION CLASS	DSS	SMURF ATTACK	NS
SERVLET	WAM	SNF'S (SECURE NFS)	OSV
SESIP	HS	SNIFFING	NS MAT
SESSION - CONTROL PROTOCOL (SCP)	NS	SNORT	SOIM
SESSION - DESCRIPTION PROTOCOL (SDP)	NS	SOAR: IMPACT AND RISK ASSESSMENT	SOIM
SESSION - HIGHJACKING	MAT	SOC (AICPA SERVICE ORGANIZATION) REPORTS	RMG
SESSION - INITIATION PROTOCOL (SIP)	NS	SOC REPORTING	SOIM
SESSION - KEYS	C	SOCIAL CONTEXT	HF
SESSION - MANAGEMENT	AAA	SOCIAL ENGINEERING - ATTACKS	AB
SESSION BORDER CONTROLLERS	SOIM	SOCIAL ENGINEERING - BAITING	AB
SESSION HIJACKING	WAM	SOCIAL ENGINEERING - PENETRATION TESTING AND	AB
SESSION KEY	C	SOCIAL ENGINEERING - PHONE PHISHING	AB
SESSION KEYS	SS	SOCIAL ENGINEERING - PRETEXTING	AB
SESSION LAYER (OSI)	NS	SOCIAL ENGINEERING - SET (SOCIAL ENGINEERING TOOLKIT)	AB
SESSION MANAGEMENT VULNERABILITIES AND	AAA	SOCIAL ENGINEERING - SHOULDER SURFING	AB
SET (SOCIAL ENGINEER TOOLKIT)	AB	SOCIAL ENGINEERING - VISHING	AB
SETUP ASSUMPTIONS	C	SOCIAL ENGINEERING USE OF IN CERTIFICATION TESTING	HF
SEXTORTION	AB	SOD (SEGREGATION/SEPARATION OF DUTIES)	SOIM
SHA (SECURE HASH ALGORITHM)	C	SOFT TOKEN	AAA
SHA (SECURE HASH ALGORITHM) 0 1 AND 2	C	SOFTWARE	SS
SHADOW IT	SOIM	SOFTWARE - AS A SERVICE (SAAS)	DSS
SHADOW SECURITY	HF	SOFTWARE - DEADLOCK	SS
SHADOW STACKS	OSV	SOFTWARE - DEFINED NETWORKING	NS
SHARED KEY AUTHENTICATION	AAA	SOFTWARE - DEVELOPMENT	SSL
SHARED-DOMAIN ISSUES	SSL	SOFTWARE - DEVELOPMENT - METHODS	SSL
SHIELDING	PLT	SOFTWARE - DEVELOPMENT - METHODS - ITERATIVE DEVELOPMENT	SSL
SHIELDS FROM LIABILITY	LR	SOFTWARE - DEVELOPMENT - METHODS - WATERFALL	SSL
SHIFT ROW TRANSFORMATION	C	SOFTWARE - DEVELOPMENT - SECURITY	SSL
SHORT MESSAGE PEER-TO-PEER (SMPP)	NS	SOFTWARE - ESCROW	SSL
SHORT TERM MEMORY	HF	SOFTWARE - FORENSICS	F
SHORT TRANSACTIONS	DSS	SOFTWARE - INSIDER THREATS	AB
SHORTEST VECTOR PROBLEM	C	SOFTWARE - LICENSING	SOIM
SHOULDER SURFING	WAM AB	SOFTWARE - PROTECTION MECHANISMS	OSV
SIDE CHANNEL ATTACKS	DSS	SOFTWARE - VULNERABILITIES AND	SS
SIDE CHANNELS (HARDWARE)	OSV	SOFTWARE AS A SERVICE (SAAS)	DSS
SIDE CHANNELS (SOFTWARE)	OSV	SOFTWARE DEFINED NETWORKING	NS
SIDE CHANNELS (SPECULATIVE)	OSV	SOFTWARE DEFINED NETWORKING (SDN)	SOIM
SIDE CHANNEL ATTACK	C	SOFTWARE DEVELOPERS	HF
SIDE-CHANNEL ATTACKS AND FAULT ATTACKS	HS		

SOFTWARE FAULT-INJECTION	SS	STICKY POLICIES	POR
SOFTWARE RECONSTRUCTION (INSURANCE COVERAGE)	SOIM	STIDE	SOIM
SOFTWARE-BASED SIDE-CHANNELS	SS	STORAGE	HS DSS
SOUND STATIC VERIFICATION	SS	STORAGE - BACKUPS	SOIM
SOUNDINESS	SS	STORAGE - CLOUD	DSS
SOUNDNESS	SS	STORAGE - PRIMARY	OSV
SOURCE - CODE - ANALYSIS TOOLS	SS	STORAGE - SECONDARY	OSV
SOURCE - CODE - SECURITY ISSUES	SS	STORAGE - THREATS	DSS
SOURCE - CODE - SECURITY ISSUES - BUFFER OVERFLOW	SS	STORAGE - VIRTUAL	DSS
SOURCE - CODE - SECURITY ISSUES - CITIZEN PROGRAMMERS	SS	STORAGE - VIRTUALIZATION	OSV
SOURCE - CODE - SECURITY ISSUES - COVERT CHANNEL	SS	STORAGE - VIRTUALIZED	DSS
SOURCE - CODE - SECURITY ISSUES - EXECUTABLE CONTENT/MOBILE CODE	SS	STORAGE - VIRTUALIZED - HOST-BASED	OSV
SOURCE - CODE - SECURITY ISSUES - MALICIOUS SOFTWARE (MALWARE)	SS	STORAGE - VIRTUALIZED - NETWORK-BASED	OSV
SOURCE - CODE - SECURITY ISSUES - MEMORY REUSE (OBJECT REUSE)	SS	STORAGE - VIRTUALIZED - STORAGE DEVICE-BASED	OSV
SOURCE - CODE - SECURITY ISSUES - SOCIAL ENGINEERING	SS	STORAGE FORENSICS	F
SOURCE - CODE - SECURITY ISSUES - TIME OF CHECK/TIME OF USE (TOC/TOU)	SS	STORAGE IN MOBILE APPLICATIONS	WAM
SP-NETWORK	C	STORAGE SYSTEMS	DSS
SPAM	WAM	STORED INJECTION VULNERABILITIES	SS
SPAM DETECTION	MAT	STORED XSS ATTACKS	WAM
SPAM OVER INSTANT MESSAGING (SPIM)	WAM	STORING	SOIM
SPANNING - TREE ANALYSIS	RMG	STRATEGIC ALIGNMENT - AS OUTCOME OF INFORMATION SECURITY GOVERNANCE	RMG
SPATIAL VULNERABILITIES	SS	STRATEGIC ALIGNMENT - AS OUTCOME OF SECURITY PROGRAMS	SOIM
SPECIAL - PUBLICATIONS (SP)	RMG	STRATEGIC ALIGNMENT - OF INCIDENT MANAGEMENT	SOIM
SPECIAL PERMISSIONS	SOIM	STRATEGIC METRICS	RMG
SPECIALISED EXAMPLES	SOIM	STRATEGIC OBJECTIVES	RMG
SPECIALISED SERVICES	AB	STRATEGIC PLANNING	RMG
SPECIFICATION VS LEARNING	SOIM	STRATEGIES	POR
SPECTRE	HS OSV	STRATEGY DEVELOPMENT	SOIM
SPECULATIVE EXECUTION	OSV	STRATEGY IMPLEMENTATION RESOURCES	SOIM
SPF (SENDER POLICY FRAMEWORK)	WAM	STREAM CIPHER	C
SPKI/SDSI	AAA	STREAM CIPHERS	C
SPLIT KNOWLEDGE	C	STREAM-BASED CIPHERS	C
SPLIT KNOWLEDGE/SPLIT KEY	C	STREAM-BASED CIPHERS - SUBSTITUTION	C
SPML (SERVICE PROVISIONING MARKUP LANGUAGE)	AAA	STRENGTH OF CONTROLS	SOIM
SPONGE CONSTRUCTIONS	C	STRESS TESTING	SSL
SPOOFING	AAA NS AB MAT	STRICT CONSISTENCY	DSS
SPOOFING - BLIND	NS	STRIDE	SSL RMG
SPOOFING - DNS	NS	STRONG CONSISTENCY MODELS	DSS
SPOOFING - DNS - QUERY MANIPULATION	NS	STRONG PUFFS	HS
SPOOFING - E-MAIL	WAM	STRUCTURAL DOMAIN	HS
SPOOFING - EMAIL	WAM	STRUCTURAL TESTING	SSL
SPOOFING - INFORMATION DISCLOSURE	AB	STRUCTURED - QUERY LANGUAGE (SQL)	OSV
SPOOFING - IP ADDRESS SPOOFING	NS	STRUCTURED - WALK-THROUGH TEST	SOIM
SPOOFING - NON-BLIND	NS	STRUCTURED OUTPUT GENERATION VULNERABILITIES	SS
SPOOFING - SESSION HIJACKING	MAT	STRUCTURED OUTPUT GENERATIONS MITIGATIONS	SS
SPOOFING - SYN SCANNING	NS	STRUCTURED P2P PROTOCOLS	DSS
SPOOFING ATTACKS	PLT	STRUCTURED QUERY LANGUAGE (SQL)	OSV
SPX (SEQUENCED PACKET EXCHANGE)	NS	STRUCTURED WALK-THROUGH	SOIM
SPYWARE	MAT	STRUCTURED WALKTHROUGH TEST	SOIM
SPYWARE - BOTNETS	MAT	STRUCTURED WALKTHROUGH TEST - RECOVERY PLAN	SOIM
SQL INJECTION	SS	SUBJECT	AAA
SQL-INJECTION	WAM	SUBJECT MATTER AND REGULATORY FOCUS	LR
SQUARE	SSL	SUBJECTS	AAA
SSAA	SOIM	SUBJECTS - ABAC	AAA
SSH (SECURE SHELL)	NS	SUBJECTS - APPLICATIONS	AAA
SSID (SERVICE SET IDENTIFIER) FLAW	NS	SUBJECTS - AUTHORIZED USERS	AAA
SSL STRIPPING	NS	SUBJECTS - BELL-LAPADULA MODEL	AAA
SSO	SSL	SUBJECTS - NETWORKS	NS
SSO (SINGLE SIGN-ON)	AAA	SUBJECTS - OBJECTS COMPARISON	AAA
SST (STRUCTURED STREAM TRANSPORT)	NS	SUBJECTS - PRIVILEGE ATTRIBUTES	OSV
STACK CANARIES	SS	SUBJECTS - PROCESSES	OSV
STACK MEMORY	OSV	SUBJECTS - REQUIREMENTS	OSV
STACKOVERFLOW	HF	SUBJECTS - SENSITIVITIES	OSV
STAKEHOLDER ENGAGEMENT	HF	SUBJECTS - SYSTEMS	OSV
STAKEHOLDERS	RMG	SUBJECTS - UNAUTHORIZED USERS	SOIM
STAMP	RMG	SUBSTITUTE BYTES	C
STANDALONE OR HOST-PROGRAM	MAT	SUBSTITUTION	C
STANDARD	RMG	SUBSTITUTION CIPHER	C
STANDARD PERMISSIONS	OSV	SUBSTITUTION ENCRYPTION	C
STANDARD PROTOCOLS	C	SUPERDISTRIBUTION	AAA
STANDARDS - COMPLIANCE WITH	SOIM	SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)	CPS
STANDARDS - DEVELOPMENT OF FOR ACTION PLAN	RMG	SUPPLEMENTAL CONTROL TECHNOLOGIES	AAA WAM NS
STANDARDS - FOR INCIDENT MANAGEMENT	SOIM	SUPPLIES FOR INCIDENT RESPONSE	SOIM
STANDARDS - FOR INFORMATION SECURITY GOVERNANCE	RMG	SUPPLY CHAIN	LR
STANDARDS AND FRAMEWORKS	RMG	SUPPLY CHAIN OPERATIONS REFERENCE	RMG
STANDARDS FOR THE PRESENTATION OF SCIENTIFIC EVIDENCE IN LEGAL		SUPPLY CHAIN OPERATIONS REFERENCE (SCOR)	RMG
PROCEEDINGS	F	SUPPORT VECTOR MACHINES	SOIM
STANDARDS MINIMUM SECURITY BASELINE	SOIM	SUPPORTED GOALS	RMG
STAR TOPOLOGY	NS	SUPPRESSION	POR
STAR TOPOLOGY - TOKEN RING AND	NS	SURVIVABILITY THROUGH REPLICATION	DSS
STATE ACTORS	AB	SVCS (SWITCHED VIRTUAL CIRCUITS)	NS
STATE CYBER OPERATIONS IN GENERAL	LR	SWAM (SOFTWARE INVENTORY MANAGEMENT)	SSL
STATE-CENTRIC	F	SWGDE (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE)	F
STATEFUL INSPECTION	NS	SWIPE CARD	HS
STATEMENT - ON AUDITING STANDARDS (SAS)	SOIM	SWISS-CHEESE MODEL	CI HF
STATIC ANALYSIS	SSL	SWITCH POISONING ATTACK	NS
STATIC - SOURCE CODE ANALYSIS (SAST)	SSL	SWITCHED NETWORK	NS
STATIC ANALYSIS	MAT	SWITCHED VIRTUAL CIRCUITS	NS
STATIC CHECKS	SS	SWITCHED VIRTUAL CIRCUITS (SVCS)	NS
STATIC DETECTION	SS	SWITCHES	NS
STATIC PACKET FILTERING	NS	SYBIL ATTACKS	DSS
STATIC PASSWORDS	AAA	SYMBOLIC EXECUTION	MAT
STATIC PASSWORDS - TOKENS	AAA	SYMMETRIC - ALGORITHMS	C
STATIC ROUTING TABLES	NS	SYMMETRIC - ALGORITHMS - ADVANTAGES AND DISADVANTAGES	C
STATION-TO-STATION PROTOCOL	C	SYMMETRIC - CRYPTOGRAPHY	C
STATISTICAL ATTACK	C	SYMMETRIC ALGORITHMS	C
STEALTH	AB	SYMMETRIC CRYPTOGRAPHY	C
STEALTH VIRUS	MAT	SYMMETRIC CRYPTOGRAPHY - AES (ADVANCED ENCRYPTION STANDARD) - CCMP	C
STEERING COMMITTEE	RMG	SYMMETRIC CRYPTOGRAPHY - AES (ADVANCED ENCRYPTION STANDARD) - RIJNDael	C
STEGANOGRAPHIC METHODS	POR		
STEGANOGRAPHY	POR		

SYMMETRIC CRYPTOGRAPHY - BLOWFISH C
 SYMMETRIC CRYPTOGRAPHY - CAST C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - 3DES C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - ADVANTAGES C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - BLOCK CIPHER MODES C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - DISADVANTAGES C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - DOUBLE DES C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - MEET-IN-THE-MIDDLE C
 SYMMETRIC CRYPTOGRAPHY - DES (DATA ENCRYPTION STANDARD) - STREAM MODES C
 SYMMETRIC CRYPTOGRAPHY - IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM) C
 SYMMETRIC CRYPTOGRAPHY - RC4 C
 SYMMETRIC CRYPTOGRAPHY - RCS C
 SYMMETRIC CRYPTOGRAPHY - SAFER (SECURE AND FAST ENCRYPTION ROUTINE) C
 SYMMETRIC CRYPTOGRAPHY - TWOFISH C
 SYMMETRIC ENCRYPTION AND AUTHENTICATION C
 SYMMETRIC KEY ENCRYPTION C
 SYMMETRIC MODE MULTIPROCESSING C
 SYMMETRIC PRIMITIVES C
 SYMMETRIC RBAC AAA
 SYMMETRY OF INTERFACES DSS
 SYN NS
 SYN FLOODING NS
 SYN SCANNING NS
 SYNCHRONOUS C DSS
 SYNCHRONOUS - DYNAMIC RANDOM-ACCESS MEMORY (SDRAM) OSV
 SYNCHRONOUS - TOKEN DEVICE AAA
 SYNCHRONOUS DYNAMIC PASSWORD TOKENS AAA
 SYNCHRONOUS ENCRYPTION C
 SYNCHRONOUS TOKENS AAA
 SYNTACTIC MATCHING F
 SYNTHETIC TRANSACTIONS WAM
 SYSLOG SOIM
 SYSTEM - COMPONENTS SSL
 SYSTEM - DEVELOPMENT LIFE CYCLE (SDLC) SSL
 SYSTEM - EVENTS OSV
 SYSTEM - LIFE CYCLE (SLC) SSL CI
 SYSTEM ACCESS OSV
 SYSTEM ADMINISTRATOR/MANAGER - ROLE OF IN CERTIFICATION TESTING SOIM
 SYSTEM AND KERNEL LOGS SOIM
 SYSTEM APPLICATIONS WAM
 SYSTEM AUTHORIZATION - ACTIONS FOLLOWING ACCREDITATION SOIM RMG
 SYSTEM AUTHORIZATION - ASSESSMENT FOCUS SOIM
 SYSTEM AUTHORIZATION - AUTHORITY SOIM
 SYSTEM AUTHORIZATION - AWARENESS TRAINING AND EDUCATION HF
 SYSTEM AUTHORIZATION - AWARENESS TRAINING AND EDUCATION - CASE STUDY HF
 SYSTEM AUTHORIZATION - BENEFITS OF SOIM RMG
 SYSTEM AUTHORIZATION - DECISION MAKING SOIM
 SYSTEM AUTHORIZATION - DEFINING SOIM RMG
 SYSTEM AUTHORIZATION - DESCRIPTION OF RMG
 SYSTEM AUTHORIZATION - GUIDANCE DEVELOPMENT LIFE CYCLE SOIM
 SYSTEM AUTHORIZATION - GUIDELINES RMG
 SYSTEM AUTHORIZATION - INTEGRATION OF INTO THE SDLC SSL
 SYSTEM AUTHORIZATION - INTERCONNECTED SYSTEMS AND AAA
 SYSTEM AUTHORIZATION - INTERRELATIONSHIPS OF PROCESSES RMG
 SYSTEM AUTHORIZATION - LEGAL AND REGULATORY FRAMEWORK FOR LR
 SYSTEM AUTHORIZATION - LEGAL AND REGULATORY FRAMEWORK FOR - LIFE CYCLE LR
 SYSTEM AUTHORIZATION - LEVEL OF EFFORT AND CERTIFICATION TESTING SOIM
 SYSTEM AUTHORIZATION - OBSERVATIONS SOIM RMG
 SYSTEM AUTHORIZATION - PROGRAM INTEGRATION RMG
 SYSTEM AUTHORIZATION - PROGRAM MANAGER (SEE PROGRAM MANAGER) SOIM
 PROGRAM SCOPE SOIM
 SYSTEM AUTHORIZATION - REASONS FOR FAILURE SOIM
 SYSTEM AUTHORIZATION - REMEDIATION PLANNING SOIM
 SYSTEM AUTHORIZATION - RESISTANCE TO HF
 SYSTEM AUTHORIZATION - RISK ASSESSMENT IN RMG
 SYSTEM AUTHORIZATION - SAMPLE POLICY SOIM
 SYSTEM AUTHORIZATION - SECURITY CONTROLS SELECTION SOIM
 SYSTEM AUTHORIZATION - SECURITY PLANS SOIM
 SYSTEM AUTHORIZATION - SECURITY PROCEDURES IN SOIM
 SYSTEM AUTHORIZATION - SYSTEM-LEVEL SECURITY USING SOIM
 SYSTEM AUTHORIZATION - SYSTEM-LEVEL SECURITY USING - TRUST RELATIONSHIPS SOIM
 SYSTEM AUTHORIZATION - TIMING OF SOIM
 SYSTEM BOUNDARIES - GUIDANCE ON THE IMPACT OF TECHNOLOGICAL CHANGES ON SSL
 SYSTEM CHARACTERIZATION RMG
 SYSTEM DEVELOPMENT SSL
 SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) SSL
 SYSTEM EXITS SOIM
 SYSTEM INVENTORY PROCESS - COMBINING SYSTEMS SOIM
 SYSTEM INVENTORY PROCESS - INFORMATION COLLECTION SOIM
 SYSTEM INVENTORY PROCESS - SMALL SYSTEMS SOIM
 SYSTEM INVENTORY PROCESS - TOOLS SOIM
 SYSTEM INVENTORY PROCESS - VALIDATION SOIM
 SYSTEM LIFECYCLE CI SSL
 SYSTEM OWNER - CRITICALITY IN THE VIEW OF SOIM RMG
 SYSTEM OWNER - DATA SENSITIVITY ASSESSMENT RESPONSIBILITY OF SOIM
 SYSTEM OWNER - RESPONSIBILITIES OF SOIM RMG
 SYSTEM OWNER - RESPONSIBILITIES OF - RESPONSIBILITY OF FOR INTERCONNECTIVITY AGREEMENTS SOIM
 SYSTEM OWNER - RESPONSIBILITY FOR CONFIGURATION MANAGEMENT/CONFIGURATION CONTROL SOIM
 SYSTEM OWNER - RESPONSIBILITY OF FOR RISK REMEDIATION PLAN SOIM
 SYSTEM OWNER - RESPONSIBILITY OF FOR SECURITY PROCEDURES SOIM
 SYSTEM OWNER - SECURITY PLANNING AND SOIM
 SYSTEM OWNERS RMG

SYSTEM SECURITY PLANS SOIM
 SYSTEM SENSITIVITY SOIM
 SYSTEM SENSITIVITY - SECURITY CONTROLS ACCORDING TO SOIM
 SYSTEM SENSITIVITY - SECURITY CONTROLS ACCORDING TO - EM-SPECIFIC CONTROLS SOIM
 SYSTEM TESTING SSL
 SYSTEM-LEVEL SECURITY SOIM
 SYSTEMS HS OSV
 SYSTEMS - ACCESS CONTROL AND OSV
 SYSTEMS - ASSURANCE SOIM
 SYSTEMS - INTEGRITY SOIM
 SYSTEMS ADMINISTRATION SOIM
 SYSTEMS CONTROL AUDIT REVIEW FILE (SCARF) RMG
 SYSTEMS COORDINATION STYLES DSS
 SYSTEMS LIFECYCLE CI SSL
 SYSTEMS NETWORK ARCHITECTURE (SNA) NS
 SYSTEMS PROGRAMMING OSV
 SYSTRUST RMG

T

TAAS (INFORMATION AS A SERVICE) DSS
 TABNABBING ATTACK METHOD WAM MAT
 TACTICAL METRICS SOIM
 TACTICAL PLANNING SOIM
 TAG COLLISION (RFID) HS
 TAILORING SOIM
 TAINT ANALYSIS SS
 TAKE OWNERSHIP PERMISSION OSV
 TAKE-DOWN PROCEDURES LR
 TAKEDOWN RESILIENT ARCHITECTURES AB
 TALLINN MANUAL CPS
 TAMARIN FMS
 TAMPER DETECTION C
 TAMPER EVIDENCE HS
 TAMPER RESISTANCE AAA HS
 TAMPERING NS
 TANGLER POR
 TARGET - IDENTIFICATION AB
 TARGET - OF EVALUATION (TOE) SOIM
 TASKS RMG
 TASKS - MEASURING PROGRAM EFFECTIVENESS RMG
 TCB (TRUSTED COMPUTING BASE) OSV
 TCO (TOTAL COST OF OWNERSHIP) RMG
 TCP (TRANSMISSION CONTROL PROTOCOL) NS
 TCP (TRANSMISSION CONTROL PROTOCOL) - DYNAMIC PORTS NS
 TCP (TRANSMISSION CONTROL PROTOCOL) - PRIVATE PORTS NS
 TCP (TRANSMISSION CONTROL PROTOCOL) - REGISTERED PORTS NS
 TCP (TRANSMISSION CONTROL PROTOCOL) - WELL-KNOWN PORTS NS
 TCP SEQUENCE NUMBER ATTACKS NS
 TCP/IP MODEL NS
 TCSEC (TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA) SSL
 TECHNICAL ASPECTS AAA
 TECHNICAL CHALLENGES F
 TECHNICAL COMPONENTS FOR INFORMATION SECURITY FRAMEWORK SOIM
 TECHNICAL CONTROLS SSL
 TECHNICAL CONTROLS - ANALOG PLT
 TECHNICAL CONTROLS - ATTACKS AND PLT
 TECHNICAL CONTROLS - AUDIT TRAILS AAA
 TECHNICAL CONTROLS - AUTHENTICATION AAA
 TECHNICAL CONTROLS - CELLULAR PLT
 TECHNICAL CONTROLS - CONVERGED NS
 TECHNICAL CONTROLS - CONVERGED - FCOE NS
 TECHNICAL CONTROLS - CONVERGED - ISCSI CPS
 TECHNICAL CONTROLS - CONVERGED - MPLS NS
 TECHNICAL CONTROLS - DIGITAL NS
 TECHNICAL CONTROLS - IDENTIFICATION AAA
 TECHNICAL CONTROLS - LOGICAL AAA
 TECHNICAL CONTROLS - PBX (PRIVATE BRANCH EXCHANGE) PLT
 TECHNICAL CONTROLS - POTS (PLAIN OLD TELEPHONE SERVICE) PLT
 TECHNICAL CONTROLS - PUBLIC ACCESS AAA
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) WAM
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) - CODECS WAM
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) - JITTER WAM
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) - PACKET LOSS WAM
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) - SEQUENCE ERRORS WAM
 TECHNICAL CONTROLS - VOIP (VOICE OVER INTERNET PROTOCOL) - SIP NS
 TECHNICAL CONTROLS CERTIFICATION TESTING OF SOIM
 TECHNICAL GUIDELINE NCSG-TG-029 RMG
 TECHNICAL SECURITY ARCHITECTURE SOIM
 TECHNICAL SECURITY MANAGEMENT SOIM
 TECHNICAL SUPPORT SOIM
 TECHNICAL THREATS SOIM
 TECHNOCRATIC RMG
 TECHNOLOGICAL CONTENT FILTERING LR
 TECHNOLOGY - FOR INCIDENT MANAGEMENT SOIM
 TECHNOLOGY - FOR INFORMATION RISK MANAGEMENT RMG
 TECHNOLOGY - FOR SECURITY PROGRAMS SOIM
 TECHNOLOGY - IN BUSINESS MODEL FOR INFORMATION SECURITY RMG
 TELECOMMUTING SOIM
 TELL STORY F
 TELNET NS
 TEMPERATURE HF

TEMPLATE ATTACKS	HS	TIME OF CONTRACT AND RECEIPT OF CONTRACTUAL COMMUNICATION	LR
TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)	NS	TIME OF FLIGHT BASED RANGING ATTACKS	PLT
TEMPORAL VULNERABILITIES	SS	TIME OUTS (AUTHENTICATION)	AAA
TEMPORARY FILES	F SS	TIME-DIVISION MULTIPLEXING	PLT
TERMINATION	DSS	TIME-DIVISION MULTIPLEXING (TDM)	PLT
TERMS	HF	TIME-OF-CHECK TO TIME-OF-USE	SS
TERRITORIAL LOCATION OF THE RIGHT TO DEMAND REPAYMENT OF BANK DEPOSITS	LR	TIME-RELATED PARAMETERS	PLT
TERRORIST FRAUD	PLT	TIMEOUTS	SOIM
TERRORISTS AND ACTIVISTS	CPS	TIMESTAMPS	SOIM
TEST	RMG	TIMING	SOIM RMG
TEST - PLAN REVIEW	SOIM	TIMING ATTACKS	HS
TEST - STRATEGIES	SOIM	TIMING BASED	DSS
TEST DATA	SSL	TIMING RESTRICTIONS	PLT
TEST PLAN DEVELOPMENT	SSL	TIMING SIDE-CHANNELS	NS
TEST PROGRAMS	SSL	TKIP (TEMPORAL KEY INTEGRITY PROTOCOL) ATTACK	NS
TEST TYPES	SSL	TLD (TOP LEVEL DOMAIN)	NS
TESTING - APPLICATION SECURITY	WAM	TLS	C
TESTING - AUTOMATED	SSL	TLS ATTACKS	NS
TESTING - BLACK-BOX	SSL	TOE (TARGET OF EVALUATION)	SOIM
TESTING - CHECKLIST TEST	SOIM	TOGAF	RMG
TESTING - DENIAL-OF-SERVICE	NS	TOGAF (THE OPEN GROUP ARCHITECTURE FRAMEWORK)	RMG
TESTING - DYNAMIC	SSL	TOGAF SECURITY ARCHITECTURE	RMG
TESTING - FULL INTERRUPTION TESTING	SOIM	TOKEN	AAA C
TESTING - FULL-INTERRUPTION	SOIM	TOKEN - PASSING	NS
TESTING - INCIDENT RESPONSE	SOIM	TOKEN - RING (IEEE 802.5)	NS
TESTING - INTERFACE	SS	TOKEN RINGS	NS
TESTING - MANUAL	SSL	TOKENISATION OF SENSITIVE DATA	SSL
TESTING - MISUSE CASE	SS	TOKENS	AAA
TESTING - NEGATIVE	SS	TOKENS - ASYNCHRONOUS	AAA
TESTING - NEGATIVE - SCENARIOS	SS	TOKENS - ASYNCHRONOUS PASSWORD	AAA
TESTING - OF CONTROLS	SOIM	TOKENS - CHALLENGE RESPONSE	AAA
TESTING - PARALLEL TESTING	SOIM	TOKENS - PASSING	NS
TESTING - PATCH	SOIM	TOKENS - STATIC PASSWORD	AAA
TESTING - PBX AND IP TELEPHONY	PLT	TOKENS - SYNCHRONOUS	AAA
TESTING - PENETRATION	SOIM	TOKENS - SYNCHRONOUS DYNAMIC PASSWORD	AAA
TESTING - RECOVERY PLAN	SOIM	TOOLS	FMS
TESTING - SIMULATION TEST	SOIM	TOOLS - BUSINESS PROCESS REVIEW	RMG
TESTING - STATIC	SSL	TOOLS - CONTROL MONITORING AND REPORTING	SOIM
TESTING - STRUCTURED WALKTHROUGH TEST	SOIM	TOOLS - DATA COLLECTION AND EXTRACTION	SOIM
TESTING - WHITE-BOX	SSL	TOOLS - RISK SCENARIO DEVELOPMENT	RMG
TESTING - WIRELESS NETWORK	NS	TOP-DOWN PROCESSES	F
TESTING A PROPRIETARY CRYPTOGRAPHIC ALGORITHM	LR	TOP-LEVEL DOMAIN (TLD)	NS
TESTING AND VALIDATING INTRUSION DETECTION SYSTEM	SOIM	TOPOGRAPHIES - BUS	NS
TESTING PHASE	SSL	TOPOGRAPHIES - MESH	NS
TF-CSIRT	SOIM	TOPOGRAPHIES - MESH TOPOLOGY	NS
TFTP (TRIVIAL FILE TRANSFER PROTOCOL)	NS	TOPOGRAPHIES - RING	NS
THE BASE-RATE FALACY	SOIM	TOPOGRAPHIES - RING TOPOLOGY	NS
THE ENFORCEMENT OF AND PENALTIES FOR CRIMES AGAINST INFORMATION SYSTEMS	LR	TOPOGRAPHIES - STAR	NS
THE FORAGING LOOP	F	TOPOGRAPHIES - STAR TOPOLOGY	NS
THE LAW OF ARMED CONFLICT	LR	TOPOGRAPHIES - TREE	NS
THE OPEN GROUP ARCHITECTURE FRAMEWORK (TOGAF)	RMG	TOPOLOGY	NS
THE SENSE MAKING LOOP	F	TOPOLOGY AWARE LOCALISED ECLIPSE ATTACKS	DSS
THEOREM PROVING	CI	TOR	POR
THEOREM PROVING TOOLS	FMS	TOTAL COST OF OWNERSHIP (TCO)	RMG
THEORY	AAA	TOTAL RISK	RMG
THIN CLIENT SYSTEMS	OSV	TOUCH-TO-ACCESS PRINCIPLE	CPS
THINKING, FAST AND SLOW	HF	TOUCHPOINTS	SSL
THIRD-PARTY - GOVERNANCE	RMG	TPM	SSL
THIRD-PARTY - SECURITY SERVICES	SOIM	TPM (TRUSTED PLATFORM MODULE)	HS
THIRD-PARTY APPLICATIONS	WAM	TPMS	HS OSV
THREAT	AB RMG	TRACEROUTE	NS
THREAT - EMERGING	AB RMG	TRACING	AAA MAT
THREAT - EXTERNAL	AB RMG	TRADE SECRETS	LR
THREAT - INTERNAL	AB RMG	TRADEMARK	LR
THREAT AGENT IDENTIFICATION	SSL	TRADEMARKS	LR
THREAT AGENTS	AB	TRAFFIC ANALYSIS	F
THREAT ANALYSIS	RMG	TRAFFIC FLOW CONTROL	CPS
THREAT ASSESSMENT - DEFINED	RMG	TRAFFIC METADATA	POR
THREAT ASSESSMENT - IN INFORMATION SECURITY STRATEGY	SOIM	TRAINING	HF RMG
THREAT ASSESSMENT - IN SECURITY PROGRAM MANAGEMENT	SOIM	TRAINING - FOR ACTION PLAN	HF
THREAT EVENT	SOIM	TRAINING - FOR RISK MANAGEMENT	HF
THREAT IDENTIFICATION	RMG	TRAINING - IN SECURITY PROGRAMS	HF
THREAT IDENTIFICATION - EXAMPLE LIST	RMG	TRAINING - OF INCIDENT RESPONSE STAFF	HF
THREAT MODEL	HS RMG	TRAINING AND INDUCEMENT OF BEHAVIOUR CHANGE	RMG
THREAT VECTOR	AB	TRANS-BORDER DATA FLOW	LR
THREAT(S)	RMG	TRANSACTION AUTHORIZATION	AAA
THREAT(S) - AGENT	AB	TRANSACTION LOG	SOIM
THREAT(S) - EXTERNAL	SOIM	TRANSACTION PROCESSING (TP)	OSV
THREAT(S) - IDENTIFY	SOIM RMG	TRANSACTIONAL SERVICES, DATABASES	DSS
THREAT(S) - INTERNAL	SOIM	TRANSBORDER DATA FLOW	LR
THREAT(S) - MODELING	SOIM	TRANSCRIPTION	F
THREATS	AB	TRANSDUCTION ATTACKS ON SENSORS	CPS
THREATS - ADDRESSING	SOIM	TRANSFER MODES	NS
THREATS - ADVANCED PERSISTENT THREATS	AB	TRANSFER MODES - ACTIVE (PORT)	NS
THREATS - DEFINED	RMG	TRANSFER MODES - PASSIVE (PASV)	NS
THREATS - ENVIRONMENTAL	SOIM	TRANSFERS PURSUANT TO INTERNATIONAL MUTUAL LEGAL ASSISTANCE TREATY	LR
THREATS - IN INCIDENT MANAGEMENT	SOIM	TRANSISTOR LAYOUT	HS
THREATS - IN RISK ASSESSMENT	RMG	TRANSISTORS	HS
THREATS - MAN-MADE	AB	TRANSMISSION (NETWORK)	NS
THREATS - TECHNICAL	SOIM	TRANSMISSION (NETWORK) - WIRELESS SECURITY - AD-HOC MODE	NS
THREATS AND RISK	SSL	TRANSMISSION (NETWORK) - WIRELESS SECURITY - INFRASTRUCTURE MODE	NS
THREATS TO SECURITY FOR MODERN OSS	OSV	TRANSMISSION (NETWORK) - WIRELESS SECURITY - OSA	AAA
TICKET GRANTING SERVER	AAA	TRANSMISSION (NETWORK) - WIRELESS SECURITY - PARKING LOT ATTACK	AB
TIER 1 RISK MANAGEMENT	RMG	TRANSMISSION (NETWORK) - WIRELESS SECURITY - SHARED KEY AUTHENTICATION	AAA
TIER 2 RISK MANAGEMENT	RMG	TRANSMISSION (NETWORK) - WIRELESS SECURITY - SKA	NS
TIER 2 RISK MANAGEMENT - MEASURING PROGRAM EFFECTIVENESS	RMG	TRANSMISSION (NETWORK) - WIRELESS SECURITY - SSID FLAW	NS
TIER 3 RISK MANAGEMENT	RMG	TRANSMISSION (NETWORK) - WIRELESS SECURITY - TKIP ATTACK	NS
TIME	HS	TRANSMISSION (NETWORK) - WIRELESS SECURITY - WEP	NS
TIME - AS RECOVERY TEST METRIC	F	TRANSMISSION (NETWORK) - WIRELESS SECURITY - WEP VULNERABILITY	NS
		TRANSMISSION (NETWORK) - WIRELESS SECURITY - WPA/WPA2	NS

TRANSMISSION CONTROL PROTOCOL (TCP) NS
TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP) NS
TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP) - TERMINAL EMULATION PROTOCOL (TELNET) NS
TRANSPARENCY POR
TRANSPARENCY IN CONTROLS SOIM
TRANSPARENT RMG
TRANSPORT LAYER (OSI) - ACK (ACKNOWLEDGEMENT FIELD SIGNIFICANT) NS
TRANSPORT LAYER (OSI) - DATA TRANSMISSIONS NS
TRANSPORT LAYER (OSI) - FIN (NO MORE DATA FROM SENDER) NS
TRANSPORT LAYER (OSI) - PROTOCOLS - FCP NS
TRANSPORT LAYER (OSI) - PROTOCOLS - RDP NS
TRANSPORT LAYER (OSI) - PROTOCOLS - SCTX NS
TRANSPORT LAYER (OSI) - PROTOCOLS - SCTP NS
TRANSPORT LAYER (OSI) - PROTOCOLS - SPX NS
TRANSPORT LAYER (OSI) - PROTOCOLS - SST NS
TRANSPORT LAYER (OSI) - PROTOCOLS - TCP NS
TRANSPORT LAYER (OSI) - PROTOCOLS - UDP NS
TRANSPORT LAYER (OSI) - PSH (PUSH FUNCTION) NS
TRANSPORT LAYER (OSI) - RST (RESET THE CONNECTION) NS
TRANSPORT LAYER (OSI) - SYN (SYNCHRONIZE SEQUENCE NUMBERS) NS
TRANSPORT LAYER (OSI) - URG (URGENT POINTER FIELD SIGNIFICANT) NS
TRANSPORT LAYER SECURITY (TLS) NS
TRANSPORT MODE NS
TRANSPORT PROTOCOL SOIM
TRANSPORT-LAYER SECURITY NS
TRANSPORTATION SYSTEMS AND AUTONOMOUS VEHICLES CPS
TRANSPPOSITION C
TRAPDOOR/BACKDOOR MAT
TRAPPED ERRORS SS
TRAVERSE FOLDER/EXECUTE FILE PERMISSION OSV
TRBAC (TEMPORAL ROLE-BASED ACCESS CONTROL) AAA
TREE TOPOLOGY NS
TRIAGE (INCIDENT MANAGEMENT PROCESSES) SOIM
TRIAGE PHASE SOIM
TRIGGERING SOIM
TRIPLE DES (3-DES) C
TRIVIAL FILE TRANSPORT PROTOCOL NS
TRIVIAL FILE TRANSPORT PROTOCOL (TFTP) NS
TROJAN CIRCUITS HS
TROJAN HORSE MAT
TROJANS MAT
TROJANS - BACKDOOR MAT
TRUE RANDOM NUMBER GENERATION (TRNG) HS
TRUST ARCHITECTURE WAM
TRUST IN CONTROLS SOIM
TRUST NO ONE (TERM) SOIM
TRUST PATH AAA
TRUST RELATIONSHIPS POR
TRUST TRANSIVITY AAA
TRUST TYPES AAA
TRUSTED - COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC) SSL
TRUSTED - COMPUTING BASE (TCB) OSV
TRUSTED - PATH SS
TRUSTED - PLATFORM MODULE (TPM) HS
TRUSTED COMPUTE POOLS SSL
TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA OSV
TRUSTED COMPUTING SSL
TRUSTED COMPUTING BASE (TCB) AAA
TRUSTED EXECUTION ENVIRONMENT HS
TRUSTED PATH SS
TRUSTED PLATFORM MODULE (TPM) HS
TRUSTED PLATFORM MODULE ENDPOINT SECURITY HS
TRUSTED SYSTEM OSV
TUNNEL MODE NS
TUNNELING NS POR
TUNNELING - FIREWALLS NS
TUNNELING - L2TP (LAYER 2 TUNNELING PROTOCOL) NS
TUNNELING - PPTP (POINT-TO-POINT TUNNELING PROTOCOL) NS
TUNNELING - RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) AAA
TUNNELING - SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) NS
TURN-ON TRANSIENT DURATION PLT
TWO-FACTOR AUTHENTICATION AAA
TWO-FACTOR AUTHENTICATION (2FA) AAA
TWO-PHASE COMMIT OSV
TWO-WAY TRUST AAA
TWOFISH C
TYPE 1 HYPERVISOR MAT
TYPE 2 HYPERVISOR MAT
TYPE CERTIFICATION SOIM
TYPE I ERROR AAA
TYPE II ERROR AAA
TYPE SYSTEMS SS
TYPES MAT
TYPES - BOOT SECTOR INFECTORS MAT
TYPES - COMPANION MAT
TYPES - EMAIL MAT
TYPES - FILE INFECTORS MAT
TYPES - MACRO MAT
TYPES - MULTIPARTITE MAT
TYPES - SCRIPT MAT
TYPES - SCRIPT HOST MAT
TYPES - SYSTEM INFECTORS MAT

U

UDP (USER DATAGRAM PROTOCOL) NS
UEFI OSV
UNAUTHORISED ACCESS, HARM OR MISUSE CI
UNAUTHORIZED CRYPTOCURRENCY MINING AB
UNAUTHORIZED DISCLOSURE POR
UNAUTHORIZED USERS AAA
UNCERTAINTY ANALYSIS RMG
UNCOORDINATED SPREAD SPECTRUM TECHNIQUES PLT
UNDER FREQUENCY LOAD SHEDDING (UFLS) CPS
UNDERGROUND ECO-SYSTEM MAT
UNDERGROUND FORUMS AB
UNDERSTANDING INTELLECTUAL PROPERTY LR
UNDISCLOSED SOFTWARE LOCKS LR
UNICAST NS
UNICAST NETWORK TRANSMISSIONS NS
UNIFIED MODELING LANGUAGE (UML) SSL
UNIFORM RESOURCE LOCATOR (URL) WAM
UNIFORM RESOURCE LOCATORS (URLS) WAM
UNIKERNEL OSV
UNINITIALISED DATA LEAKAGE OSV
UNIQUENESS PLT
UNIT TESTING SSL
UNITED STATES - COMMERCE CONTROL LIST LR
UNITED STATES - COMMERCE CONTROL LIST - CATEGORY 4 LR
UNITED STATES - COMMERCE CONTROL LIST - CATEGORY 5 PART 1 LR
UNITED STATES - COMMERCE CONTROL LIST - CATEGORY 5 PART 2 LR
UNITED STATES - GOVERNMENT CONFIGURATION BASELINE (USGCB) RMG
UNIXITRIX EXPLOIT MAT
UNIVERSAL DECOMPOSABILITY C
UNIVERSAL DESCRIPTION DISCOVERY AND INTEGRATION (UDDI) WAM
UNIVERSAL FORGERY C
UNIVERSAL SERIAL BUS (USB) HS
UNIVERSAL VERIFIABILITY POR
UNIVERSALITY PLT
UNKNOWN KEY SHARE SECURITY C
UNLOCK PATTERNS WAM
UNSTRUCTURED P2P PROTOCOLS DSS
UNSUPERVISED TECHNIQUES SOIM
UNTRAPPED ERRORS SS
UPDATE ROUTINES MAT
UPTIME SOIM
URL HISTORY F
US NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION SSL
US SPY CAR ACT SSL
US-CERT (UNITED STATES COMPUTER EMERGENCY READINESS TEAM) LR
USABLE SECURITY HF
USAGE CONTROL AAA
USE APPROVED TOOLS SSL
USE CONTINUOUS LEARNING AND MONITORING SSL
USE OF RFID TAGS SSL
USE SOFTWARE COMPOSITION ANALYSIS AND GOVERNANCE SSL
USE THE MANUFACTURER USAGE DESCRIPTION SSL
USE TOOLS AND AUTOMATION SSL
USER - ACCESS MANAGEMENT AAA
USER - CHOICE HF
USER - DATAGRAM PROTOCOL (UDP) NS
USER - MODE HS
USER - PROVISIONING SOIM
USER - TRUST HF
USER ACCEPTANCE TESTING (UAT) SSL
USER AUTHENTICATION AAA
USER AUTHORIZATION TABLES AAA
USER DATAGRAM PROTOCOL (UDP) NS
USER MODE OSV
USER PROVISIONING SOIM
USER REPRESENTATIVE RESPONSIBILITIES OF RMG
USER UPLOADED FILES WAM
USER-MODE ROOTKITS MAT
USERS - AUTHORIZED AAA
USERS - INCIDENT RESPONSE AND SOIM
USERS - INSIDER THREATS AB
USERS - TRAINING HF
USERS - UNAUTHORIZED AAA

V

VALIDATION SOIM
VALIDATION - CONTROLS SOIM
VALIDATION - PARAMETER VALIDATION SS
VALIDATION - VULNERABILITIES AND SS
VALIDITY DSS
VALIDITY CHECK SS
VALUABLE PAPERS AND RECORDS (INSURANCE COVERAGE) SOIM
VALUE AT RISK (VAR) RMG
VALUE BASED DSS
VALUE DELIVERY - AS OUTCOME OF SECURITY PROGRAMS SOIM
VALUE DELIVERY - AS RESULT OF INFORMATION SECURITY GOVERNANCE RMG
VAR (VALUE AT RISK) RMG
VASCULAR PATTERNS AAA
VECTORS MALCODE MAT
VELOCITY SOIM

WEB-BASED ATTACKS - STATIC FILE ANALYSIS - PE FILES MAT
 WEB-BASED ATTACKS - STATIC FILE ANALYSIS - SOFTWARE PACKERS AND MAT
 WEB-BASED ATTACKS - STATIC FILE ANALYSIS - STRING ANALYSIS MAT
 WEB-BASED ATTACKS - VIRTUALIZED ENVIRONMENTS TESTING MAT
 WEB-BASED ATTACKS - WINDOWS REGISTRY INSPECTION SOIM
 WEB-BASED ATTACKS - XSS (CROSS-SITE SCRIPTING) SS
 WEB-BASED ATTACKS - ZERO-DAY EXPLOITS WAM
 WEB-BASED EDI NS
 WEBASSEMBLY (WASM) WAM
 WEBAUTHN WAM
 WEBFICATION WAM
 WEBTRUST RMG
 WEBVIEWS WAM
 WEP NS
 WEP (WIRED EQUIVALENT PRIVACY PROTOCOL) NS
 WEP (WIRED EQUIVALENT PRIVACY PROTOCOL) - VULNERABILITY NS
 WESTERN UNION AND UNTRACEABLE PAYMENTS AB
 WHITE BOX TESTING SOIM
 WHITE WASHING DSS
 WHITE-BOX FUZZING SS
 WHITELISTING WAM
 WHOIS WAM MAT
 WI-FI NS
 WI-FI PROTECTED - ACCESS (WPA) NS
 WI-FI PROTECTED - ACCESS 2 (WPA2) NS
 WI-FI PROTECTED ACCESS (WPA) NS
 WI-FI PROTECTED ACCESS 2 (WPA2) NS
 WIDE AREA NETWORK (WAN) NS
 WIMAX NS
 WINDOWS LIVE PHOTO GALLERY FACE RECOGNITION AND POR
 WINDOWS ROOTKIT MAT
 WIPS/WIDS (WIRELESS INTRUSION PROTECTION/ WIRELESS INTRUSION DETECTION SYSTEMS) NS
 WIRED EQUIVALENT PRIVACY (WEP) NS
 WIRED EQUIVALENT PRIVACY PROTOCOL (WEP) NS
 WIRELESS NS CPS
 WIRELESS - BLUETOOTH NS
 WIRELESS - CONNECTION NS
 WIRELESS - LOCAL AREA NETWORK (WLAN) NS
 WIRELESS - NETWORKS NS
 WIRELESS - NETWORKS - CELLULAR NETWORK NS
 WIRELESS - NETWORKS - DIRECT-SEQUENCE SPREAD SPECTRUM (DSSS) NS
 WIRELESS - NETWORKS - FREQUENCY DIVISION MULTIPLE ACCESS (FDMA) NS
 WIRELESS - NETWORKS - FREQUENCY-HOPPING SPREAD SPECTRUM (FHSS) NS
 WIRELESS - NETWORKS - LAN NS
 WIRELESS - NETWORKS - MAN NS
 WIRELESS - NETWORKS - MESH NETWORK NS
 WIRELESS - NETWORKS - MULTIPLEXING (OFDM) NS
 WIRELESS - NETWORKS - PAN NS
 WIRELESS - NETWORKS - SPREAD SPECTRUM NS
 WIRELESS - NETWORKS - TIME DIVISION MULTIPLE ACCESS (TDMA) NS
 WIRELESS - NETWORKS - WAN NS
 WIRELESS - PERSONAL AREA NETWORK (WPAN) NS
 WIRELESS - WIMAX NS
 WIRELESS ACCESS POINTS NS
 WIRELESS LAN SECURITY NS
 WIRELESS LOCAL AREA NETWORK (WLAN) NS
 WIRELESS NETWORKING - CELLULAR NETWORKS PLT
 WIRELESS NETWORKING - SECURITY ISSUES - AD-HOC MODE NS
 WIRELESS NETWORKING - SECURITY ISSUES - INFRASTRUCTURE MODE NS
 WIRELESS NETWORKING - SECURITY ISSUES - OSA AAA
 WIRELESS NETWORKING - SECURITY ISSUES - PARKING LOT ATTACK AB
 WIRELESS NETWORKING - SECURITY ISSUES - SHARED KEY AUTHENTICATION AAA
 WIRELESS NETWORKING - SECURITY ISSUES - SKA NS
 WIRELESS NETWORKING - SECURITY ISSUES - SSID FLAW NS
 WIRELESS NETWORKING - SECURITY ISSUES - TKIP ATTACK NS
 WIRELESS NETWORKING - SECURITY ISSUES - WEP NS
 WIRELESS NETWORKING - SECURITY ISSUES - WEP VULNERABILITY NS
 WIRELESS NETWORKING - SECURITY ISSUES - WPA/WPA2 NS
 WIRELESS NETWORKING - TESTING SOIM
 WIRELESS NETWORKING - WIMAX NS
 WIRELESS PERSONAL AREA NETWORK (WPAN) NS
 WIRELESS SENSOR NETWORKS DSS
 WIRELESS SHIELD CPS
 WIRELESS WIDE AREA NETWORK (WWAN) NS
 WIRETAPPING PLT
 WORK FACTOR CI
 WORK FACTOR ENCRYPTION C
 WORK PLAN RMG
 WORK PLAN - EXAMPLE FOR SECURITY PLAN DEVELOPMENT SOIM
 WORKAROUNDS TO SECURITY MECHANISMS HF
 WORKFLOWS AND VOCABULARY SOIM
 WORKING F
 WORKLOAD HF
 WORKLOAD MEASUREMENT HF
 WORM MAT
 WORMHOLE ATTACK NS
 WORMHOLE ATTACKS PLT
 WORMS MAT
 WPA NS
 WPA/WPA2 (WI-FI PROTECTED ACCESS) NS
 WPA2 NS
 WPA3 NS
 WRITE ATTRIBUTES PERMISSION OSV
 WRITE EXTENDED ATTRIBUTES PERMISSION OSV
 WRITE XOR EXECUTE OSV
 WRITE-ONCE, READ-MANY AAA

X

X-KISS (XML KEY INFORMATION SERVICE SPECIFICATION) C
 X-KRSS (XML KEY REGISTRATION SERVICE SPECIFICATION) C
 X.25 NS
 X.400 AAA
 XACML 3.0 AAA
 XDAS[CADF] SOIM
 XEN OSV
 XKMS (XML KEY MANAGEMENT SPECIFICATION) C
 XMAS SCANNING NS
 XOR (EXCLUSIVE-OR) C
 XSS (CROSS-SITE SCRIPTING) ATTACKS SS

Y

YARA SOIM

Z

ZACHMAN FRAMEWORK RMG
 ZERO KNOWLEDGE PROOF C
 ZERO TCB IMPLEMENTATIONS HS
 ZERO-DAY EXPLOITS SS
 ZERO-DAY/ZERO-HOUR MAT
 ZERO-FORCING PLT
 ZERO-KNOWLEDGE C
 ZERO-KNOWLEDGE PROOFS POR
 ZERO-KNOWLEDGE-BASED PROTOCOLS C
 ZK-SNARK POR
 ZONE INFORMATION PROTOCOL (ZIP) NS
 ZONES DNS NS