Security Management

Introduction

Sec Mngmt = take security controls, integrate, configure, monitor, replace, and update in accordance w a security policy.

Approaches

Threat-based

define info sec as ability 2 resist specified threats 2 resoures * threat model of sys gives set of threats sys is designed 2 combat * threats give rise 2 security violations (unauth – as defined by sec policy - info release, modification, denial of use) * sec violations from inadaq phsycial/computer sys/comm network controls. * vuln = flaw in design or implementation could → security violation (it reps a threat, can be exploited by an attacker) * attackers = active opponents of sys security (insiders/outsiders) * risk assessments = list possible threats, asses likelihood, give potential cost (prob(occurrence) * cost of threat realisation)

Objective-based

ID security goals (positive properties we wnt) like CIA (Parkerian Hexad = possession or control of info, authenticity – ensure origin correct - , utility – ensure info usable-) , accountability, reliability/dependability (perfm reliably in adverse conditions)

Sec evnt = occurance that may indicate a sec violation (must be logged and investigated)
Sec evnt mgmt = defining procedures 4 reporting and mnging security breaches.
Sec awareness training
Business Continuity Training

OECD Sec Principles = Awareness * responsibility * response * ethics * democracy * risk assessment * sec design and implementations * sec mngmt * reassessment.

Data Privacy = orthogonal 2 data security * proection of PII * relies on provisions of data scrity *

Computer security = protection of data stored/processed in main/secondary memory * protection typically rules based * protection mechanisms incl. Crypto (dist sys and storage), auth policies * access cntrl mechanisms. * Trusted Computing Base (collective mechnisms 4 enforcing sec of stored data)

Info sec mngmt = all aspects of mking sec happen in org * CISO responsible * key stages: Leadership (commitment, policy, responsibility, risk appetite), Planning (risk asses process, risk treatment process, set sec obj), Support (allocate resourc, awareness, doc key aspects), Operation (op plning/control, prform risk assessments/treatments routinely), Performance Evaluation (monitoring, audit, review), Improvement.

Standards For Info Sec Management

ISO/IEC 27000 series

2700: Info Sec Mgmt Sys – Overview and vocab
Descriptive
Clause 2 = def ISMS terms
Clause 4 = desc of mmbers of 27000 fam
Clause 3 = desc of what consitutes ISMS
General : treats info as asset & maintain CIA * orgs must monitor effectiveness, id risk, impl and improve controls * 2 co-ordiante above, estab policy and obj and meet objs thru mgngmt system
What is an ISMS: ISMS = systematic approach 4 estb, imp, op, monit, rev, main, impro info sec sys 2 meet bus needs, consists of policies, procedures, guidelines, and based on risk assessment linked 2 orgs risk acceptance lvl * successful ISMS incl.: Awareness of need, assignment of responblty, mngment commit & stakeholders interests, enhance societal values, rks assessments, sec treated as essential, actv prevention & detection, comprehensive approch, continued reassessment w approp modifications
Process Approach: id & manage activities (wch involve processes = transformation of inputs to outputs, which → input of anthr process. Process approach = use of set of processes and their interactions)
Why ISMS: risk address tailored 2 org * security complex * sec not just tech problem
Establish: ID reqs (the info, tech, and legal)→ assess risks (periodic assments tht estimate magnitude [risk analysis] & compare against risk criteria 4 significance [risk eval]) → risk treatment (control, accept, avoid, share) → select cntl (Statement of applicability against 27002) → monitor (ISMS review = check ISMS incl. Cntrls suitable 4 risks within scope, chck perofrmace etc) → improve (no assumption ISMS is good enough)
Benefits of ISMS stndrds family: structured frmwrk * help mngmt * promote global accepted good practices * common language * increase stakeholder confidence * satisfy societal needs and expactations * more effective economic mngmt of security investments

27001 – Standards requirements
Instructional ('shall') * can be audited against
Clause 4 - org context: scope of ISMS (anticipate external/ cntrl interal, reqs of interested prties, interfaces & dependencies etc) * establishing an ISMS

Clause 5 – leadership: ldrship & cmmtmnt (policy compatible w strategic direction, ISMS reqs in orgs processes, rsrcs needed available, communication of importance of conforming, ensuring ISMS achivs objs, directing and supporting ppl, promote contnual improvement, sppt other management roles) * Policy (approp for org, has info sec obj or framework for setting them, has commitment 2 satisfy reqs and 2 continually improve, documented, available, communicated) * roles, responsibilities, authorities (assignment and commincated)

Clause 6 – Planning (actns 2 address risk and plan 2 meet sec objs): Risk Assessment (estblish criteria [4 rsk acceptamce and 4 performing assessment], ensure repeatability/validity of results, IDs risks, analyses risks [consequences, prob of occurance, lvl of risk], eval risk [cmp results of analysis w risk criterial → prioritise → treat) * Risk treatment (SOA, also obtain risk owners approval of treatment plan and acceptance of residuals) * Sec Obj (what to be done, resources, who responsible, when 2 be completed, how results evaled. Each obj: consistent w sec policy, measurable if poss, into account info sec reqs, b communcated, b updatd as approp)

Clause 7 – Support: Resources * Competence (train persons, keep evidence) * Awareness (of info sec policy, of their contribution 2 effectiveness, of implications of not conforming) * Communication (what, when, to who, from who, and how) * Documentation (creation: id and desc, format, review and approval. Control: available & suitable, adeq protected, distribution/access/retreival/use, storage/preservation, control of change, retention and disposition, also external doc should be ID and controlled)

Clause 8 – Operation: Planning & Control (plan and cntrl processes, implement plans 2 achieve objs, keep docs as confirmation processes carried out as plned, cntrl planned chnges and review [incl. Consequences of *unintended changes* 2 mitigate adverse effects], outsrced processes are cntrlld) * Info sec risk assessment (prfmed at planned intervals & when changes occur, using established criteria) * Info sec treatment (carry out treatment plans)

Clause 9 – Performance eval: general (wht to be monitored/measured, methods 4 montior/measure/analysis/eval, when monitor/measure, who monitor/measure, when analysis and eval, who analyse) * Internal Audit (define criteria/scope, select auditors 4 objectivity, report results 2 relevent mgmnts, retain docs) * Management review (status from prev reviews/internal and external audits, feedback on performance [measurments from monitoring and results], feedback from intersted parties) 2 produce decisions on continual improv opps and need for changes to ISMS

Clause 10 – improvement: Nonconformity and corrective action (react/eval/implement/review/make change) * Continual improvement

27002 – Security Controls
Code of practice for info sec controls (catalogue w guidance of sec policies and 34 cntrl objectives w implementation guidance etc)

27003 – Audit and cert
Guideliens for ISMS auditing (for bodies providing ISMS cert, supplement to 17021 wch guidelines cert for general mngmt systems)

Other standards: PCI-DSS (Payment Card Industry Sec Standards) * NIST 800-53 Sec Controls (guidance of controls used by federal info systmes)* NIST 800-30 Risk assessment (4 use by federal info systems)

Risk Management

Inherent risk = from inate props/chars of asset/situation
Residual risk = what remains aft risk mngmt applied
Risk capacity = lvl of loss org can absorb
Risk appetite = lvl of loss an org will accept (shud only rise w capacity)
Risk tolerance = lvl of loss org will accept for short term over risk appetite
Ris exposure = varying lvl of risk being managed/accepted/retained
Risk assessmnt= set of struct processes 4 capturing what is at stake, potential for (un)desirable events, measure outcomes
Risk management = process of dev and eval options 2 address assessed risks in way agreeable 2 impacted ppl
Risk governance = overarchn set of ongoing processes & principles 2 ensure awareness & education of risks faced whn actions tkn/occr

ISO/IEC 31000 – general apprch 2 risk management
Steps: Comm and consult * establish context * risk assessment (risk id, analysis, eval) * Risk treatment * montoring & review (throughout). ITERATIVE

ISO 27005: guidelines for risk mgnmt
Should bes: align w overall risk mgntm * continual process * ITERATIVE
Steps:
Context establishment (collect info on sys/services/apps/equipment in scope; set basic criteria for evaluation/impact/risk acceptance; define scope & boundaries; estb approp organisation like roles/responsibilities recording intentions & escalation paths)*
Risk Assessmnt :
Risk Identificaiton (assets/owners/threats/existing cntrls/vulns/consequences),
Risk Analysis (depends on criticality of asset, known vulns, and prior incidents. Qualitative = uses scale of attributes, adaptable 2 circumstances, simple 2 understnd, subjective choice of scale, used for initial screening/inadeq numerical data/approp 4 decisions. Quantiative = scales of numbers, uses usually historical data, depends on accuracy & completeness of data, but no data on new risk or weakness?, data not auditable/ factual => illusion of accuracy)

Risk treatment (risk modification, retention/acceptance, avoidance, sharing) *
Risk communicaion (stakeholders, awareness, coordinate response, collection) *
Risk monitoring *
Risk reporting & Escalation

Risk acceptance (residual risk should always be explicity accepted)

Risk management
Obj: Give decision mkrs confidence, ensure sys not manipulates, miminise impacts
Success factors: strong risk gov (top down) * focused & clear assessment (clear goals set agnst risk appetite)* robust framework * risk culture & leadership
Failure factors: confusion (abt lvl of risk, scope) * tik box exercise * internal reputation damage 2 risk functions * external reputation damage shud loss occurrence

Three Lines of defence:
1LOD – risk owners * op management responsibl & accountable 4 assessing/mitigationg/controlling risk
2LOD – monitor/facili risk mgnmnt practices & assist reporting risk related info
3LOD – internl audit 4 assurance 2 stakeholders * **INDEPENDENT for objectivity**

Risk grid – gives impact vs likelihood (& mybe 3d maturity)

Risk Registry = record of residual risk * gives risk owners, mitigations, timelines * provides risk exposure

Human Factors: Risk asymmetry (too averse not considering benefitys, too causal etc) * confirmation bias * knowledge & expertise (an immature field) * deference (unable 2 chllng senior mngmt) * personal impact (how it impacts indiv will imapct decision making)

Security Policy And Controls

ISO/IEC 27001
Code of prctc 4 info sec cntrls * not needed 4 cert but needed 4 SOA needed 4 cert. * *covers security policy like its a cntrl*

Clause 5 – Policy
Procedure = steps to achieve obj of policies
Policy = scene settr giving principles, rules, responsblits
Obj of sec polcy = provide mngmt w dirctn and support 4 info sec accordin 2 bus reqs/laws/regs
Top level sec pol: signed by execs * def on ifno sec, obj, principles 2 guide activites * assign responsibilities * proc 4 handling deviation/exceptions
Topic specific sec pol: cn cover: access control * info classification * phys & env sec * end usr sec (accptbl use, clr desk, info transfer, mob devics, soft restriction etc) * backup * inf transfer * mal protection * mngmt of tech vulns * crypto cntlrs * policy/protct of PPI * supplier relationships

All policies should be reviews (w owners tht ensure they are) and communicated

Controls
Clause 6 – Organisation of Info sec: internal org (rls respons, segregation, contract w auth and special interest groups, info sec in proj man) * mobile devices & teleworking

Clause 7 – Human resources sec:
prior/during/after/changing employment

Clause 8 – Asset Mgmt: Responsibility 4 assets (inventory, classifct, accpt use, rtrn) * Information classfct (labellign, handling) * Media handling (mgnt, removal, disposal, phy media transfr)

Clause 9 – Access Control: Busns reqs for acces cntrl (policy, accs 2 network/net services) * User access mgntmt (mngmt, provisioning, priv accs rights, secret auth mngmt, review rights, rmvr/adjustments of rights) * User Responsibilities (use of secret auth ID) * System & applctn access cntrls (restriction, secure log on, psswd mgnt sys, accs 2 progrm source code)

Clause10 – Cryptography: crypto cntrls (policy for the use, key mngmnt)

Clause 11 – Physical and environmental security: Secure areas (perimiter, contrl, secure pl8 aces, protection from external and env threats) * Equipment (maintanence, re-use, security off premise, disposal, unattended equip, secure desk)

Clause 12 – Operation Security: op procedures and responsibilities (documented procedures, chng mngmt, capacity mngmt, sep of dev testing and op env) * Protection from malware * Backup * Logging and monitoring (event logging, protection of log info, admin an op logs, clock sync) * Control of op software (installation) * Technical vulnerability mgntm (but alos restrictions on soft installation) * Info systems audit considerations

Clause 13 – Communication Security: Network sec mngmt (net cntrl, sec or net services, segregation of networks) * Information transfer (info trnsfr policies/ procedures, agreements, electronic mssging, conf or non-disclosure agreements)

Clause 14 – System Acquisition, Development, and Maintenance: Security reqs of info systems (analysis & specs, secure app services, public net connection?, scr transactions) * Sec in development and support processes (dev policy, change control procedures, technical review aft plat change, restrictions on chnges, engineering principls, secure dev env, outsourced dev, syst security testing, system acceptance testing) * Test Data (protection of test data)

Clause 15 – Supplier relationship: Info sec in supplier relationship (policy, agreements, info and comm tech supply chain) * Supplier service delivery mgmnt (mntr/review supplier services, mng changes)

Clause 16 – Info Sec Incident Mngmt : mngmt of info sec incidents & improvements

Clause 17 – Security Aspects of continuity mngmt: jnfo sec mngmt * redundancy

Clause 18 – Compliance: w legal and contractual reqs (Identify applicable leg and contractual req, intellectual property rights, protection of rights, priv & prvil of PII, regulation of crypto cntlrs) * Info sec reviews (independent review, compliance wsecurity policies & stndrds, technical compliance review)

Application Specific Controls

27010: Inter-Sector and Inter-organisation Comm
27011: Telecommunications organisations
27015: Financial Services
27017: Cloud Services
27018: Protection of PII in public clouds acting as PII processors
Help CSP comply & be transparent/assists in contractual agreemnetnts/ provide cloud cust w auditing & compliance rights mech * supplements to 27002 reccomends: addtn mech 4 offline backup, mult copies in diverse locations, CSP 2 provide clear info aout backup and restore capabilities, sec policies should contain clear allocation of responsibilities & stmnt concerning support for achieving compliance * Additional contrl: oblig 2 co-op regarding PII principles rights (mechs for access, correction, erasion) * Reqs depend on legal jurisditction & terms of contract
27019: Process control systems specific to the energy utility industry
27799: Health Informatics

Legal & Regulatory Issues

EU Law

Council Of Europe conventions – not binding but agreements
EU Decisions – binding upon those it addrsses
EU Regulations – immdllt enforcable law 4 all mmb states
EU Directives – do this obj in ur own way

General Issues:

Open 2 interpratation/hard 2 undstnd/ inconsistent: GDPR article 35 'likely to' 'high risk' * UK's 10 step clarification 'certain cirumstances' * UK's cndcting priv assessments code of practice says parts will 'depend on usual practice'
Jurisdiction issues: business operating in territory subject 2 laws of that territory (how do u define doing business, what abut wht they do outside of territory)

Privacy Law

UK 1984 (personal) data protection law:
1) processed fairly 2) 4 specified puprose 3) not used/disclosed incompat w purpose 4) adequate, relvant, nt exessive 4 purpose 5) accurate, up 2 date 6) nt kept longer than needed 7) principle can ask 2 see without undue delay/expense 8) secure against unauth.

EU protection directive 1995: uk data protection act 1998/2018:
1) Notice 2) purpose 3) consent 4) security 5) disclosire 6) access 7) accountability
2018 goes beyond GDPR (intel service/ imigration service/ local auth data processing)

EU general data protection regulation (GDPR):
Applies 2 EU data wherever stored * open 2 national interpratation * stiff penalities * what it did (widen def of personal data, tighten consent getting rules, refines basis 4 lawful processing PD, required Data Protection officer, mandatory Privacy Impact Assessment, right 2 be forgotten, common data breach notification, extends liability 2 orgs touchng PD, set rules on law enforcement access)

National trend: inconsistent international privacy rules * trend towards extraterritorial * req 2 report breaches widespread * individuals greater control * tend 2 mandate encryption.

Security And Corperate Regulations

Financial:
US: Sarbanes-Oxley – req policies 4 security gov, availability, integrity tht are documented ad commun * IT depart. Risk assessmnt integrated 2 overall risk assessment processe
UK: Uk Companies (audit, investigation & community enterprises) Act ; Uk Turnball Guidance On Internal Cotnrol & Risk Management – req formal statemnt on internl risk in annual accounts

Third Parties:
outsourced/managed services, partneships, supplies, customers, and contractors * req audit security capabilities & define security aspects of contract.

EU NIS Directive:
Goal: bring cyb securtiy in line 4 increased cooperation & efficient info exchange
Reqs: setup Computer Security Incident Response Team and National NIS Authority * Cooperation Group 2 suuport strategic cooperation & info exchange * business ID'd as essential services 2 tk proper sec measures and notify on incidents (inclds. Digital service providers [search engines/cloud providers/online marketplaces]).

Data Retention Reqs:
Uk Legislation to Mitigate Money Laundering (retain data 4 at least five years)

Other

Consumer Protection:
not much in place * 2018 Uk Code Of Practice 4 consumer IOT sec (no default passwords, vuln disclosure policy, keep software updated, secure store credentials, + 9 others) * 2019 approved EU cyber Security Act: framework will spt single sys 4 providing assurance in sec properties of IT products and services

Cryptography
wide international variance * political implications * law conflicts (data protection vs law enforcement rights) * orgs need policues on crypto use & key management (tht recognises naitional legal vartiation & covers export/import use.

Law Enforcement Access:
many countries have mechs for requesting access (some countries dont require formal processes)

Discovery and retention:
not relevant data deleted * archived =/= backedup (archived also not tampered with) * info can be outside direct control (e.g IM, cloud, personal devices)

Employee Monitoring:
Lawful Business Practice Regulations (montioring must be relevant to business)
UK ICO Guidlines (employees right to privacy overules but theres balance * conduct impact assessment * clear purpose/benefits * employees aware * covert monitoring only in specific cases * establish and communict acceptable use policy)

Computer Misuse
Criminal offence in mny countries * delegation of authority is issue (must be formally documented) * orgs myst have acceptable use policy (4 all types of devices , covering personal use & common prct) to shud be signed by user (alth doesnt always help in prosecuting)

Electronic Signatures
liability needs 2 be defined and what is being signed understood * e.g Uk electronic commerce act

EU Payment System Directives
2007 – regulate services and providers * goal increase participation/competition, harmonise protection/rights/obligations of consumer
2015 – bettr protection 4 online customers * promote dev of innovative online/moile payments * make cross border EU payment service better

Fraud: Uk fraud act
Copy rights and digital rights management (DRM): EU copyright directive, UK copuright act * can cnflict w customers security controls
UK Sexual offences act

Audit

Internal Control
Internal Control = process invol. all in org to provide reasonable asurance that obj will be achieved in: effectivnss and efficiency of op (make mony) * Reliability of financial reporting (accurt not misrepeesented) * compliance wth applicable lws and regulations.
Five components:
Control evironment (=culture/tone, demstrt commit 2 integrity/ethics, brd of directors sep from mgnmt 4 oversights, etsbsh struct/rprting lines/auths/responses 4 persuit of obj, attract competency, hold indiv respons 4 intern controls)
Risk Assessmt
Control activities (= policy/procedures 2 ensure mgmt drectives carried out, e.g approvals/auth/verificaion/reviews4performace/seg of duties)
Info and Comm (generate rel info and comm it)
Monitoring (ongoing -by supervisor? - or sep eval – by independent? - , always timely)

Sec in internal control (= subset of internal controls, incl. Risk assesment/control activites/ monitoring – principally relates 2 operation)

Audit
Provide 3rd party assurance 2 stakeholders that sbjt matter is free from misstatement (so can eval and imporv mgmnt/control/governance) * audit standards say consider risk posed by IT
External financial audit – audit financial stmnt * dn by indep accountant * cn involve looking at IT syss and sec (more efficient than looking at each interaction)
Internal audit – look @ internal controls * specialist function sep from rest of org * part of monitoring
Security audit – look @ sec controls * internal or external.
Issues 4 reg bodies: audit quality * independence/conflict of interests * competition and choice (can be worse due 2 independence reqs)

FRCs UK ethical standard
Principles: Integrity (trustworthy, compliant w spirit of ethics laws/regs/principles, respect conf exept in better interests of public)* Objectivity * Independence (free from conditions/relationships tht would compromise integ or objectivity)
Threats 2 independence: self-interest (having stocks)* self-review * management (crossing line from giving advice to managing) * advocacy * familiarity (or trust) * intimidation

Extenral audit carrying out security work?
Adv: Know buiss * legal etc expert as well as tech * can translate tech into busin
Disadv: shud financially focus on auditing functions (regs oft limit amount of 'other work') * scope of work conflicts w auditor role (self-review)

Examples of security audits
Security Control Review and Audits
incl. Business proces review (restricted access etc) * It process review (change cntrl, dev and impl, sec and op over env)
Adv: benchmark against: good practice/other companies/other internal divisions/managements assessment of risk

Pen Testing
ensure u know scope (also dont topple systems) , testers have integrity, results are kept secure

Security Incident Investigating
Clear purpose as goals aren't always congruent (preventing further problem? Recover assets? Prosecution of crims? Reassuring stakholders?) * what skills needed (specialist, in-house vs external etc) * comm approp (who needs to know what and when) * put strategy in place quickly * know when investigation is done else ull go on forever.

Incident Management, Business Continuity, & Disaster Recovery

Info sec event = identified occurance tht cud indicate a sec relevant situation
Info sec incident = single or series of info sec events that have high prob of compromising business ops & threatning info security
Info sec inciden mgmt = proceses 4 detect, report, assess, responding 2, dealing w, and learning from info sec incidents

Reporting info sec events

27002/ control 16.1.2 – *reprted thru approp mngmnt channels quickly* * usrs must be aware of the channels and procedures * use standard form to ensure al info captured (identity of reporter, office/geography/dept, contact deets, brief desc of incident, dangers posed 2 health/assets, oth impacts to buis ops, desc of actions tkn, time incidnt first noticed) * all actions after report shud also be logged

Incident Report Team – appoint in advance frm across org, in pos of authority, w resources * have escalation process 2 reach snr mngmt * have copy of incident reposnse plan doc * readily contactable

Maybe involve law enforcement if terrorism/child pon/ sus financial activities)

Procedures

27002/ control 16.1.1 – *proc estblsh 4 quick, effective, orderly response* * proc 4 response planning/prep, logging incident mngnt activities, handling forensic evidence, asses of events, response escalation/controlled recovery/ and communication * focus on high prob and high impact event * each procedure shud ensure competent personell handlers and points of contact in and outside organisation

Assessment of Security

27002/ control 16.1.4 – *events assessed 2 decide if classified as info sec incident* * done by POC who may send to IRS for conf or reasses * help ID impact * record results

Response to Info Sec Event

27002/ control 16.1.5 – *respond in accordance w documented procedures* * done by POC and incl. Rapid collection of evidence, conduct forensic anal, escalation, logging response activites, comm, dealing w what caused incident, formal closure

27002/ control 16.1.7 – *define and apply procedures 4 IDing, collection, acquisition, and presentation of evidence*

Learning from Security Events

27002/ control 16.1.6 – *use knowledge 2 reduce likelihood or impact of future incidents* * use info to ID recurring * mechs 2 quanitfy/monitor types/volumes/costs

Reporting Security Weaknesses

27002/ control 16.1.3 – *employees/contractors req 2 notify/report observed/suspected info sec weakness in sys/service* * report mech shud be easy, accessible, and available (but b wary of ppl taking advantage)

ISO/IEC 27035 'Security Incident Management'

Three parts: principles of incident management * guidelines 2 plan and prepare for incident response * (under dev) guidelines for ICT incident response mgmnt
5 phases: plan and prepare * detection & reporting * assessment and decision * responses * lessons learnt

Disaster Recovery and Business Continuity

Business Continuity = measures implemented by org 2 enable it 2 continue after a major incident
Buisness cont plan = maintaining cont of bus ops in the face of problems that vary in severity
Disaster recovery = required when a problem is so major tht normal ops are damaged or disrupted beyond reasonable/rapid repair
Difference in in scale of steps involved and magnitude of financial consequences (if minor adjustments => BCP, if widers impact – and normally aout contingency planning for IT- => DR)

ISO/IEC 27002 Clause 17 'Info sec aspects of BC Management'
27002/ 17.1 – *info sec cont shud b imbedde din orgs BC mngmt sys.*
27002/ control 17.1.1 - *'org shud determine reqs 4 continuity in crisis/disaster'* * org check if info sec captured by normal BCP or DR processes
27002/ control 17.1.2 - *'org shud estb, doc, implement, maintain proc, proced, controls, 2 ensure reqd level of continuity of info sec during adverse situations'* * adq mngnmt control structure in place 2 prepare * incident response personell r competent * documented plans w approved recovery processes * establish security controls,processes,procedures, imp changes (4 maintaining whats there), compensation controls (4 what cant be maintained)
27002/ control 17.1.3 - *'org shud verify sec continuity controls regularly ensure they are effective in adverse situations'* * exersise/test the procedures and routines to operate them

27002/ control 17.2.1 - '*info processing facilities shud be implemented 2 sufficient redundancies 2 meet availability rews'* * and test redundant systems 2 ensure they work as expected

ISO/IEC 27031 – Guidelines 4 Info and comm tech readiness for BC
Covers planning, implementation/operation, monitoring/review, and improvement * diff orgs diff reqs * dont care about specifics but classes (incl. Magnitude and likelihood) * mgmnt decide what parts of DC plan implemented (Invocation Decision) and degree * awareness and education essential so staff aware of plan and import. * doc of plans 2 be available and accessible but also secure since may contain sensitive info * you can outsoure DC * test procedures (like whether backup accessible and readable), Full Enactment = following procedures as if there's an emergncy

Staff Management

People

ISO/IEC 27002 Clause 7 – 7.1 Prior To Employment
Obj: ensr employees/contrcts undstnd reposnibilities suitable fr roles for which they are considered
7.1.1 Screening - 'bckcgnd verification checks shud be carried out in accordance w laws/regulations/ethics, and proporional to bus reqs/classif of info access/percieved risks' * if permitted get character witness, cv verification, qual conf, indie ID verification, credit review, criminal record etc
7.1.2 Terms and Conditions of Employment – contract agreement shud state e/c and orgs responsibiities 4 info sec * reflect org policies and state NDA/legal responsibilities/rights and actions taken if ignored.
Employee contract = stndrd of behaviour/IP ownership/grounds 4 discipline/NDA etc
Service Contract = nature of service/ policy, proc 2 follow/performance commitment/shared risk w provision 4 ompensation in failure event

ISO/IEC 27002 Clause 7 – 7.2 During Employment
Obj: ensr e/c aware of/fulfil sec responsibilities
7.2.1 Mgnmnt responsibilities - 'mgnt shud req all 2 apply info sec inline w policies/procedures of org' * brief e/c on roles/responsibilities * motivation 2 fulfil sec policies/T&Cs * have appropr skills/training * provide anon reporting channels.
7.2.2 Info sec awareness/ed/training - 'e/c receive approp awarness/ed/training/reg updates on policies, procedures/ all relevant job functions.'
7.2.3 Disciplinary process – shud be a formal and communicated disciplinary process in place 2 take ation against employees who have committed info sec breach'

Code of conduct = CIA obligations and also standard and ethics * e.g not accepting gifts
Acceptable Use Policy (end-user code of practice) = how employee can use org info and systems * org can be held accountable 4 employee actions so get them to sign 2 show due diligence * must specify severity levels/disciplinary steps 4 each offense
Segregation of Duties = minimise power and reliance on indiv (e.g sarbanes oxley, uk financial services demands etc)

ISO/IEC 27002 Clause 7 – 7.3 Termination/Change of Employment
Obj: 2 protect org interests when changing or term employement

7.3.1 Termination or change of employement responsibilites - 'some info sec responsibilities are ongoing after termination and these should be defined, commed, enforced.'

User Access Controls

ISO/IEC 27002 Clause 9 'Access control'

9.2 user access management – to ensure auth access and prevent unauth access:

9.2.1 user acces mngmt * 9.2.2 user access provisioning * 9.2.3 mngmt of priv access rights * 9.2.4 mgmnt of secret auth info of users * 9.2.5 review of user access rights * 9.2.6 removal or adjust rights

9.3 User responsibilities - 'make users accountable 4 safeguarding auth info'

9.3.1 Use of secret auth info – keep secret/good password/don't share/ protect property etc

Access Control is based on auth'd ID's (RBAC roles based where roles have permissions shud be mngm)

Data classification: assets shud be classified in a sys (e.g top secret, confidential, unclassified etc) and protection shud correspond to potential damage

Training and Awareness

Culture: **most important** * top down * what we actually do, not wht we should do * dont make obstructive to productivity * dont give too much to read (dont exhaust compliance patience) * make relevant to job functions etc * awareness (why)

ISO 7.2.2 training/education should incl: commitment of company * points of contact/resources * legal/regulatory obligations * basic info sec proc/controls * cover acceptable use policy

Awareness = why

Training = How

Procedural Issues

Policies = general rules and principles

Procedures = describe how to achieve task [fulfilling/conforming 2 policy] in series of actions in certain oder * cud be thought of as security cntrl * configuring security cntl, config new sys etc

Information Security process = mngmnt security + procudures + process doc * mjr part of ISMS

Documentation shud be proportional 2 risk * unreadable => nt used

Why procedures important: Correctness (ops done right, cover all important tasks) * consistency and recording (same across staff, clear records 4 obligations and ease of backups etc) * Accountability (so all important ops carried out by approp staff members, specification of segregation of duties, approp records of who did what when)

Whats in procedures; depends on applicable corp standars/style of author/skill set of target audience * Norm include: roles/segregations/equip or data needed 4 procedure/ seq of steps and roles needed / wht 2 be recorded upon completion

ISO 27002 Clause 12

Clause 12.1 - 'Op procedures shud be doced and made avail 2 all who need them' * 4 all ops associated w info procesing * shud specify op instructs

ISO 27002 Clause 6: Organisation of Information Security

6.1 'Establish mngmt framework 2 initiate & control the implenation ad op of info sec within org'

6.1.1 Information Security Roles & Responsibilities - 'all info sec responsibilities shud be defined and allocated' * responsibilities 4 protecting assets/security risk mgngmt/ accountability when delegating etc

6.1.2 Segregation of duties - 'conflicting duties and areas of responsibility should be segregated' * prevent collusion * prevent dependence * difficult 4 smaller orgs (so consider other controls eg. activity monitoring, logging, supervision etc)

Examples

Backup – who/when/where/ how often/ what/ protections/ recording details of backup (who/when/problems/ID attached to medium)

Restoring from backup

Auditing backup

Checking backup

Production sign off – checks needed b4 authoisation (on tests, docs, timing of release etc) / who is authorised/recording authorisation/ when made

Soft/Sys production testing

Documentation

Defect Management

Staff induction – correctness of cv/ crim record/reference/sign of contract & acceptable use policy/ intro and training/ policy briefing/ access granting

Staff termination

Disciplinary actions

Incident Reporting

Failurers

Preventative
Benefits: make more secure, required for regulation/legal, user confidence that ur trying,
Make sure to improve upon
Disadvantages: Never 100% secure, zero-day etc

Reactive:
Benefits: improve learning, improve damage control, business continuity, etc