CISSP Skillset

General Skillset

Access Controls	understanding of the various types of access control methodologies and when each is appropriate.
Business Continuity and Disaster Recovery Planning	understanding of the importance of continuity planning and how to develop disaster recovery and continuity plans.
Cryptography	understanding of the role cryptography and cryptosystems play in securing the enterprise environment.
Information Security Governance and Risk Management	an understanding of the critical components of information security and risk that are needed in order to manage security in an enterprise environment.
Law, Regulations, Compliance and Investigations	understanding of the roles played by laws and ethical standards and handling incident investigations.
Physical and Environmental Security	understanding of the importance of physical and environmental security in an enterprise environment.
Security Architecture and Design	understanding of how to properly design and implement a secure enterprise environment.
Security Operations	understanding of the managerial, administrative, operational aspects of information security.
Software Development Security	understanding of the key security principles related to secure application development.
Telecommunications and Network Security	discuss major concepts associated with network defense and telecommunications security.

Domain I Overview

Domain 1 - Information security governance and risk management	
Concept	goals, mission and objectives of the organization
	budget
	metrics
	resources

	security governance
	information security strategies
Security policies and procedures	standards | baselines
	guidelines
	documentation
data classification	
security awareness training	evaluate personnel security
	background checks and employment candidate screening
	employment agreements and policies
	employee termination processes
	certification and accreditation efforts
	ensure security in contractual agreements and procurement processes
	ethics
risk management concepts	identify threats and vulnerabilities
	risk assessment and analysis
	risk assignment and acceptance
	countermeasure selection
	assess the completeness and effectiveness of the security program

Domain I detail

	General Skills	Skills	Details Skills	Tools
Domain 1	**Information Security Governance and Risk Management**			
	expectation	identification and securing organization information assets		
		personnel security		
		managerial security policies		
		security awareness training		
		data classification		

		CIA of information on systems		
		risk management		
		security best practices		
		BCP | DRP developmental understanding		
	concept and terminology	confidentiality		
		integrity		
		availability		
		identification		
		accountability		
		authorization		
		privacy		
		authentication	something you have	token
				smart card
				badge
			something you are	biometrics
			something you know	
			something you are	GPS
		biometrics	crossover error rate (CER)	
			false rejection rate	
			false acceptance rate	
	DATA CLASSIFICATION			
	data classification	top secret		
		secret		
		confidential		
		sensitive but unclassified (SBU)		
		unclassified		
		public		
		official use only		
		internal use only		
		company proprietary		
	data classification criteria	value		

		age		
		useful life		
		personal association		
	data classification process		identify the admin | custodian	
			specify the criteria for how the info will be classified and labeled	
			classify the data by its owner who is subject to review by a supervisor	
			specify and document exceptions to the classification policy	
			specify and control that will be applied to each classification level	
			specify the termination procedures for declassifying the information or for transferring custody of the information to another entity	
			create an enterprise awareness program about the classification	
	distribution of classified information	court order	FOIA	
		government contracts		
		senior-level approval	NDA	
	data classification role	data owner	executive | manager of an organization	
			final corporate responsibility of data protection	
		custodian	running regular backups and routine	
			perform data restoration from the backup	
			maintaining those retained records in accordance with the established information classification policy	
		application owner		
		manager		
		user		

		administrator		
		analyst		
		auditor		
	data classification responsibility		establishment of an organization's computer security programs and goals	
			priorities to support the mission of the organization	
	rotation of duties	person responsible should be changed on a regular basis		
		prevent someone from becoming "comfortable" in a position		
		helps to detect and minimize fraud		
		reduce collusion when used with separation of duties		
	POLICY			
	Policy	senior management directives	create a computer security program	
			establish the goals of the program	
			assign responsibilities	
			consistent with other existing directives, laws and missions	
			Integrated with organizational policies.	
	Define a policy	program policy		
		issue-specific policy		
		system-specific policy		
	Content of a Policy	purpose	explain the reason for the policy	
		related document	list any documents that affect the contents	
		cancellation	identify existing policy that is cancelled when this policy becomes effective	
		background	provide info on the need for the policy	
		scope	state the range of coverage for the policy	
		policy statement	identify the actual guiding principle	
		action	specifies what action are necessary	
			when they are to be accomplished	
		responsibility	identify who is responsible for what	

		ownership	identify who sponsored the policy	
			identify who can change the policy	
			identify whom it derive its authority	
	levels of policy	enterprise-wide | corporate policy		
		division-wide policy		
		local policy		
		issue-specific policy		
		procedures and checklists		
	checkpoint: procedure guidance	policy worksheet		
	PROCEDURE			
	definition and issues	organizational		
		specified uniform use of specific technologies or parameters		
		compulsory		
		usually refers to specific hardware and software		
	BASELINE			
	definition and issues	specific implementation of a standard		
	GUIDELINE			
	definition and issues	suggestions	assist users, system personnel	
			ensure that specific security measures are not overlooked	
			applies to security measures that might be implemented in more than one way	
	DOCUMENTATION	Policy		
		Standard		
		baseline		
		procedure		
		guidelines		
	SECURITY CONTROLs			
	Objective		determine the impact a threat may have and the likelihood that the threat can occur	
	Goal	lower the probability of an adverse occur		

	Defining Risk	Risk		
		Threat	define business goal	
			validated data	
			industry best practice	
		Vulnerability	define vulnerability	
	Threat Model	Threat	outsider attack from network	
			outsider attack from telephone	
			insider attack from local network	
			insider attack from local system	
			attack from malicious code	
		Vulnerability		
		compromise		
	risk assessment method	qualitative		
		quantitative		
		knowledge-based		
		best practices		
	risk choices	acceptance		
		mitigation		
		transference		
	risk management : key formulas	exposure factor (EF)		
		single loss expectancy (SLE)		
		annualized rate of occurrence (ARO)		
		annualized loss expectancy (ALE)		
		risk requires uncertainty		
		risk management questions	what could happen?	
			the impact of the threat	
			the frequency of the threat	
			the recognition of uncertainty	
	Risk management	identify		
		assess	physical damage	
			human error	
			malfunction	

			attacks	
			data misuse	
			data loss	
			application error	
	risk management process		asset identification	
			threat analysis	
			vulnerability analysis	
			preliminary risk evaluation	
			interim report	
			risk acceptance criteria	
			risk mitigation measures	
			ROI analysis	
			final report	
			operation and maintenance	
	SLE	asset value		
		exposure factor	define % (from 0% to 100%)	
	ALE		identify the frequency with which the threat is expected to occur	
	ARO		how often does this problem occur?	
			how does this relate to the overall risk	
	TCO		what is the total cost of maintaining a security device?	
			includes installation maintenance and hidden costs	
	Controlling your environment	policy	tell user what to do	
		training	provides the skillset	
		awareness	change user behavior	
		key threat	social engineering	
	SECURITY AWARENESS			
	Solution	live, interactive presentation		
		publishing distribution		
		incentives		

		reminders		
	Security training	implementation		
		targets an audience		
		motivates management and employees		
		maintains programs		
		evaluates program		
		training for specific groups or department		
	Outsourcing	monitoring		
		coding		
		offshoring		
	Service Level agreement	contractual arrangement		
	ETHICS			
	Ethics bodies	internet activities board IAB	Not to do list	
		computer ethic institute	ten commandments	
		association for computing machinery		
		Australian computer society		
		IEEE		
		ISACA		
		ISC^2	protect society, the commonwealth and the infrastructure	
			understanding and acceptance of prudent information security measures	
			preserve and strengthen the integrity of the public infrastructure	
			discourage unsafe practice	
			act honorably, honestly, justly and legally	
			provides diligent and competent service to principals	
			advance and protect the profession	
	Ethical Standards	software piracy		
		data security		
		individual privacy		
		data integrity		

		human | product safety		
		fairness, honesty and loyalty		
	Ethical dilemma			
	Assessing security posture	completeness		
		effectiveness		

Domain 2 general

Domain 2: Access Controls	
Agenda	systems and methodologies
	terms and principles
	model
	measures
	identity, authentication, and authorization
	techniques
	protocols
	passwords and cracking
Expectations	describe concepts and methodologies
	identify security tools and technologies
	describe auditing mechanisms of information system

Domain 2 detail

	Skills	Skills	Details Skills	Tools
Domain 2	**Access Control**			
	AC System and methodology		**who are the individual**	
			what are your resources?	
		confidentiality		
		integrity		
		availability		
		reducing risk	identify risk	
	organizational control	centralized control		
		decentralized control	controls map to individual business units	

	controlling access	least privilege	need to know	
		separation of duties	static | dynamic	
	AC MODEL		collusion	
	Terminology	subjects: active	identify user, process or device, active entity	
		objects: passive	identify files, directories, pipes, devices	
			sockets, ports.	
		rules: filters	each rule a security attribute	
			Unix: read | write | execute	
			Windows : Read | write | execute | no access	
		labels: sensitivity		
		interaction	what are the business rules?	
			how will be business rules be enforced?	
	Mandatory AC			
	Define	security label		
		data classification		
		entity	define users	
			define objects	
		access level		
	Strength	controlled by the system		
		not be overridden		
		no subject to user error	enforces strict controls on multi-security systems	
			prevent information leakage	
	Weaknesses	trused users | admin		
		proper levels		
		proper physical security		
	Discretionary AC			
	Define	access control lists		
		tabular listing		
		user-directed-user specifies with limitations		
		identity-based-based only on ID of subjects and objects		
		hybrid-combination of ID-based and user-directed		
		access control triple	program	
			user or subject	

			file of object	
	Strength	convenient		
		flexibility		
		ownership concept		
		simple to understand		
		software personification		
	Weaknesses	fail to recognize the differences between users and programs		
	AC MODELS			
	Models	Role-based access control	Non-RBAC	
			Limited RBAC	
			Hybrid RBAC	
			Full RBAC	
		rule set based access control		
		list-based access control		
		access control matrix ACM		
	New implementation	Content-dependent access control		
		constrained user interface		
		capability tables		
		temporal (time-based) isolation		
	AC MEASURE			
	Types of controls	preventive	firewall	
			packet filtering	
			stateful	
			proxy	
		detective	IDS	
			pattern matching	
			anomaly detection	
		corrective		
		physical	security laptops	locks
			security magnetic media	
			protection of cable	
	Control combination	preventive | administrative		
		preventive | technical		

		preventive | physical		
		detective | technical		
		detective | physical		
	Implemented across	administrative	background checks	
			policies and procedures	
		technical	encryption	
			smart cards	
	MONITOR			
	Step	review		
		watch		
		take action		
	Methods	real-time		
		adhoc	vulnerability checkers	
			file integrity	
			network sniffers	
			log consolidation tools	
		passsive		
		auditing	monitoring and looking for change	
	Types	keystroke		hardware
				software monitoring
		illegal software		
		traffic analysis		
		trend analysis		
	Analysis	establish clipping levels	baseline or user activity	
	Auditing	compliance checks		
		internal and external		
		frequency of review		
		standard of due care		
	CONTROL CATEGORIES			
	Control	Deterrent		
		compensating		
		corrective		

		recovery		
	Control combination	preventive | administrative	organizational policies and procedures	
			pre-employment background checks	
			employee agreements	
			employee termination procedures	
			vacation scheduling	
			labeling of sensitive materials	
			security awareness training	
			evaluate personnel security	
			vendor, consultant and contractor controls	
		Preventative technical (logical)	protocols	
			encryption	
			smart cards	
			biometrics for authentication	
			constrained user interface	
			database views	
		Preventive | physical	environment control systems	fences
			temperature	mantrap
			humidity	magnetic card
				biometrics
				guards
		Detective | technical	IDS	
			violation reports from audit trail information	
		Detective | physical	motion detectors	
			thermal detectors	
			video cameras	
	IDS			
	IDS goals	creation and maintenance of IDS and process		
		creation of CIRT	analysis of an event	
			respond to an incident if the analysis warrants	
			escalation path procedures resolution	
			post-incident follow up	
			report to appropriate parties	

	Types	Network based	passive	
			active	
		host based		
	Method of operation	pattern matching	signature detection	
		anomaly detection		
		protocol behavior		
	IDS events defined	true positive		
		true negative		
		false positive		
		false negative		
	IDENTITY			
	AA	authentication	something you know	
			something you have	
			something you are	
			some place you are (new)	
		authorization		
	Identity		identify who someone is	
		positive identification		
		negative identification		
		issuing of identity		
		naming standards		
		non-descriptive		
		tracking and auditing		
		unique		
		not shared		
	BIOMETRICs			
	Access control	fingerprint		
		palm scan		
		hand geometry		
		voice print		
		retina pattern		
		iris scan		
		facial recognition		

		keystroke dynamics		
		signature dynamics		
	Requirements	resistance to counterfeiting		
		data storage requirements		
		acceptability to users	privacy	
			invasiveness	
			psychological comfort	
			physical comfort	
		reliability and accuracy	practical consideration	
	performance	false reject rate Type I error		
		false accept rate FAR type II error		
		crossover error rate CER		
		enrollment		
	PASSWORDs			
	PASSWORDs	static password	user picked	
			system generated	
		dynamic password	one time	
		account lockout		
		length range	passphrase	
			lifetime	
	password cracking	dictionary attack		
		hydrid attack		
		brute force attack		rainbow Crack
	TOKEN			
		smart cards	contact	
			contactless	
		one time passwords OTP	counter based	
			time based	
	smart cards	static password tokens		
		synchronous dynamic password tokens		
		asynchronous dynamic password token		

		challenge response token		
	SINGLE SIGN-ON			
	Methods	host to host authentication		
		authentication servers		
		user-to-host authentication		
	Kerberos	Kerberos SSO		
		Kerberos operation	KDC	
			session key	
			ticket granting ticket TGT	
		vulnerabilities		
	SEASAME	symmetric and asymmetric encryption		
	network vulnerability scanner			
	vulnerability assessment VA		scanning key servers looking for a set of vuln	vul scanning tool s
	penetration testing	war dialing		
		sniffing		
		eavesdropping		
		radiation monitoring		
		dumpster diving		
		social engineering		
	security assessment		complete list of risks against critical assets	
	THREATS			
	Threat	malicious code	virus	
			worms	
			logic bombs	
			trojan horses	
			trap doors	
		DOS		Smurf
		cramming	buffer overflow	overflow condition
				exploit on memory stack

				overwrite return pointer
				set return pointer to exploit code
		spamming		
		flooding	DDoS	SYN Flood
		brute force attack		
		remote maintenance		
		TOC | TOU		
		interrupts	fault line attack	
		code alteration	rootkits	file level
				kernel level
		inference	traffic analysis	
		covert channels	timing channel	
			network bandwidth utilization	
			storage channel	
			hard drive storage	
	MiTM	masquerading		
		replay attack		
		spoofing	impersonation	
			active threat	
	remote maintenance	backdoor		
		default passwords		
	emanations	information leaving a system		
		protected with TEMPEST		
		similar to virtual shoulder surfing		
	browsing	data mining		
	dumpster diving	defeat with shredding		
	traffic analysis	passive threat		
	shoulder surfing			
	object reuse	allocation or reallocation of system resources to another subject		

	data remanence	data released by another process allowing for its recovery		
	social engineering			
	threat to AC	user distrust of biometrics		
		misuse of privilege		
		poor administration knowledge		

Domain 3 General

Domain 3 - Cryptography	
Agenda	basic cryptographic concepts
	application of public and private key algorithms
	key distribution and management
	methods of attack
	digital signatures
Expectations	fully understand
	algorithm construction, distribution, key management
	methods of attack

Domain 3 Detail

	Skills	Skills	Details Skills	Tools
Domain 3	**Cryptography**			
	TERMS			
	Cryptography	cryptography		
		cryptology		
		codes		
		cryptanalysis		
		cryptographic algorithm		
		block cipher		
		cipher		
		cipher text or cryptogram		
		clustering		

		plaintext		
		cryptosystem		
		exclusive OR		
		one time Pad		
		work function		
	History	secret writing		
		spartan scytable		
		caesar sipher		
		UNIX ROT 13		
		polyalphabetic cipher		
		battista cipher disk		
		cryptanalysis		
		jeffersib disk		
		stafford		
		enigma		
		hebern machines		
		japanese red and purpose machines		
		american sigaba		
		vernam cipher		
		book or running key cipher		
	Import and export issues	COCOM		
		Wassenaar arrangement		
		european union controls		
		united state controls		
	Goals	confidentiality		
		authentication		
		data integrity		
		non-reputation		
	Encryption techniques	substitution	arbitrary	
			rotation	
		permutation		
		hybrid		
	Cryptosystems	symmetric	secret keys	

			single or one-key encryption	
		asymmetric	public key	
			dual or two key encryption	
			multiplication vs factorization	
			exponentiation vs logarithms	
		hash	one way transformation	
			no key encryption	
			HMAC	
			MD2	
			MD4	
			MD5	
			SHA	
			SHS	
	Kerberos	secret-key protocol		
		distributed service for 3rd party authentication		
		confidentiality	DES CBC mode	
		integrity		
		authentication		
		non-reputation		
		Kerberos operations		
	data encryption standard DES	Mode	ECB	
			CBC	
			CFB	
			OFB	
			CTR	
		Weakness	MiTM attack 2DES	
		2DES		
		3DES		
	advanced encryption standard	AES	MARS	
			RC6	
			Rijndael	
			Serpent	

			2fish	
		basic functions	Addroundkey	
			SubBytes	
			ShiftRows	
			Mixcolumns	
		IDEA		
		SAFER		
		Blowfish		
		twofish		
		RC5		
	asymetric encryption	el gamel encryption and signature schemes		
		diffie hellman key agreement scheme		
		Schnorr signature scheme		
		NIST's digital signature algorithm DSA		
		Elliptic curve El Gamal encryption and signature schemes		
	elliptic curve cryptosystem			
	diffie-hellman			
	digital signatures	implementation		
	hash functions and MD			
	integrity control	checksums		
		hashing		
		digest algorithm		
		Haval		
		RIPEMD-160		
		MAC		
	public key electronic signatures			
	crypto attack	brute force		
		MiTM		
		Known plaintext		
		ciphertext only		
		chosen plaintext		

		adaptive chosen plaintext		
		chosen key attack		
	cryptographic attack cryptanalysis	analytic		
		statistical		
		differential		
		linear		
		differential linear		
		birthday attack		
	PKI	components	certification authorities CA	
			organizational registration authorities ORA	
			certificate holder	
			clients	
			repositories	
		include	digital certificates	
			certificate authority	
			registration authorities	
			policies and procedures	
			certification revocation	
			non-repudiation support	
			cross certification	
	Escrowed encryption	define		
		components		
		fair cryptosystems		
	key management	protection	against modification	
			against unauthorized disclosure	
		procedures	key generation	
			distribution	
			storage	
			entry	
			use	
			recovery	
			destruction	

			archiving	
			key notarization	
		issue	key recovery	
			key storage	
			key retirement | destruction	
			key change	
			key generation	
			key theft	
			frequency of key use	
	PGP	confidentiality	CAST	
			IDEA	
			3DES	
		integrity	MD5	
		authentication	private key	
		non-repudiation	digital signature	
	IPSec	AH		
		ESP		
		SA		
	Steganography	data hiding		
		how steganography works		
		types	injection	
			substitution	
			generate new file	

Domain 4 General

Domain 4	**Physical Security**
Objectives	personnel safety
	authorized access
	equipment protection
	information protection
	availability
expectations	understand types of threats and sources

	internal and perimeter defenses
	environmental controls
	procedures and weak physical security measures

Domain 4 Detail

	Skills	Details Skills	Misc
Domain 4	**Physical Security**		
	Types of System		
		Static systems	
		mobile systems	
		portable systems	
	Counter examples		
		authentication	password
			two factor
		encryption	disk encryption
		redundancy	local system backup
	Access control types	deterrent	weapon
		detective	CCTV
		preventive	locks
	Administrative control		
	personnel controls		
		personnel screening prior to employment	
		prior employment	
		references	
		education	
		criminal record	
		general background checks	
	employee checks		
		security clearances	
		performance rating	
		supervision	

	post-employment procedures		
		exit interviews	
		termination of computer accounts	
		change of passwords	
		return of laptop	
	safety		
	impact	personnel safety	
		authorized access	
		equipment protection	
		information protection	
		availability	
	evacuation		
	procedures	evacuation routes	
		meeting point	
		posting	
		practice	
	roles	safety warden	
		meeting point leader	
		employee	
	Threat		
		smoke and fire	
		toxins	
		water | flood	
		temperature extremes	
		structural failure	
		power failure	
		human actions	
		intentional or unintentional	
		fire and related contaminants	
		explosions	
		loss of utilities	
		toxic materials	
		earthquakes	

		weather	
		malicious acts	
		sabotage	
		strike	
	source of physical loss		
		temperature	extreme variations
		gases	war gases
			commercial vapors
			humidity
			dry air
			suspended particles
		liquids	water
			chemicals
		organisms	viruses
			bacteria
			people
			animals
			insects
		projectiles	tangible objects
		movement	collapse
			shearing
			shaking
			vibration
			liquefaction
			flows
			waves
			separation
			slides
		energy anomalies	electric surges
			failures
			magnetism
			static electricity
			aging circuitry

			radiation
			sound
		l	light
			radio
			microwave
			electromagnetic
			atomic waves
	smoker and fire		
	detective	smoke detectors	light beam with optical sensor
			change in ionization
		heat sensors	detect room temp
		flame detector	sense the pulsation of the flame
			sense the IR energy produced by the flame
	suppressive	sprinklers	chemical | H20
		fire extinguishers	ABC | halon
	evacuation		
	Fire classes	A common combustibles	wood product
		B liquid	
		C electrical	
		D combustible	metals
	suppression method		
	Methods	CO2 and soda acid	remove fuel and O2
		water	reduce temp
		gases	interfere with chemical reaction
	Types	zones of coverage	
		time-release	
		HVAC off before activation	
		wet pipe	
		dry pipe	

		pre-action	
		deluge	
		gas discharge	
		portable extinguisher	
		other consideration	inspected quarterly
		halon	
	Floods (water)		
	detective	detectors	moisture
			humidity
		3rd party	news
			emergency
			warning system
	corrective	bilge pumps	
		evacuation	
	earthquakes		
	detective	structural assessment	
		sudden impact	
	corrective	structural reinforcement	
		evacuation	
	restricted area		
	definition	restricted visitor	
		non-restricted visitor	
		motion detector to sense activity	
		escort from restricted area	employee
			guard
		perimeter of restricted area	space
			time
	Deterring unauthorized access		
	educate	employees only sign	
	discourage	uniformed pseudo-guards	
		unauthorized personnel will be prosecuted	
	lock		

	type	ward	
		wafer or disc	
		pin tumbler	
		replacement core	
		cipherlock	
		combination lock	
		smart card	
		smart code with passcode	
		biometric	
	locker components	body	
		strike	
		cylinders	low
			medium
			high
		key	
		master lock	
	Analyzed factor	construction and mechanism	
		range of possible key and uniqueness	
		association with individual	
		copying	
		distribution	
		initial cost and re-keying cost	
	Mantrap	physical control	
		entrance path protected by 2 doors	
		intruder confined between doors	
	CCTV		
	Cameras CCTV level	detection	
		recognition	
		identification	
	primary components	camera	
		transmission media	
		monitor	

	secondary components	pan and tilt units	
		recorders, controls	
		multiplexing, mountings	
		panning devices	
		infrared device	
	types	cathode ray tube CRT	
		charge coupled discharge CCD	
	camera lens	fixed, zoom	
	key design factor	field of view	
		depth of field	
		illumination range	
		lighting	
	Contraband checks		
	component	X-ray scanner	
		metal detectors	
		bag inspection	
	computer lock down		
	Asset	server	
		workstation	
		laptop	
	Protection mechanism	port controls	
		PC locking devices	
		switch controls	
	Intruder detection		
	manual	security lights	
		watch tower	
		dog patrols	
	automatic	motion detector	
		heat | infrared sensor	
	facility control	fences	
		landscapes	
		vehicle barriers	
		guards	

		dogs	
		badges	
		lights	
		motion detectors	
		sensors	
		alarms	
		security guard	
	gates	class I - residential gate	
		class II - commercial gate	
		class III - industrial gate	
		class IV - restricted access	prison
			airport
	security guards	availability	
		reliability	
		training	
		cost	
	badges	photo image	dumb card
		digitally encoded	smart card
	lights		
	outside lighting	floodlights	
		streetlights	
		Fresnel lenses	
		gaseous discharge	
		continuous lighting	
		trip lighting	
		standby lighting	
		emergency lighting	
	consideration		
	motion detector		
	technologies	photometric system	
		motion detection system	sonic
			ultrasonic
			microwave

		acoustical seismic detection system	microphone type device
		proximity	
	site selection consideration	visibility	neighbors
			external markings
		local consideration	near hazards
			crime rate
		natural disasters	earthquake fault
			weather related
		transportation	excessive air, highway
		joint tenancy	access to environment
			HVAC controls shared
		external services	proximity of fire
			police
			hospital
	facility design		
	IS IT construction standard	light frame	
		heavy frame	
		fire rated	
	floor slab	loading	
		fire rating	
	raised flooring	grounded	
		nonconductor surface	
	walls	floor slab to ceiling stab	
		fire rating	
		adjacencies/exterior	
		paper | record | tape storage	
	enclosed areas	floor	
		wall	
		ceiling	
	door	interior | exterior	
		directional opening	
		forcible entry	
		fire rating equal to walls	

		emergency egress	
		monitored and alarmed	
		emergency exit	
		hollow and solid core	
		panic bars	
	windows	laminated glass	
		wired glass	
		solar window film	
		security film	
		glass breakage	
		bullet proof	
		explosive resistant	
	HVAC	water | steam | gas lines	
		shut-off values	
		positive drains	
		dedicated | controllable	
		independent power	
		positive pressure	
		protected air intakes	
		environmental monitoring	
	temperature and humidity		
	static charge voltage damage		
	air quality		
	electrical power		
		EMI	
		RFI	
	Protection mechanism	shielding	
		proper grounding	
		conditioning of power lines	
		care in routing of cables	
	definition	fault	
		brownout	
		blackout	

		spike	
		sag	
		surge	
		transient	
	object reuse		
	media storage	paper printouts	
		data backup tapes	
		CDs	
		diskettes	
		hard drives	
		flash drives	

Domain 5 General

Domain 5	**Security architecture and design**
Overview	hardware
	firmware
	trusted computing base
	assurance models
Expectations	identify physical components
	various software use relationship
	enterprise segin architecture principles
	security models and theory
	evaluation method and criteria
	certification and accreditation

Domain 5 Detail

Domain 5	**Skills**	**Skills**	**Skills**	**Tools**
	design architecture	diskless workstation		
		thin clients		
		thin processing		
	OS	memory management		

		process management		
		file management		
		I/O management		
	OS State	user		
		privileged		
	OS protection	layering		
		abstraction		
		process isolation		
		hardware segmentation		
	Ring layer protection	ring 3: applications and programs		
		ring 2: I/O drivers and utilities		
		ring 1: OS components that are not part of the kernel		
		ring 0: OS kernel		
	programming languages	machine		
		assembly	assembler	
			disassmebler	
			compiler	
			interpreter	
		high level		
	database	data definition language		
		data manipulation language		
	PDAs	technologies	java based	
			PALM operating system	
			Win CE	
	computer architecture	the CPU	arithmetic /logic unit	
			control unit	
			primary storage memory unit	
		instruction cycle	fetch phase	
			execute phase	
		pipelining		
		complex instruction set computer CISC		

		reduced-instruction set computer RISC		
		interrupt	CPU execution	
		scalar processor		
		superscalar processor		
		multitasking		
		multiprocessing		
		multithreading		
		multiprogramming		
		memory	cache	
			RAM	DRAM
				SRAM
			ROM	firmware
				PROM
				EPROM
				EEPROM
				PLD
			secondary memory	
			sequential memory	
			virtual memory	locked memory
		memory addressing	memory isolation	
			TOC | TOU protection	
			direct addressing	
			absolute addressing	
			register direct addressing	
			register indirect addressing	
	storage devices	primary		
		secondary		
		virtual		
		Write once read memory WORM		
		volatile		
		non-volatile		
	trusted computing base	access control mechanisms		
		reference monitor		

		kernel		
		protective mechanisms		
		monitor	process activation	
			process execution domain switching	
			memory protection	
			I/O operation	
	security models	lattice		
		confidentiality: Bell-LaPadula	no read up	
			no write down	
		integrity: biba	no read down	
			no write up	
		commerical: clark wilson	constrained data item are consistent	
			transformational procedures act validly	
			duties are separated	
			accesses are logged	
			unconstrained data items are validated	
	state machine models			
	research model	noninterference		
		information flow		
	graham-denning model	create object		
		create subject		
		grant access right		
		read access right		
		delete object		
		delete subject		
		delete access right		
		transfer access right		
	harrison-ruzzo-ullman	add granular control		
	chinese wall model			
	enforcement	security kernel		
		reference monitor concept		

		reference monitor		
	domain separation	execution rings		
		base address registers		
		segmentation descriptors		
	TCSEC Classes			
	Orange book	4 classes	A: verified protected	
			B: mandatory protected	
			C: discretionary protected	
			D: minimal security	
		based on	security policy	
			object marking	
			subject identification	
			accountability	
			assurance	
			documentation	
	ITSEC classes	european		
		first common standard		
		main attributes	functionality	
			assurance	
		target of evaluation	TOE	
		functionality	F1	
			F5	
			F6	
			F7	
			F8	
			F9	
			F10	
		assurance	E0	
			E1	
			E2	
			E3	
			E4	
			E5	
			E6	

	evaluation assurance level EAL		EAL 1	
			EAL 2	
			EAL 3	
			EAL 4	
			EAL 5	
			EAL 6	
	ISO 17799	security policy		
		security organization		
		assets classification and control		
		personnel security		
		physical and environmental security		
		computer and network management		
		system access control		
		system development and maintenance		
		BCP		
		compliance		
		risk based		
		holistic approach		

Domain 6 General

Domain 6	**BCP and DRP**
Term	BCP
	BIA
	business resumption planning
	contingency plan
	COOP
	crisis communication plan
	critical systems
	critical business functions
	incident response plan
	DRP

Domain 6 Detail

Domain 6	Skills	Skills	Skills	Misc
	BCP			
	Business Continuity Planning (BCP)	Why?		
		key component	assess	
			evaluate	
			prepare	
			mitigate	
			respond	
			recover	
	Disaster Recovery Planning (DRP)	recovery of data center		
		recovery of business operations		
		recovery of business location		
		recovery of business processes		
	BCP phases	project initiation phase	define plan goal	
			define why the plan is important	
			provide a set of priorities	
			write a statement of organizational responsibilities	
			appoint project manager	good leadership skills
				understand business process and management
				experienced in IT and security management
				strong project management skills
			establish executive support	provide critical resources
				helps define and agree on the scope of project
				final approval of the BCP and its contents

			build the team	business unit managers
				IT and security staff
				human resources
				payroll
				physical plant manager
				office managers
			scope the project	what do you include in the plan?
				how do you collect information?
				what recourses are required?
				what is the continuity team's management structure
				top-down or bottom-up approach
			define objectives and deliverables	
			objective	create a BCP
			deliverables	risk analysis and impact
				disaster recovery steps
				plan for testing
				plan for training
				procedure to keep the plan up-to-date
		current state assessments	include a statement of urgency	
			include information on vital records	
			define an emergency response procedure	
			define emergency response guidelines	
		design and development phase		
		implementation phase		

		management phase		
	Process	identify assets		
		what threatens those assets		
		how can we protect and recover those assets		
		document the results		
		test and review		
		provide training and raise awareness		
	Risk analysis			
	Process	identify critical business system and processes		
		identify the specific threats		
		evaluate vuln of an asset and probability of an attack		
		determining protection mechanisms		
		calculate loss of assets vs cost of implementation		
	Types	risk avoidance		
		risk acceptance		
		risk transfer		
		risk reduction		
	BIA			
	Process	determine the tolerable impact levels your system can have		
		evaluate the effect of a disaster over a period of time		
	Assessment	business function priorities		
		timeframe for recovery	immediate recovery	
			quick recovery	
			same-day recovery	
			72 hours recovery	
			24 hours recovery	
			72+ hours recovery	

		resource requirements		
	maximum allowable downtime	total time for nonfunctioning before major financial impact		
		identify point of no return		
		derived from BIA		
		used to define resource requirement		
	risk analysis and reduction	vulnerability assessment		
	design and development phase			
	recovery strategies			
		use BIA		
		minimum requirements	determine space | equipment needs	
		start planning for continuity		
		no backup, no recovery		
		no strategy		
		self-service		
		reciprocal agreements		
		alternative sites	hot	
			warm	
			cold	
			hybrid	
			mobile	
	Disaster Recovery Plan			
	structure	introduction		
		emergency management team		
		emergency operation center		
		emergency notification procedure		
	no backup no recovery	frequency		
		availability		
		location		
		backup	not real time	
		mirroring	electronic vaulting	

			realtime backup of data	
	backup solution	electronic vaulting	batch process	
		remote journaling		
		database shadowing		
		disk duplexing		
	implementation phase	clear plan	short term	
			long term	
		testing and training strategies		
		enterprise crisis management plan		
	developing plan	introduction		
		crisis management structure		
		locations		
		procedures		
		exercise log		
		revision history		
	supporting information	purpose		
		applicability		
		scope		
		references | requirements		
		record of changes		
		concept of operations		
		system description		
		line of succession		
		responsibilities		
	notification | activation			
	recovery	execute temporary processing capabilities		
		repair or replace		
		return to original operational capabilities		
	reconstitution	return to permanent facility		
		test system		
		shutdown temporary facility		
	appendices	contact info		

		vendor contact info		
		standard operating procedures		
		checklists for system recovery or processes		
		detailed equipment and system requirement list of resources		
		vendor service level agreement		
		reciprocal agreements		
		alternative sites		
	type of testing	checklist		
		validate testing		
		simulation		
		active simulation		
		full interruption		
	Management Phase			
	Mistake	lack of BCP testing		
		limit scope		
		lack of prioritization		
		lack of plan updates		
		lack of plan ownership		
		lack of communication		
		lack of public relations planning		
		lack of security controls		
		inadequate insurance		
		inadequate evaluation of vendor suppliers		
	Threat	lack of management support		
		lack of business unit support		
		lack of change control		
		lack of funds		
		poor updates		
	Planning process lifecycle			
		project initiation phase		
		risk analysis		

		BIA		
		build the plan		
		test and validate the plan		
		modify and update the plan		
		approve and implemented the plan		

Domain 7: Telecommunication and Network Security

General:

Key components of network security
Intrusion detection
Firewalls
Packet filtering
Stateful
Proxy
Network vulnerability scanning
Penetration testing
Security assessment
Methods of attack
Types of networks
LANS
MANS
WANS
Topologies
Physical
Bus

Ring
star
Logical
Ethernet
Token ring
FDDI
WAN technologies
VoIP
Remote Access
Virtual applications
Screen scraping
Multi-media applications
Network hardware
Wiring
Routers bridges
Switches
Hubs

Numbering systems
Binary
Octal
Decimal
Hex
Protocol stacks
OSI
TCP/IP
Multi-layer protocols
Network addresses
MAC
IPv4 and IPv6
VPNS
IPSEC
Virtual Machines

Domain 7 Detail

Technologies	Skills	Skills	
Intrusion detection and response			
firewall	packet filtering		
	stateful		
	proxy	application level	
		circuit level	
firewall architecture	packet filtering	manages connection to DMZ	
		separate external | internal	
	dual-homed host		
	screened host firewall		
	screened subnet firewalls		
	bastion host		
	SOCKS		
Internet | extranet | intranet			
data network services	file services		
	mail		
	print service		
	client | server services		
	domain name service		
type of network	LANs		
	MANs		
	WANs		
	GANs		
LANs			
LAN transmission method	unicast		
	multicast		
	broadcast		
topology	physical	bus	
		ring	
		star	
		mesh	
		tree	
	logical	ethernet	

		token ring	
		FDDI	
		ATM	VPI
			fixed data cell size
		HDLC	
		ISDN	
		X.25	
LAN transmission protocol	CSMA		
	CSMA-CA		
	CSMA-CD		
	token passing		
	Polling		
Ethernet			
cable	thinet		
	thicknet		
	unshielded twisted pair 10 base t		
802.11 wireless	radio	FHSS	
		DSSS	
	802.11b		
	802.11a		
	802.11g		
WAN			
Device	routers		
	multiplexers		
	switches	circuit switched network	
		packet switched network	
	access servers		
	modem		
virtual circuit	switched virtual circuits SVC		
	permanent virtual circuits PVC		
technologies	dedicated lines		
	frame relay		
	X.25		

	HDLC and SDLC		
	VoIP		
	Integrate services digitial network		
	DSL and cable modems		
	SMDS		
	ATM		
	private circuit technologies	dedicated | leased line	
		leased line types	T1
			T3
			E1
			E3
		serial line IP SLIP	
		PPP	
		EAP	
	ADSL and SDSL		
	HDSL and VDSL		
cable	coaxial cable	baseband	
		broadband	
	twisted pair	shielded STp	
		unshielded UTP	CAT1
			CAT2
			CAT3
			CAT4
			CAT5
			CAT6 | 5E
	fiber optic		
	cross over cable		
asynchronous communication			
synchronous communication			
network devices			
	hubs		
	switches		
	bridges		
	routers		

	CSU | DSU		
	repeaters		
Protocol			
Encapsulation			
OSI Model	app layer		
	presentation layer		
	session layer		
	transport layer		
	network layer		
	datalink layer'		
	physical layer		
TCP/IP stack			
Ipaddress class	class A		
	class B		
	class C		
	broadcast address		
	private network addressing		
NAT	one to one NAT		
	Pool NAT		
	Many to one NAT		
Name resolution	host table		
	DNS	DNS def	
		DNS hierarchy	
		DNS queries	gethostbyname
			gethostbyaddr
		domain hijacking	
IPv6	definition		
	fetures	route aggregation	
		improved delegation/management	
		autoconfiguration support	
		tunneling	
		translation	
	addressing		
	header		

UDP	features		
	ports		
	header		
TCP	features		
	header		
	flags		
	ports		
	code bits		
TCP vs UDP			
ICMP	Ping		
	Traceroute		
Application layer security protocols	S/MIME		
	SET		
	SSH		
	web security	SSL	
		TLS	
Other protocols	telnet		
	FTP		
	TFTP		
	SMTP		
	SNMP		
Routing			
Address	MAC address		
	IP address		
Protocol	ARP		
	RARP		
Routing protocols	distance vector	RIP	
	link state	OSPF	
	BGP		
remote access security method	Caller ID		
	Callback		
	VPN	advantages	
		client to site	

		site to site	
	type of remote access	dial-up, async	
		xDSL	
centralized authentication control	RADIUS		
	TACACS		
	DIAMETER		
	Domains and trusts		
	Security Domains		
	Constrained user interface		
	CHAP		
	PAP		

Domain 8 General

Domain 8	**Application Security**
overview	application control
	software life cycle development model
	software process capability maturity model
	object-oriented systems
	artificial intelligence systems
	database systems and security issues
	data warehousing
	data mining
Expectation	principles related to secure design of information systems
	security and controls to ensure data and application CIA
	malicious code
	software life cycle

Domain 8 Skillset

	Application security		
	programming languages	Cobal	

		fortran	
		c, C#, c++	
		pascal	
		java	
		Visual C	
	programming procedure	compiler	
		process	
		elements	
	software enviroment	CPU	
		memory	
		i/o request	
		storage devices	
	application control		
	input control	limit or range tests	
		logical checks	
		self-checking digits	
		control totals	transaction counts
			total
			cross footing
			hash totals
			error detection
			error correction
			rejection
			resubmission
	output control	reconciliation	
		physical handling procedures	
		authorization controls	
	processing controls		
	threat		
		buffer overflow	
		scripting | script kiddies	
		covert channel	

		malware	
		object reuse	
		mobile code	
	system life cycle & development		
	capability maturity model for software	quality management practices	
		evaluation of the developmental process	
	system development life cycle	initiation and planning	
		definition of requirement	
		design specifications	
		actual development	
		documentation of application	
		tesing	
		evaluation	
		acceptance	
	method	waterfall	no customer involvement
			no going back
		structured	
		spiral	what should be done next?
			how long should it continue?
		cleanroom	
		iterative	
		prototyping	
		modified prototyping	
		rapid app development	
		joint analysis development	
		object oriented OOP	
		distributed	
	applets	Java	object-oriented

		untrusted Java applets	platform independent
		trusted java applets	sandboxing
			browser setting control actions of applets
			JVM run checks on each object to ensure integrity
		Java security	java authentication and authorization
			java socket extension JSE
			JSSE
			JCE
	ActiveX	object-oriented	
		ActiveX control	
	Rapid prototyping model	XP eXtreme Programming	
	Object-oriented development	class	
		object	
		methods	
		messages	
	Object-oriented system		
	Object-oriented system	black box	code
			data
		delegation	
		polymorphism	
		binding	
		polyinstantiation	multi-level database
		encapsulation advantage	managing complexity
			managing change
			protecting data
	concepts	class	
		instance	
		methods	
		inheritance	
		encapsulation	

		polymorphism	
	advantages	reusability	
		reduce risks	
		model of the real world	
	security aspects	security control for program library	
		communication between objects	
		access control by class	
	enforce security control	abstraction	
		data hiding	
		tight cohesion	
		loose coupling	
	OORA	object oriented requirement analysis	OORA
		object oriented analysis	OOA
		domain analysis	DA
		object-oriented degisn	OOD
		object oriented programming	OOP
		ORB	
		common object request broker architecture	CORBA
		common object model	COM
		distributed common object model	DCOM
	Application control scope		
		distributed enviroment	
		local | non-distributed	
		open source	
		closed source	
		coupling	
		cohesion	
	distributed system req	portability	
		interoperability	
		transparency	
		extensibility	
		robustness and security	

		accommodation of standards	
		meet user's functional requirement	
	distributed system req	CORBA	
		DCOM	
		DDP distributed data processing	better availability
		pros	economic
			increased user involvement and control
			distance and location independence
			privacy and security
			vendor independence
		cons	
	client-server req	fault tolerance	hardware
			disk duplexing
			shadow database
			fail-over
		support	shadow database
			fail-over
	P2P		
	software environment		
	issue	open source	public development
		full disclosure	intentional release of bugs
			exploit code to force security issues
	centralize		
	decentralize		
	general security principle		
	authorization		
	risk reduction	code review	
	separation of duties		
	accountability		
	least privilege		
	layered defense	multiple controls	
	Application control		
	preventive		
	detective		

	corrective		
	apply control to	input	
		processing	
		data hiding	
		interprocessing communication	
		interfaces	
		access control	
		output	
	form of control	administrative	
		physical	
		technical	
	security control	input	
		output	
		transactions	
		process isolation	
		hardware segmentation	
		security kernel	
		modes of operation	dedicated
			system high
			multi level (MAC)
		reference monitor	
	change control	ensure	approved
			incorporated properly
			no original functionality addected adversely
		process	make formal request
			analyze: review security implications
			submit for approval
			develop the change
	security perspective	project initiation	sensibility of information
			critically of system
			security risks
			level of protection needed
			regulatory | legal | privacy issues

		functional design	
		design specifications	design security control
			review design
		software development	document security issues and controls
			conduct code walk-throughs
		software development	review tests
			certify system
		field (installation and implementation)	acceredit
			property configure system
			begin configuration management fielded releases
		maintain (operations and maintenance)	
		destruction	
	operation control concepts		
	least privilege	access control	
		necessary data fields only	
	layered defense		
	change control		
	Artificial intelligence systems	expert systems	
		neural networks	
		knowledge base	
		expert system operating mode	forward chaining
			backward chaining mode
		verification and validation	
	service level agreement		
		turn around times	
		average response times	
		number of online users	
		system utilizaiton rate	

		system up times	
		volume of transactions	
		production problems	
	software prototyping		
	CASE tool		
	software capability maturity model (CMM)	level 1 initial	
		level 2 repeatable	
		level 3 defined	
		level 4 managed	
		level 5 optimizing	
	database		
	databases : CIA	concurrency	
		semantic integrity	
		enforcer DBMS	
		referential integrity	
		commit	
		executes changes that were just made	
		2 pahse commit	
		rollback if commit is unsuccessful	
		database returns to its previous state	
		checkpoints	
	database system	database	
		database management system DBMS	
		types of data models	hierarchical
			mesh
			object-oriented
			relational
		data warehouse	
		datamining	intrusion detection
			fraud detection
			auditing the database
	vuln & threat	aggregation	

		inference	
	web app threats & protection	information gathering	
		parameter manipulation	
		XSS	

Domain 9 General

Security operations
Legal requirements
Privacy and protection
Configuration management and change control
Non-disclosure agreement
Sensitivity markings
Control types
Directive controls
Preventive controls
Detective controls
Corrective controls
Recovery controls
Auditing
Reporting concepts and mechanisms
Roles and responsibilities
Incident response
System resilience

Domain 9 Detail

Skills		
Operation security		
addresses	threats in an operating environment	

	external attackers	
	internal malicious intruders	
	operators inappropriatedly accessing resources	
threat		
vuln		
asset	computer resources	
	hardware	
	software	
	information	
	personnel	
OPSEC	resource protection	
	privileged entry control	control and limit access
	hardware control	
Role	manager | custodian	user IDs
		contractors
		termination procedures
		passwords
	owner	
	user	
administrative management	job requirements	
	background checking	
	separation of duties	
	job rotation	
	vacation and leave	
	termination	
employment agreements	general clauses	
	work hours and overtimes	
	holiday	
	non competition	
	non solicitation	
	confidentiality	
	NDA	
individual accountability		
IS IT functions	audits	

	physical security	
	disaster recovery	
	monitoring	
	incident response	
	training and awareness	
audit trails	date	
	time	
	location	
	audit log backup	
	central logging	NTP server
reconstruction of events	console messages	
	logs	
	correlation from multiple sources	
	extract data from system	
avoid threats	erros and omissions	
	fraud and theft	
	employee sabotage	
	malicious attackes	
	malicious code	
loss of infrastructure	power failures	
	spike and brownouts	
	loss of communication	
	water outage or leaks	
	lack of transportaiton	
	fire	
	flood	
operation controls	resource protection	
	privileged entry control	
	hardware control	
	i/o control	
	media control	
	admin control	
sensitive information	marking	
	handling	

	storage	
	destruction	
control types	directive	
	preventive	
	detective	
	deterrent	
	corrective	
	recovery	
	compensatory	
media security	controlling access	
	proper disposal	
	sanitizing media	removing data
		overwriting
		degaussing
		destruction
RAID	RAID 0	
	RAID 1	
	RAID 2	
	RAID 3 and 4	
	RAID 5	
	RAID 7	
Redundant server	server clustering	
	full backup	
	incremental backup	
	differential backup	
OPSEC vuln assessment	identify critical information	
	assess the threat	
	assess vul of critical info to the threat	
	conduct risk vs benefit analysis	
	implement appropriate countermeasures	
	repeat	
intrusion detection	intrusion prevention	before
	intrusion detection	during
	intrusion reponse	after

	Types	integrity checking
		anomaly identification
		attack signature identification
configuration management	configuration identification	
	configuration control	
	configuration accounting	
	configuration audit	
change control	applying to introduce a change	
	cataloging the intended change	
	scheduling the change	
	implementing the change	
	reporting the change to the appropriate parties	
patch management	identify updates when needed	
	obtain updates	
	test updates	
	deploy updates	
	verify updates	
	document updates	
documentation	security plans	
	contingency plans	
	risk analysis	
	security policies and procedures	