**IY5501 SM**

concerned with how to use this security technology in the ‘real world’ to protect organisational assets, of most important = information.

In practice:

- More than just deciding  
everything = designed according to security policy

- No. of ppl designing + building < no. of users

- Tech not used properly = wont help ensure security

- using security tech effectively  
- ppl and how their activities interact with tech

Information security

- Ability to resist certain specified threats to resources

- Maintenance of certain objectives for resources

Threat-based approach

- specific threats -> controls to prevent threats

- diff sys in diff env = diff threats  
- threat model  
  
Threats = security violation = damage to system

Security violation:  
- unauthorised information release  
- unauthorised information modification  
- unauthorised denial of use

- might have other possible consequences (other sensitive data may be leaked, priv escl)

Authorised? (or not)? = defined in security policy

Why security violation? – inadequate controls

Controls = measures in place to provide security

Vulnerabilities   
= flaw/weakness/implementation leads to security violation  
= threat to system security  
= exploited by attacker = security violation  
 (attacker must know the vuln, exploit the vuln)

Attackers = insiders/outsiders   
insiders = difficult, if insider is trickier, is it insider/outsider?

Risk Assessment = assessing imptance of each threat -> should combat? = managing risk

Cost of threat MAY < cost of prevent

Scope of threats  
security issues = many = poor implementation of sys, coding/design issues

**Objective-based approach**

- identify Security Goals

- trying to preserve desirable properties (CIA)

Confidentiality – prevention of unauthorised information release;

Integrity – prevention of unauthorised information modification;

Availability – prevention of unauthorised denial of use.

Security goal = met IF violation don’t occur

Difficult = anticipate all possible ways atker cause a security violation = achieving security goal = difficult

Other Goals = accountability, reliability (perform in adverse conditions), security event management

Security event management = defined procedure for reporting + managing possible security breaches/ suspicious events

Others = security awareness training, BCP, DRP

MORE! = possession/control, authenticity(non-repudiation), utility(usable/reachable)

OECD = Awareness Responsibility, Response, Ethics, Democracy, Risk assessment, Security Design and implementation, Security management, Reassessment

Privacy in this sense is not really part of security, although enforcing privacy relies on the provision of security. That is, protecting user privacy requires the correct implementation of security measures, but security does not necessarily require user’s privacy rights to be enforced.

Network Security = data in transit

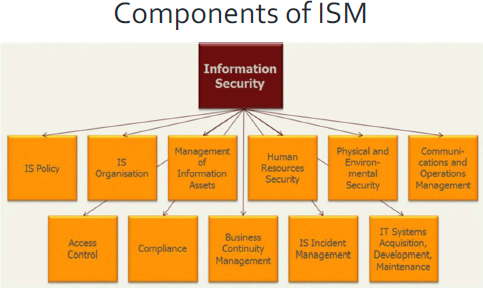
Computer Security = data at rest (Trusted computing base)

Security + functionality  
user expectation + requirements changes a lot in last 30 years

ISM = broad = make security happen = CISO

Leadership, planning, support, operations, performance eval, improvements

Different standards = notation of ISMS (27000)



Security Policy = intentions and directions of organization as expressed by top management

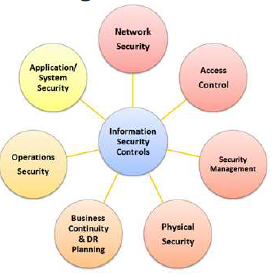
- Includes security objectives, provides framework for setting info security objectives

Security objectives = highest = CIA

- depends on assets and criticality of assets on business

- developed as part of risk assessment (identifying key assets of organization)

Security controls= measure to modify risk (processes, policies, devices, working practices)



Risk assessment = risk identification, analysis, evaluation

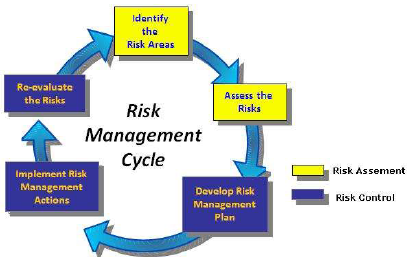
Risk criteria = significance of risk evaluated

(depends on org objective and legal requirements)

Risk evaluation = process of comparing results of risk analysis with criteria = determine risk = acceptable or tolerable

Risk treatment = process to modify risk

(avoid, accept, removing source, change likelihood, sharing)



Legal and Regulatory (GDPR) = module 5

Audit = module 6

Incident management and DR = module 7

Staff = module 8

Procedures = module 9

Failures of ISM = module 10

Case studies = module 11

Conclusion = module 12

**ISO Standards**

International Standards Organisation = ISO

International Electrotechnical Commission = IEC

Joint Technical Committee = JTC

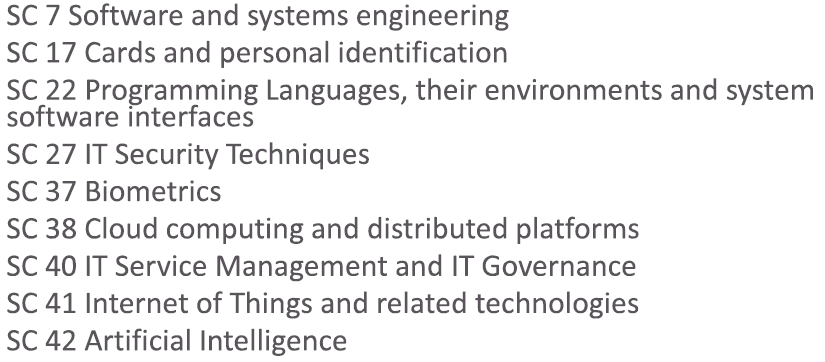
Subcommittee = SC

Working Group = WG

ISO/IEC JTC 1 = Information Technology

Scope = standardisation

JTC = standards dev env where experts come tgt to dev ICT standards for business and consumers apps



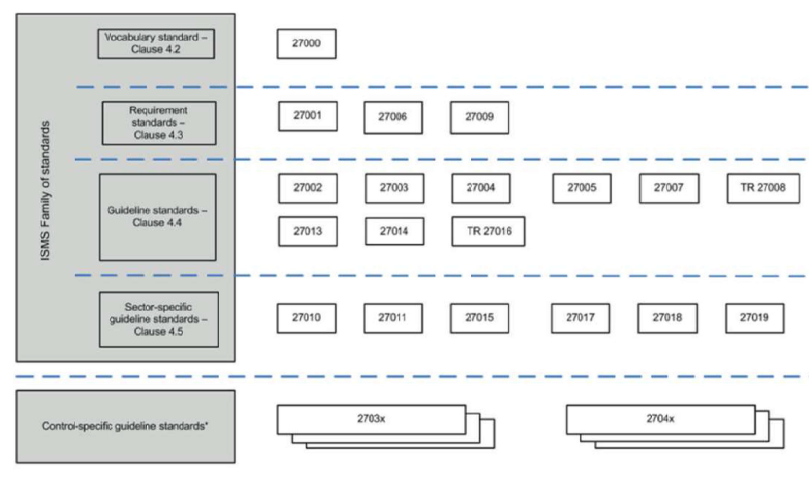
SC27 = IT Sec Techniques = created in 1989

- dev of standards for protection of info + ICT, including generic methods, tech, guidelines for security + privacy

Working Group



Summary of 27000 Series

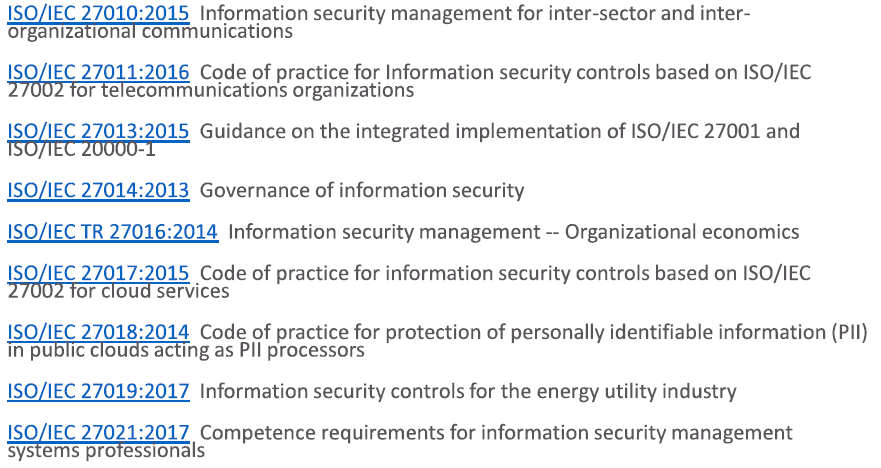


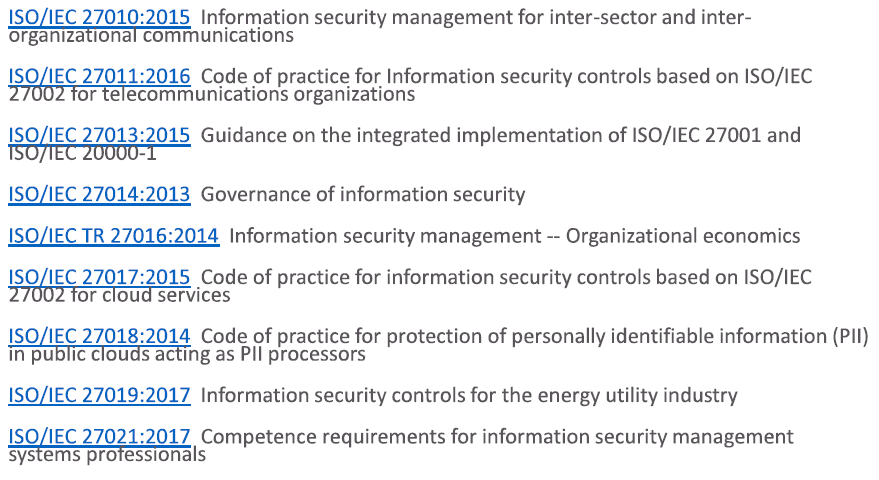
Requirements

Guideline

Sector Specific

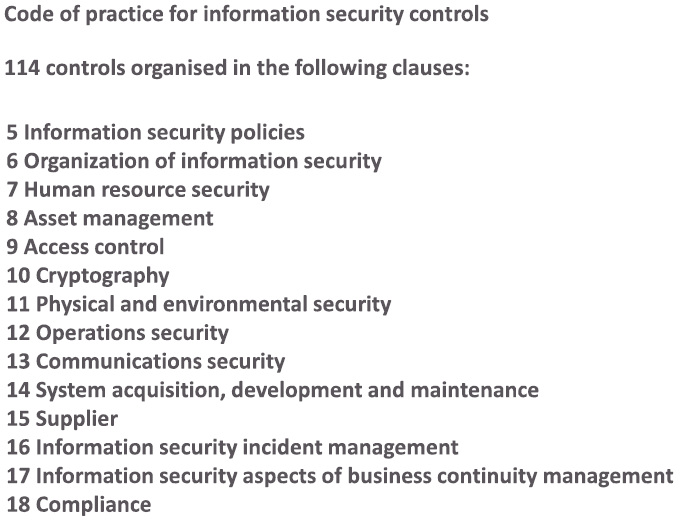
Control Specific Guide Standards







ISO/IEC 27002 (Guideline)



**Others** = NIST, NCSC(UK), CIS/SANS20, PCIDSS

**Risk** = “effect of uncertainty on objectives”, combination of consequences of potential events, and associated likelihood of occurrence

**Control** = measure that is **maintaining+**modifying risk

**Management Sys** = set of interrelated/interlacing elements of organization to establish polices + objectives + processes -> achieve objectives

**ISO/IEC 27001 DeepDive**

**4 Context of the organization**

* 1. Understanding the organization and context

4.2 Understanding the needs + expectation of interested parties

4.3 Determine scope of ISMS

4.4 ISMS

**Impt points:**

- internal + external context needs consideration

- dynamic nature of issues

- interested parties?

- Consider interfaces + dependencies   
(when determining scope)

- Continuous improvement = key to ISMS

**5 Leadership**

5.1 Leadership and commitment  
5.2 Policy  
5.3 Organizational roles, responsibilities and authorities

**Impt points:**

- Board level engagement = key to success of ISMS

- IS policy can vary at different levels

- Policies = clear and written for different audience

- IS gov needs to be part of ORG gov structure to be efficient + effective

**6 Planning**

6.1 Actions to address risk + opportunities

6.2 IS objectives + planning to achieve them

**Impt points:**

- Why risk and opportunities?   
(opp = where money will be well spent)

- Define IS objectives, setting direction + setting specific goals + targets

- Setting out short + long term plans to IS Objectives

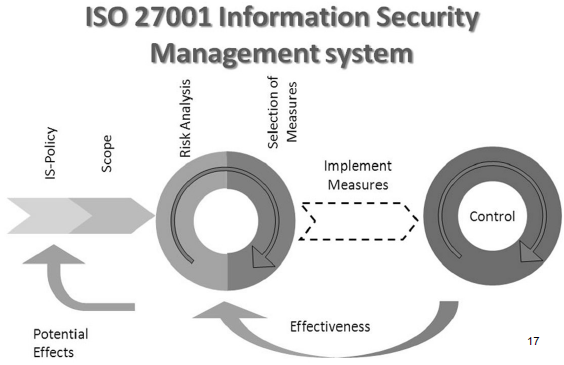
- Plan = risk based, aligned to ORG/Business objectives

**Best Friends to convince board to spend money:**

Regulators (Risk Adverse)

Auditors (Showing reports)

Clients (money makers, need to maintain reputation)



**7 Support**

7.1 Resources

7.2 Competence (in ORG, not only IS team)

7.3 Awareness

7.4 Communication

7.5 Documented Information

**Impt points:**

- Typical ORG of IS team

- IS awareness program = should be part of every ORG

- IS professional needs marketing skills, selling security to both internal + external stakeholders

**8 Operation**

8.1 Operational planning and control

8.2 IS risk assessment

8.3 IS risk treatment

**Impt points:**

- Risk assessment = fundamental discipline of ISMS

- Different ways to perform risk assessment (choose 1 that is aligned to ORG’s risk management framewk)

- Different ways to treat risks

- Accept risk = perfectly acceptable

- Project/Vendor/M&A/App/Sys/Product = all shld be part of security program

- Determine controls that mitigate risks (then compare with Annex A – Statement of Applicability )

**9 Performance EVAL**

9.1 Monitoring/measurement/analysis/evaluation

9.2 Internal Audit

9.3 Management Review

**Impt points:**

- define effective KPI + KRI (impt, but very hard)

- good Qn = how do you know if it has not worked?

- assurance program = help with monitoring + eval

- Uds ORG’s 3 lines of defence model

- Proactively seeking management feedback, and provide regular information

**10 Improvement**

10.1 Noncomformity (testing/IA) and corrective action

10.2 Continual Improvement

**Impt points:**

- incident management = ensure root cause is analysed and feedback to ISMS

- exercise X times

**Annex A = Ref. Control Objectives + Controls (27002)**

**ISO 27002**

**=** code of practice for IS controls

- best practice controls + implementation guidance

**Clause 5** = security policy

- provide management direction + support for IS (with business req. and laws + regulations)

**Security Policy**

- approved by management

- sets out org approach to manage IS objectives

(created by business strat, regulations, legislation, controls, current + projected IS threat env)

- published + communicated to employees + 3rd party

Contents

- define IS, obj, principles = guide IS activies

- assignment of gen + specific responsibility for ISM to define roles

- process to handle deviation + exception

**Topic Specific Policies (related to clause 6-18)**

- IS policy, supported by topic specific policies

- implementation of IS controls (meet target groups)

**Policy communication**

- in a way that is relevant, accessible, understandable

e.g. when in IS awareness, education, training

Need for policies

- useful for larger/complex org

- level of controls separated from implementing controls

- single/set of doc

Review = planned interval, significant change = adequate

Each policy = have owner = responsible for dev

Review = assess opp for improvement of policy

**Clause 6-18** = implementation advice + guidance   
(13 categories of controls)

- each clause = general class (set of control objectives)

- >=1 control(s) to meet objective

**Clause 6:** Org of IS

**6.1** Internal ORG (management framework of IS)

**6.1.1** IS roles + responsibilities (defined + allocated)

- for protecting assets + security processes

- for security risk management + accept residual risk

- can delegate, but still accountable

- indiv responsibility = specified, competent

- authorisation levels should be documented

- oversight of security in supplier relationship = doc

**6.1.2** Segregation of duties (conflicting, reduce opp for mod/misuse of ORG assets)

- no 1 person, should RW assets without authorisation/detection

- event initiation SEPARATE authorization

- Collusion = possible

- small ORG = segregate = hard (use logging)

**6.1.3** Contact with authorities

**6.1.4** Contact with special interest group

**6.1.5** IS in project management

**6.2** mobile device + teleworking (security + usage)

Controls = mobile device policy (supporting security measures); teleworking policy

**Clause 7:** HR Security

Objectives = prior to employment, during employment, termination/change of employment

(in module 8, staff management)

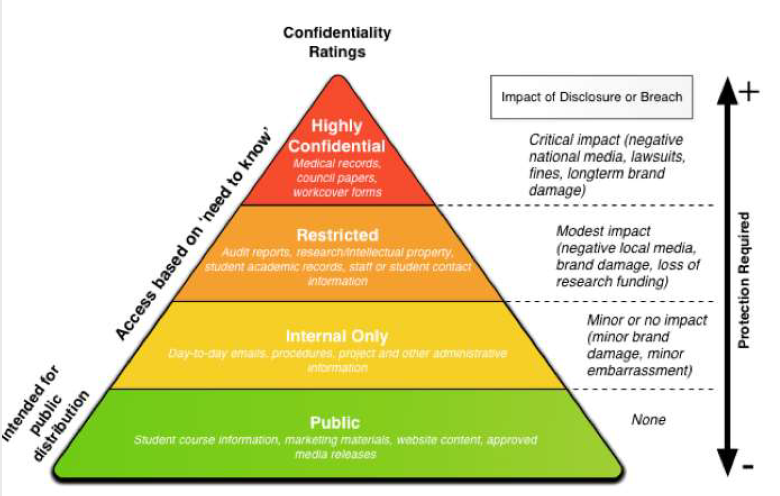
**Clause 8:**  Asset Management

Objectives = 8.X; Controls=8.X.Y

**8.1** Responsibility

Controls = inventory, ownership, acceptable use return of assets

**8.2** Information classification

Controls = Classification, labelling, handling of assets

**8.3** Media handling

Controls = Management of removable media, disposal, physical media transfer

**8.3.2** Disposal

**Clause 9:** Access Control

Objectives = Business Req. for AC, User access management, user responsibilities, Sys + application AC

**9.1.1** AC policy

**9.1.2** Access to networks + network services

**9.2.1** User access management

**9.2.2** User access provisioning (with revoke)

**9.2.3** management of privilege access rights

**9.2.4** management of secret auth info of users (gen pw, secret keys)

**9.2.5** review of user access rights

**9.2.6** removal/adjust of access rights

Provisioning Entitlements = restrict access, monitor priv users, protect cred, enforce entitlements

**9.3.1** Use of secret auth info

**9.4.1** info access restriction

**9.4.2** secure logon procedures

**9.4.3** pw management sys

**9.4.4** use of priv utility program

**9.4.5** AC to program source code

**Clause 10:** Cryptography

Objectives = Crypto controls

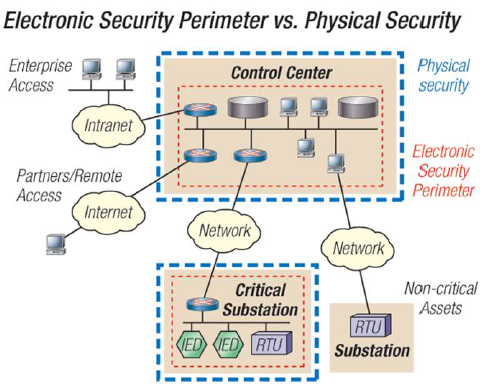
Controls = policy of usage, key management

Key mgmt. = Gen > Pre-activation > activation > expiration > post activation > escrow > destruction

**Clause 11**: Physical + env security

Obj = secure areas, equipment

Controls = physical sec perimeter, physical entry controls, securing offices+rooms+facilities, protect agst external/env threats, working in secure area, delivery+loading areas



11.2 Controls: Equipment sitting+protection, support utilities, cabling security, equipment maintenance, removal of assets, security of equipment and assets off-premise, secure disposal or reuse of equipment, unattended user equipment, clear desk/screen policy

Clause 12: Ops Security

Objectives = Ops procedures + responsibilities, malware protection, backup, logging + monitoring, control of ops software, tech vuln management, info sys audit considerations.

12.1 controls = documented operating procedures, change management, capacity management, separation of dev/test/ops env

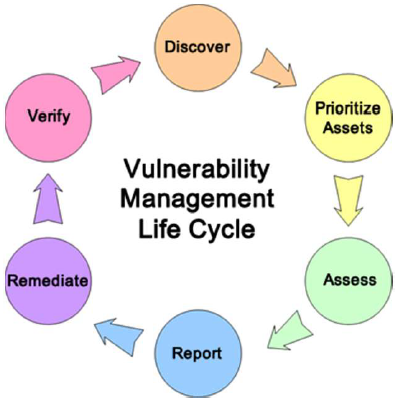
12.2 controls = controls against malware

12.3 controls = info/sw/sys backup   
(tested, follow policy)

12.4 controls = event logging, protection of log, admin+operator logs, clock synchro

12.5 controls = installation of sw on ops system

12.6 controls= mgmt. of tech vulns, restriction on sw installations



12.7 controls = info sys audit controls (verification of ops = planned, minimize disrupions)

**Clause 13:** Comms Security

Objectives = network security management, info trf

13.1 Controls = network controls, security of network services, segregation in networks

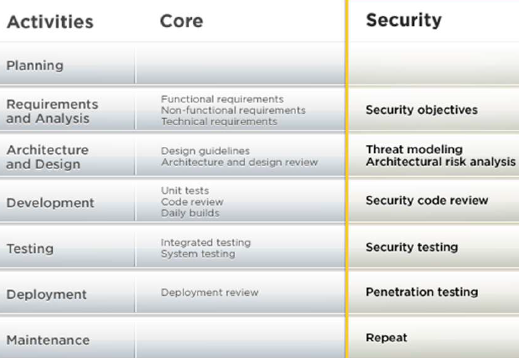
13.2 Controls = info trf policies and procedures, agreement on info trf, electronic msg, confidentiality on NDA

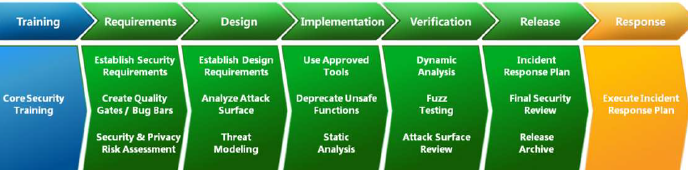
Clause 14: Sys acquisition, Dev, Maintenance

Obj = Security Req. of info sys, security in dev+support process, test data

14.1 Controls = IS req. analysis and specification, security app services on public network, protecting app services transactions

14.2 Controls = Secure dev policy, sys change control procedures, tech review of apps after operating platform, restrictions on changes to sw packages





14.2 controls = secure sys engineering principles, secure dev env, outsourced dev, system security testing, sys acceptance testing.

14.3 controls = protection of test data

Clause 15: supplier relationship

Objectives = IS in supplier relationship, supplier service delivery mgmt.

15.1 Controls = IS policy for supplier, addressing security within supplier agreements, info+comm tech supply chain

15.2 Controls = monitor + review of supplier services, managing changes to supplier services

Clause 16: IS incident management

Objectives = mgmt of IS incidents and improvements



Clause 17: Security aspect of BCP

Objectives: IS continuity, redundancy

Clause 18: Compliance

Objective: compliance with legal+contractual req., IS reviews

18.1 Controls = identification of applicable legislation + contractual req., intellectual property rights, protection of records, privacy + protection of PII, regulation of crypto controls.

18.2 Controls = independent review of IS, compliance of security policies + standard, technical compliance review

ISO27018 = PII controls

BG = cloud who process PII have to operate in way to allow service users to meet their legal/regulatory req. relating to PII. (legal contracts with customer) PII is different place to place (hard for cloud providers)

= Security controls implemented by CSP processing PII

Help CSP comply, enable CSP transparent, assist both CSP/cloud customer, help cloud customer to audit+ comply (impractical if each customer audit)

= offers supplementary implementation guide on security policies

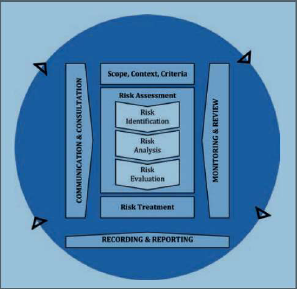
= helps 12.3.1 backup

**Risk Management 27005**

31000 = enterprise rise management (not IT/IS issue)

Follow steps: (iterative)

1. Comms + Consultation
2. Establish Context
3. Risk Assessment (identify, analyse, evaluate)
4. Risk Treatment
5. Monitor + review



**Assessing risks**

**- to manage, one have to assess and treat**

Includes: cost-benefit est, legal, stakeholder concerns

Should IDENTIFY, QUANTIFY, PRIORITIZE

**Guide management actions** to manage risk, select controls to address risk

Est risk = Risk analysis

Risk sigf. = Risk evaluation

Done PERIODICALLY (reproducible)

Needs clear scope

270005 = risk assessment, treat, acceptance, reporting, monitoring, review ATARMR

**Treating Risks**

Needs criteria for determining **acceptance** of risks

If low/ not cost effective = might accept

Actions:

1. Applying appropriate controls to reduce
   * **Needs selection and implementation**
2. Accept risk, (meet ORG criteria)
3. Avoid risk (not allowing action causing it)
4. Sharing the risk with other parties (insurers)

**Risk Assessment Actions**

1. Define and apply IS RA
2. Establish risk criteria
   * Risk acceptance criteria
   * Criteria for ISRA
3. Ensure RA give consistent + valid + comparable results
4. IDENTIFY security risk (loss of CIA, and owners)
5. Analyse IS Risk (consequences, likelihood, overall level of risk)
6. Evaluate IS Risk (Risk analysis with Risk criteria, prioritize)
7. Document ISRA process

**Risk Treatment Actions**

Define IS RT process

1. Select risk treatments, using RA results
2. Choose controls to implement RT
3. Compare controls and check nothing left out
4. Statement of Applicability (SoA) justify inclusion/exclusion
5. Formulate RT plan
6. Obtain risk owner approval of RT plan + acceptance of residual IS Risk
7. Document ISRT process

**27005:2018 ISRM**

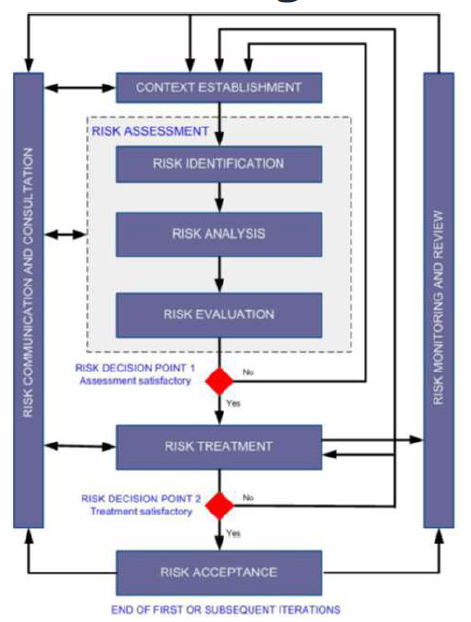
- Guideline, no specific method

Minor revision from 2011

Not accepted n UK, BS7799-3:2017

**Remarks**

* Systematic approach needed to identify security req
* Align with overall enterprise risk mgmt.
* Security Risk management integral to ISM
* Continual process



**Iterative process**

= increase depth/detail of assessment

= balance min effort in ID control, ensure High risk assessed

**Establish Context**

1. Setting the **Basic Criteria**
   1. Risk evaluation criteria (set Priority)
      1. Strategic value of business info
      2. Criticality
      3. Legal/regulatory
      4. Ops/business impt for CIA
      5. Stakeolder
   2. Impact criteria (degree of dmg/cost)
      1. Classification/breach/loss of business/disruption/dmg to reputation/legal
   3. Risk acceptance criteria (defined threshold)
      1. Ratio of est. profit
      2. vary on risk type (legal, not allowed)
      3. inc. req. for future additional treatment
2. Define **Scope and Boundaries**
   1. Ensure all assets covered by RA
   2. Info should be collected to determine ENV of ORG, relevance to ISRM
   3. Consider business/ORG struct/legal/assets/culture/expectations
3. Establish **appropriate ORG**

RA is conducted in the context

(info insufficient = iterate RA with new context)

Effectiveness of RT depends of results of RA

**Resourcing**

Should ensure resource avail

* To perform RA + RT plan
* Define+implement policies
* Monitor controls
* Monitor ISRM

**Risk Management ORG** = setup, with Roles

**Risk Treatment & Acceptance**

RT = cyclic process

* Assess a RT
* Decide residual risk = acceptable
* Assess effectiveness of treatment

RT may not immediately lead to acceptable.

Residual risk must be explicitly accepted

**Risk comms =** communicated to manager/ops staff

* Identified = valuable (may reduce dmg)
* Awareness = mitigate them, dealing with incidents/unexpected
* Significantly affect decisions

**Risk Assessment**

Risk should be IDENTIFY, QUANITY, QUALITATIVELY DESCRIBED + PRIORITISTED

Risk = effects X likelihood

Quantify/qualitatively describe = enables managers to prioritize

RA = Identification + Analysis + Evaluation

* Determine value of info assets
* Identify Threat + Vulns
* Identify controls + effects on risk
* Determine potential consequences
* Prioritize risks and rank them against risk evaluation criteria

>2 iterations

1st time = high level, next low level

ORG need select approach

**Risk Identification**

Determine what could happen (potential loss, gains insights, where/why loss might happen)

Risk = source under ORG control

Asset-threat-vuln approach (not the only way)

Assets within scope = identified

Assets = anything with value, requires protection

Sufficient info for RA

Lvl of detail = lvl of amount info collected

Asset owner (best person to value) should be identified = provde responsibility + accountability

**Threat Identification**

Potential to harm assets (info, process, sys)

Insider/Outsider

Identify generically and type

Input to threat identification + Likelihood est. (from list of ppl)

Consider Internal EXP + past threat assessments

Consult Threat catalogue to complete list

**Existing Controls Identification**

Avoid unnecessary cost

Working correctly (or else become vuln)

Possibility of control failure (may need more)

Consider Controls planned in RT and implemented

Existing controls MAY ineffective/insufficient/unjust

* (then have to remove/replace/remain)

Review doc, check with ppl, Onsite review, Audit Review

**Vulnerabilities Identification**

Vuln = exploitable to cause harm to assets/ORG

No harm itself, need threat to exploit

Might not need control, but need recognised

Poor implemented/malfunction control = vuln

Control (effective/ineffective) = env

Threat W/O vuln = not a risk

**Consequences Identification**

Those that losses CIA

Incident scenario

Impact determination (impact criteria)

Cost/Business Values (temp/perm)

**Risk Analysis**

* Criticality
* Extent of known vuln
* Prior incidents

Methodology = qualitative/quantitative

* Qualitative = general indication
  + (High medium low)
  + Ease of understanding
  + Scales to suit circumstances
  + Initial screening
  + Decision (numerical data inadequate)
* Quantitative = major risks

**Consequences Assessment**

* Business impact = result from security incident, taking account of consequences
* Asset Valuation (classification, criticality)
* Business impact value (qualitative/quantitative)

Value = determine from (replacement value, business consequences of damage to asset)

**Likelihood Assessment**

Qualitative/Quantitative

How often, how easily

* Experience + applicable statistics
* Deliberate threat source (motivation/capabilities/resources/attractiveness/vulnerability)
* Accidental (e.g. geo location)
* Vulns (indiv or added tgt)
* Existing controls, how effective

Need for accuracy, assets can be grouped/split

Determining lvl of risk = can consider other var

Est risk = combine likelihood + consequences

**Risk Evaluation**

Lvl of risk = compared to risk evaluation criteria + risk acceptance criteria (decided when doing context)

Based on acceptable of risk

Consequences/Likelihood/Degree of Confidence = should be consider

Aggregation of low+medium risks = much higher risk

Using UDS of risk by risk analysis = make decisions

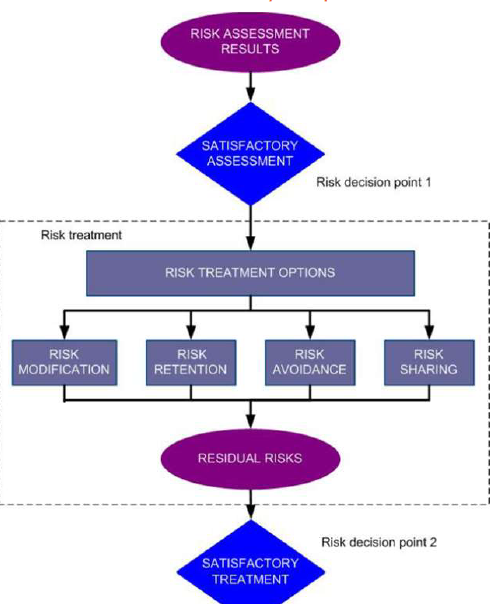
Decisions = activity undertaken? / priorities for RT

**Risk Treatment**

Controls selected + RT plan defined

4 options

* Risk modification
* Risk Retention (or acceptance)
* Risk Avoidance
* Risk Sharing



RT options based on :

**RA, expected costs, expected benefits**

Large reduction, low cost = implement control

Some = not economic, but judgement required

Adverse consequences of risk = as low as practicable (irrespective of absolute criteria)

Prioritize treatment

Some = can address multiple (e.g. IS training)

Risk Ranking + cost benefit analysis

Remove redundant/unnecessary controls = can save

**Risk Modification**

Use controls to meet needs

Cost/time/risk acceptance criteria/legal/contractual

Cost of control (acq, impl, admin, ops, mon, maintenance) VS value of assets

ROI in risk reduction + potential to exploit new business opportunities

Specialised skills may be needed to define + implement new controls

**Risk Acceptance**

Decision to retain risk without further action depend on risk evaluation

Level of risk = risk acceptance, no need to implement additional controls, risk retained.

Decision to accept risks, resp for decision = recorded

RT plan = reviewed/approved by mgmt.

Risk acceptance criteria = more than risk thresholds

Residual Risk may not meet Risk Acceptance Criteria (not address exact circumstances)

Suggest Risk Acceptance Criteria need revision

Need Exceptions

**Risk Avoidance**

Risks = too high/ or cost too high for RT

**Risk Sharing**

Shared to manage particular risk

Can create new risk

Can use insurance or subcontract

**Risk Factor Monitoring and Review**

* Risks + factors monitored + reviewed to identify change for complete risk pic
* Risks not static (Threats Vulns Likelihood Consequences change)
  + Can increase risk
  + Can be aggregated as well
* Constant monitoring = detect changes
* Remains relevant + appropriate

**Example: User PW Mgmt**

**Risk Probability Scale** = 0 (once in 100 year, 5 = once a year, 10 (once a month)

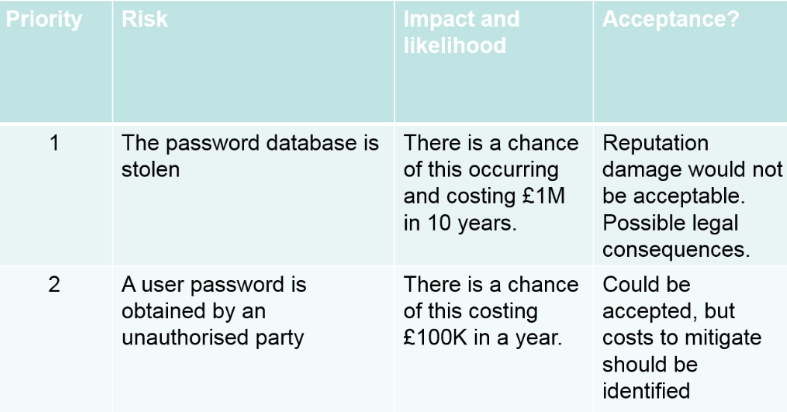
Risk lvl calc = Probability X impact (semi quantitative)

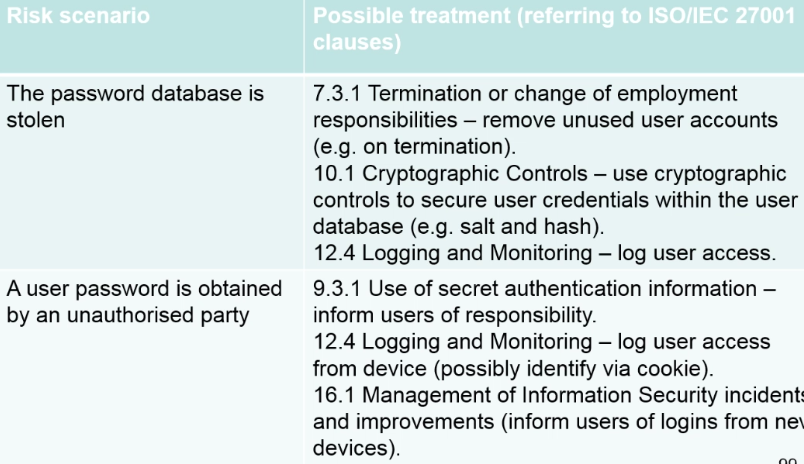
2 risks = pw obtained by unauthorized, pw db stolen

(can be threats, not risk)

2 diff companies can come out with 2 diff set of results (but main goal = must cover basics)







Most of 27005 = 6 annex (guidance and bg info)

Annex A = defining scope + boundaries of IS risk mgmt. process

Annex B = identification + valuation of assets + impact assess

Annex C = Examples of typical threats

Annex D = Vuln + methods for VA

Annex E = IS risk assessment approaches

Annex F = Constraints for risk modification

In Practice = adopt 1 of many commercial risk mgmt. methods (own measurement, tools, support, trng)

Open Group = standard + cert program (FAIR) for open + independent IS RA method

UK NCSC = collection of guidance on Risk mgmt + RA

27001 VS 27005

27001:2013 aligns with ISO31000:2018

31000, 27001 no need to ID infosec risk by ID of threat + vuln

BS7799-3 = 2 approaches

Scenario (Events/consequences -> then likelihood/severity)

asset-threat-vuln (info/data > threats/vuln that apply)

**Legal and Regulatory**

Privacy Mgmt != InfoSec Mgmt

Privacy is about what you collected from ppl, and how you manage it

security **supports/enables** privacy

Not serious for business, but employees can be jailed

privacy = what u can(not) do with certain info + consent  
Nothing to do with CIA

Rapid Change in law/regulations impacting ISM

Data privacy = change faster

Role of employee = key in ensure company comply

= might infringe law accidentally

Many Laws (in)direct impact in infosec mgmt.

More penalties financially/procedurally

Compliance burden = ^

**Types of Laws/Regulations:**

National (UK DataProtection Act, US SarbanesOxley )

Supranational (EU DataProtectionDirective, GDPR)

Industry Specific (PCI DSS)

Data Privacy Laws (GDPR, California <data breach notf>)

Corporate Controls/Auditing/Regulation

Surveillance + Monitoring (InvestigatoryPowerAct)

Export Control (Crypto)

Security Governance (EU Network + IS Directive)

**Highly Dynamic Env**

- ORG changing + evolving legal env

- Not security related, but impacts ISMS

- Legal req = inconsistent + conflicting

- danger = accidental violation of law + regulation

- tech changing (faster than regulators)

-> cloud, partnering, outsourcing, remote working, BYOD, IoT

**Privacy Law**

GDPR = major issue.

Likely = new litigation of offending companies

Privacy law = how PII collected/stored/managed/moved

**Cloud Impact**

Privacy law in EU = where PII located

Use of cloud, less of where

Issues in contract with cloud provider (security wise)

Swedish Gov Breach = exposed info of vehicle (police+military)   
PROBLEM = IT staff no security clearance

**Extra Territorial Issues**

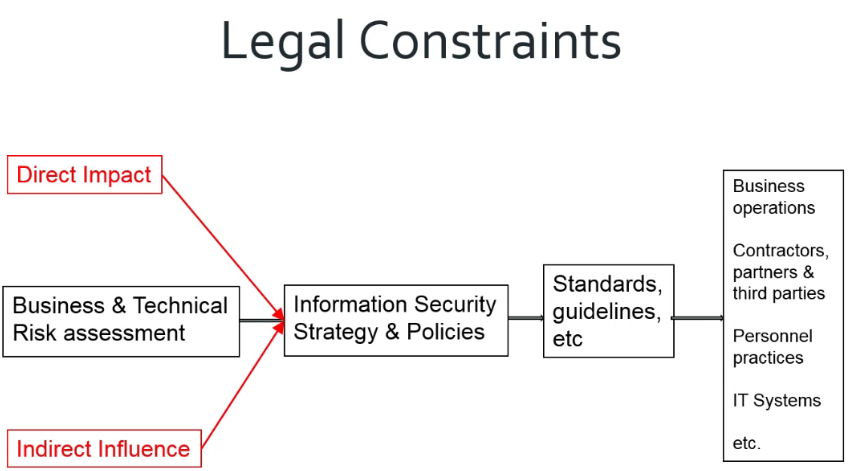
US DoJ wants MS data in Dublin (new Cloud Act = can get data easily)

FB = class actions in EU, trf of PII of EU citizens from EU to US

**IoT** = unregulated = major consumer threat

- internet kettle reveal wifi pw

- dish washer with vulnerable embedded web server



**Type of laws:**

Each jurisdiction = own range of legal instruments

Europe:

Council of Europe Conventions => EU Decisions => EU Regulations (need to convert) => EU Directives (nation need to implement law)

**Problem with laws:**

Natural language = open to interpretation

Not easy to uds

Potentially inconsistent (internally, with other law)

Lack of precision = lvl of control required to meet law

* ORG decide what is necessary
* “likely to”, “high risk” = vague

UK ICO published guide to GDPR

Privacy Impact Assessments = Mandatory in CERTAIN

50 pg guide on when PIA required/involved in

39 pg guide on Consent

**Jurisdiction issues**

Country right to intervene (if behaviour of company/indiv outside border)

* Legal expert = if u operate in the country, need to comply, since u enjoy protection of law
* “Doing business in territory” = ?
* “Need to subject to other country law, just by doing some business there” = ?

**Civil Law (as well)**, US trf IS risks to customer unfairly

Privacy Law

Big Picture = ORG need protect PII, ORG sensitive data

PII subject to legal safeguards

* extra-territorial
* mandatory breach reporting = ^ common

HOW to store data = policy, not security, how technically (CIA) = put security requirements

Security breach = usually PII breach = privacy issues = law issue, or corp regulations, or civil

Commercial Info = rarely direct legal protection, use criminal breach (IPR, copyright, unauthorized access)

* Criminal market in stolen data
* ORG need to prepare/prevent data lass

UK personal data protection (1984) = Basic CIA

EU Data Protection Directive 1995 = similar to 1954, 1980 OECD + processing of PII

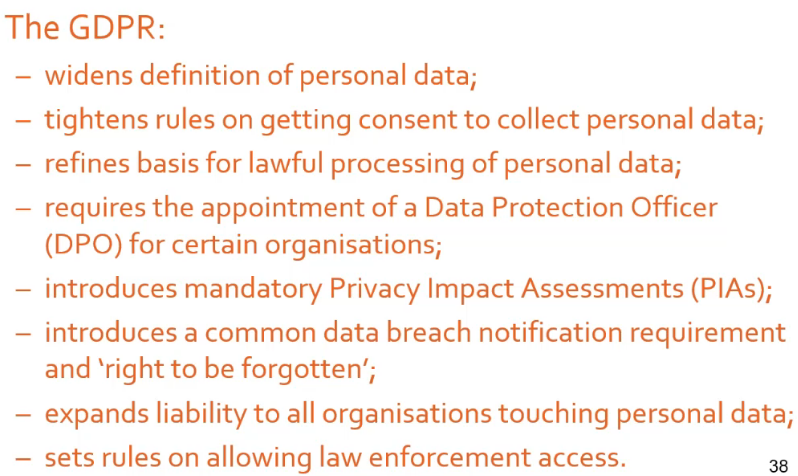
* Notice, Purpose, Consent, Security, Disclosure, Access, Accountability

Data Protection Act 1998 (implement directive)

*But some country is softer, hence GDPR*

**GDPR** replaces 1998 Data Protection Act

* By May 2018
* Parts open for interpretation
* Stiff Penalties = 20 Mil or 4% turnover (larger)
* ORG responsible (wherever data stored)



International Situation = Inconsistent privacy rules

* National = widespread + inconsistent
* Cross border initiatives
  + EU Privacy Shield (replace safe harbour)
  + EU binding corporate rules (standard contracts clauses)
  + APEC Cross Border Privacy Rules
* Implemented variously thru legal/regulatory/standards/guidance docs at nation/state/industry

**Trends**

National law/regulation = ^ common

PII definition broader

More extraterritorial (DP laws protect my citizens, need to be in my country)

USER = greater control

Mandate encryption = portable/media/remote/health

**Data Protection Failures**

Equifax breach = 143 mil

Exploited vuln on website, access PII (social security, DOB, Addr) on May – July 2017

Breach = bad, FOLLOWUP = worse

2007 HMRC = 25 mil ppl identity theft, 2 child benefit CD gone

Risk mgmt procedure failure + human error = blame

* Hard to relate role + responsibilities of senior mgmt to accountability
* Data sec policy avail, no staff read

**Financial GOV**

US

= Sarbanes-Oxley (SOX), Dodd-Frank, Gramm-Leach-Bliley, HIPAA (health)

UK

= UK companies (audit, investigations, community enterprises) Act, UK Turnbull (internal control, risk mgmt.), Basel III (Control of OPS risk)

SOX = CIA establish, documented, communicated to all, IT-Risk Assessment merge with Company RA

Interaction with 3rd parties (like outsource, partnership, supplier, crossborder systems, terms for employees)

* Business process conformance with local laws
* R/L with 3rd parties
* Agreement on each party legal responsibilities
* Knowledge where/how secure data

To check

* Audit security capability (maturity of controls, security expertise/service/support, data)
* Define security aspects of contracts (infosec obligations, security policy params, influence on ops, legal responsibility)
* Degree of rigour = how critical 3rd party is

**EU NIS Directive**

1st piece of EU legislation on cybersecurity

Intent = bring cybersecurity capabilities = same lvl of dev across EU, ensure coop, exchange of info

July2016 = 21 months = local law, 6 months = ops

NIS REQ

* Member state needs CSIRT team, national NIS
* Strategic coop, exchange of info
* Businesses (essential) take appropriate security measure + notify serious incidents
* Key digital service provider = infosec + notify req

Legal Controls on Crypto

* On Import/export/use
* ORG = provide plaintext/keys
* Conflict national security + privacy
* Conflict with other laws
  + Encrypt req
  + law enforcement access rights
  + controls on import/export use of crypto
* ORG need policy on crypto + key mgmt.

Law Enforcement Access

* Crypto widely use
* Law enforcement = wants plaintext

(countries have legal process)

(demands for keys where justified/informal)

* Req = influence use of product/services

(Apple imessage and US DoJ)

* Huge variants of legal rights of access (UK: PACE Act, IP Act, ATCS Act, Terrorism Act)
* Procedures required to manage access
* ORG need formality manage the grant of access
* ORG need to uds legal constraints (Extraterritorial)
* In UK, law enforcement = police, trading standards, health+safety, HMRC, InfoCommO

Data Discovery + Retention

* Legal request can include all info
  + Email, doc, video, blogs, servers, …
* ORG need to conform with legal for retention + discovery
  + Conflict between jurisdiction
  + Conflict between law (vs privacy)
* Requires proper “Chain of custody” if used as evidence
* Needs clear policy (archive security, info about 3rd party, delete non-relevant info, not tampered, employees uds)
* All relevant contracts = with security clause
* Info can held outside control (email)
* IMPT = diff between backup + archive
* 98% of lawyers = ediscovery = impt

**Employee Monitoring**  
- must be solely for business (training, QC, regulatory checks, investigation, security, effectiveness)

- UK ICO = employee’s right to privacy

- All effort required to inform all persons affect

- NO automatic right of monitoring, or privacy

(balance btwn employee/employer needs)  
(monitor = possible, employers must uds legal)

- GAP between law and tech/social media at work

- Tech ^ = employees have access to mobile/socia media (e.g. leaking of confidential info, security/privacy)

**Computer Misuse**

- Criminal Offence in many countries

(unauthorised access, alteration, destruction), penalties increased

- “Unauthorised” = exceeding authority (knowing it was unauthorised)

- Delegation of authority = major issue (need formal documentation, concern with external ppl/ORG)

- ORG = Acceptable Use policy (what is ok and not)

(all devices, pw sharing, right to monitor, user accept responsibility, prosecuting internal misuse)

- Computer misuse = seen as not a real crime

**Electronic Signature**

* ^ pressure to use signed transactions
* Dig sig = liability defined, uds what is signed

EU Payment System Directives

* Regulates payment services, and payment providers
* Increase competition, participation in payment industry
* 2007 -> 2015, new rules, online/mobile payments, across EU safer

**Others**

Fraud, EU ecommerce, DRM, Sexual offences, Insurance req.

**Internal Control, Audit, Security**

Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

● Effectiveness and efficiency of operations;

● Reliability of financial reporting; and

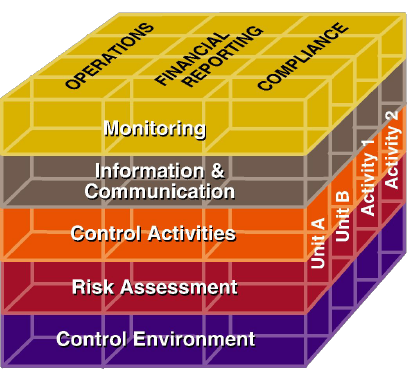
● Compliance with applicable laws and regulations.

Internal Control = **Process** -> Means to an end

Internal Control = effected by **PEOPLE** = not just policy manuals/forms, but ppl at every level of ORG

Expect to provide **REASONABLE assurance** (not absolute)

Achievement of **objectives** in 1or^ overlapping categories



**Control Environment**

1. ORG commitment to integrity + ethical values
2. Board of Directors DEMOSTRATES independence from mgmt, oversights for dev + perf of internal control
3. Mgmt establishes structures, reporting lines, appropriate authorities + responsibilities
4. Commit to attract/develop/retain competent indv
5. ORG holds indv accountable for internal control responsibilities

Risk Assessment

1. Specifies objective with clarity (to identify/assess risk)
2. Identifies risks when achieving objectives, and analyse risk managed
3. Potential for fraud
4. Identifies and assess changes could impact internal solution

**Control activities** (approval authorizations, verifications, reconciliations, reviews, security of assets, segregation)

1. Select and dev control activities (mitigate risk)
2. Select and dev general control activities over tech to support
3. Deploy control activities through policies. Establish what’s expected.

**Information and communication**

1. Obtain/Generates/Use quality info to support function
2. Internally communicate info
3. Externally communicate info

**Monitoring**

1. Select/dev/perform ongoing/separate evaluations if internal controls present+ functioning
2. Evaluate and communicates internal control deficiencies timely to senior mgmt.

Infosec => contribute to several components

* RA
* Control activities
* Monitoring

Principally relates to OPS (efficient + effective) rather than compliance/reporting

**Audit**

* Check of accounts, efficiency check

Audits provide third party assurance to various stakeholders that the subject matter is free from material misstatement.

Stakeholders = effectively eval + improve effectiveness of risk management, control, governance process over subject matter

Infosec audit

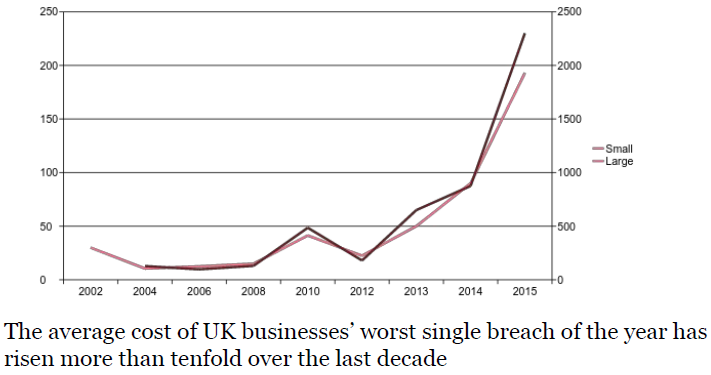
3 types that may apply

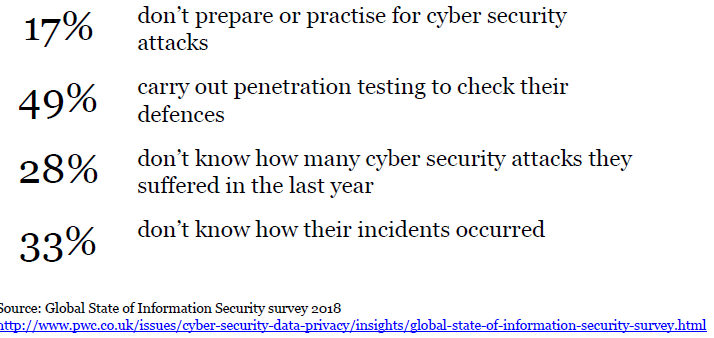
1. External financial audit – true+ fair view on information reported in financial statements, accountant independent from company
2. Internal audit – monitor which adequate internal control is in place, done by IA function of company
3. Security audit – monitor which security controls are in place, (internally/externally)

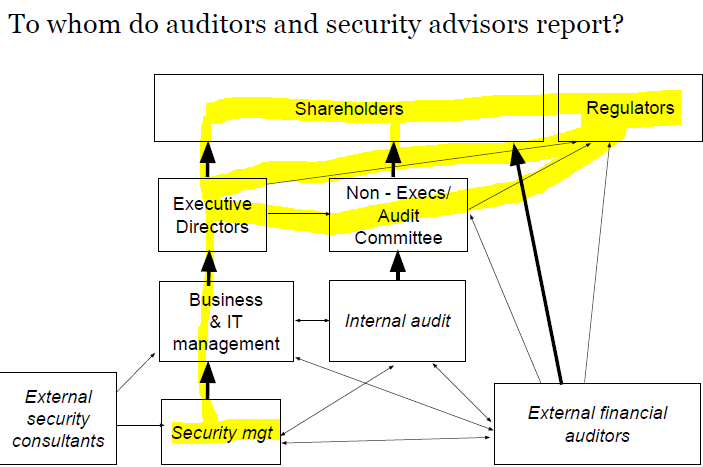
Why external financial audit involve security audit?

* If a big security breach could take company out
* Needs to do RA, and infosec risk is part of it
* Cost effective way to prove financial number
  + Reduce substantive testing
  + Check high volume, low value, check that the controls are satisfactory, and controls are working
* Infosec controls = enforce segregation of duties, reduce fraud
* Audit standards guide auditors to infosec risks

Infosec Risks Risks



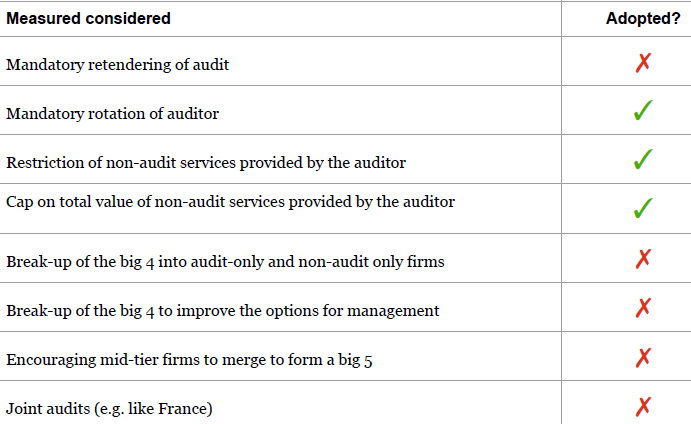


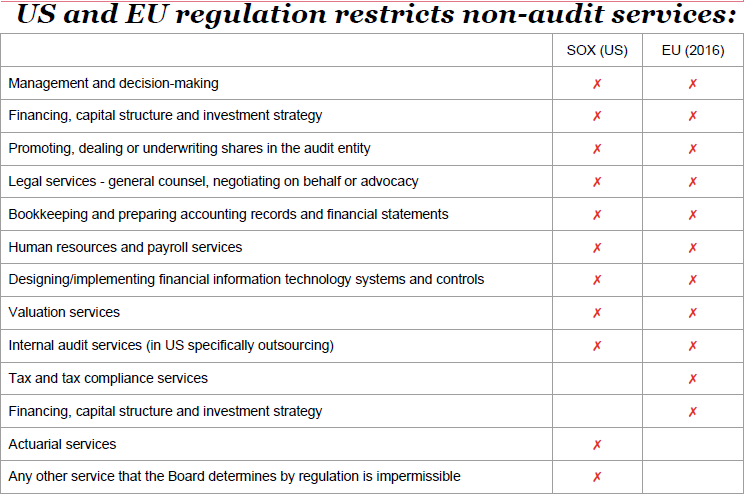


Non-execs/audit comm = check and balance, prevent execs from going rogue. No control, but liable

3 Big issues from regulatory

* Audit Quality
* Independence and Conflicts of interest
* Competition and Choice (potential audit companies to choose from)





FRC UK Ethical Standards

* Integrity
* Objectivity
* Independence

These would be compromised if an **objective, reasonable, informed 3rd party**  would conclude that the threats, arising from R/L, conditions, would impair integrity/objectivity would be inappropriate for firm to accept/continue the audit



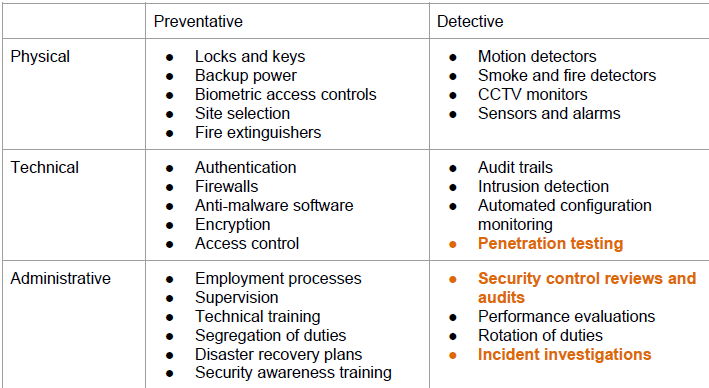
Management = acting as the management of the company to make decisions

Advocacy= Cannot support your client (in court of law)

Appropriate for external financial auditor to carry out security work?

* Know the business and management well
* Can provide legal, expertise, technical
* Can translate technical into business speak
* Excessive fees
* Must not compromise independence
* Scope of work conflicts with auditor role

Effective checks/audits = integral to IS risk mgmt.



Security Control Reviews and Audits

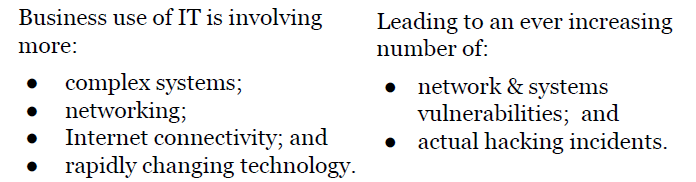
* Business process reviews
  + Completeness, accuracy, validity of transactions
  + Restricted access to assets and records
* IT Process reviews
  + Change control
  + Dev/implementation over new systems
  + Security and ops over env

Benefits

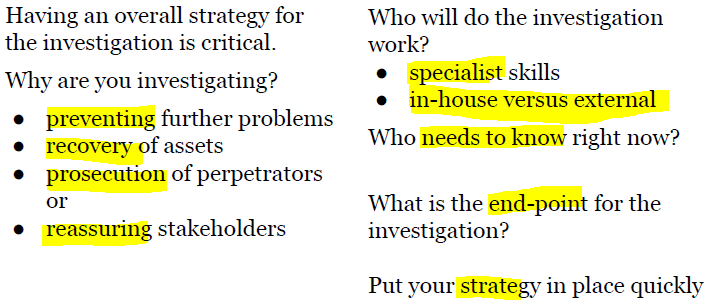
* Comparing with others (standard practice, externally, internally, mgmt assessment of risk)
* Test whether procedures followed
* Report technical issues to mgmt. (so they can uds and address)

Pentesting = ethical hacking, attack and vuln analysis

Why?



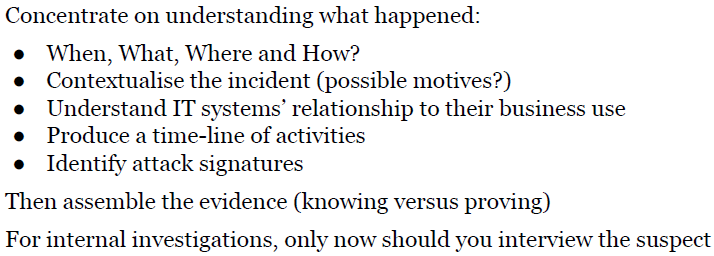
**Security incident response**



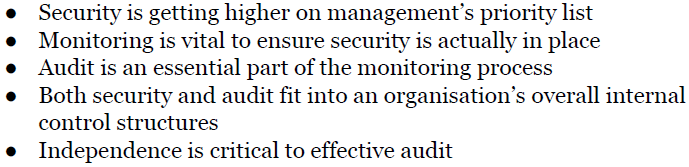
**Evidence source**



**Investigating**



**Summary**



**Incident Management and disaster recovery**

**Information security event:**

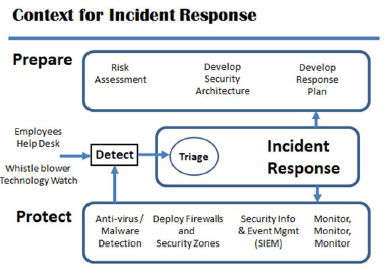
‘identified occurrence of system/service/network, possible breach of IS policy, or failure of control, previously unknown security situation.

**Information security incident: (more serious)**

Series of unwanted/unexpected Infosec event, sig. probability of compromising business ops, threatens infosec

**Infosec mgmt:**

Set of processes for detecting, reporting, assessing, responding, dealing, learning from infosec incidents



When Business Ops, regardless of the security controls in place, security incidents (affects CIA) happen. -> have plans in place to prep (after=ineffective)

**Planning:** tested IR plan, like insurance policy

Too late to do it after incident

TOP priority = recognize incident + who to report

(Awarness, learning site, exercises)

IR management

* Reporting
* Investigation
* Assessment
* Correction Actions
* Review

Incident Report form: contain details

* Actions after report need to be logged

IR team

* Needs to be briefed/prepared
* Come from ORG (breath of knowledge to deal effectively)
* Senior + experienced = authority to decide
* Can request more resources(in/ex)ternal
* **Escalation**
* Everyone has copy of IR plan documentation, contactable
* Documented process = IRT can reach ORG

**IR Procedures**

* IR procedure = broad, (cos u cant predict nature of event)
* Likely event = look at risks identified (probability/impact)

**Law Enforcement**

* Contact if likely to be criminal
* Impt = legal req. for reporting events
* UK mandatory to inform police if (terrorist/childporn/suspicious finance)

ISO/IEC 27002: Clause 16 = IS incident mgmt.

* To ensure a consistent + effective approach to infosec incident mgmt., including security events + weakness

All controls not mandatory (but consider)

MGMT respon. + procedures = established to ensure quick/effective/orderly response to IS incidents

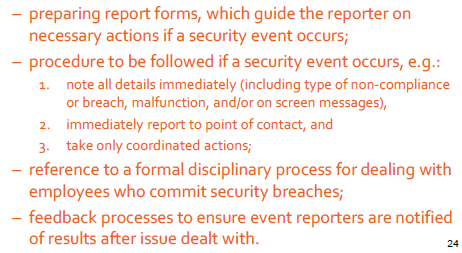
MGMT response established for defining and implement procedures for:



Scope of procedures:

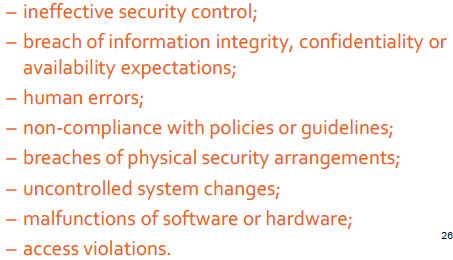
* Competent personnel (handle isssues to infosec incidentS)
* Point of contact = infosec incident detection/reporting
* Appro. Contacts with authorities/3rd party

Reporting procedures includes:



* Infosec events **= reported thru appropriate mgmt channels ASAP**
* Employees/contracts NEED to report infosec events ASAP
* AWARE of procedure for sec events, OOC

Situations requiring reporting =



Reporting security weakness

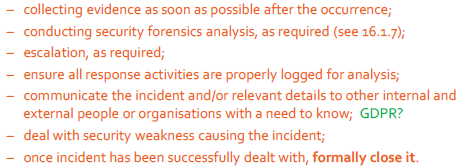
* Everyone should report ASAP to prevent infosec incidents
* Should be easy/accessible/avail – danger of getting intercepted (can be exploited)

Assessment of security events

* Assessed to see if it’s incident
* POC assess each event using classification scale (& what to do & impact/extent)
* ISIRT = can be sent for confirm/reassess
* Result/assessment/decision = recorded (for future ref. & verification)

Response to security incident

* Responded in accordance to documented procedures
* Includes:



* Post-incident analysis = identify source

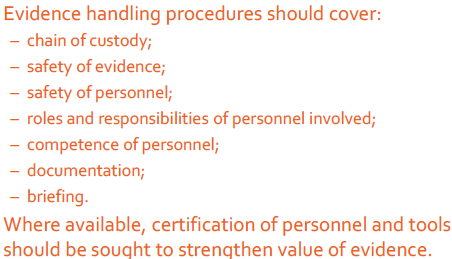
Learning from sec inc:

* Knowledge gained = reduce likelihood/impact
* Mech in place to quanify/monitor types/volumes/costs of infosec inc.
* Info gained = eval sec incident identify recurring/high impact incidents

Collection of evidence

* ORG define & apply procedure for identification/collection/acquisition/preservation of info (evidence)

Internal proc = (handle evid. for disciplinary/legal)



ISO/IEC 27035: Infosec incident mgmt.

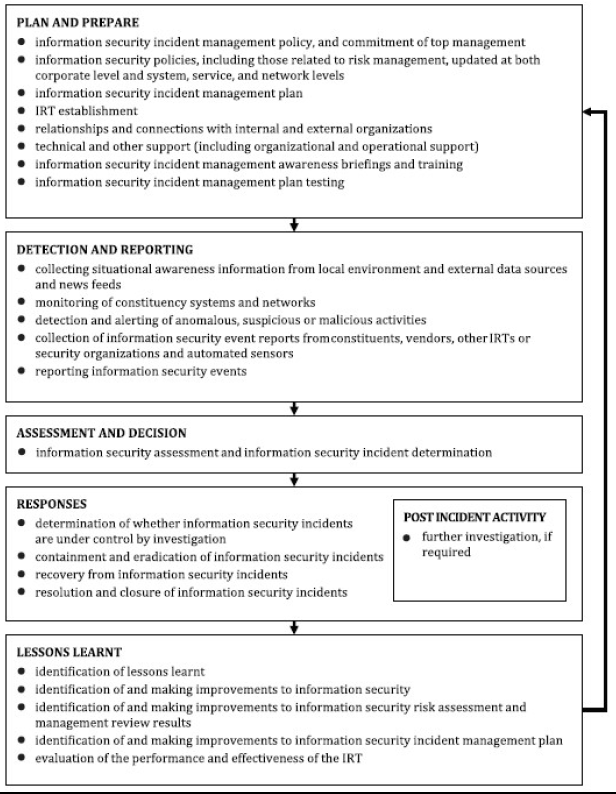
(now = 2 part, will be 3 part)

3rd = Guideline for IR ops

1st = notion of infosec incident mgmt, model

**Phases**

1. Plan and prepare
2. Detection & reporting
3. Assessment & decision
4. Responses
5. Lessons learnt



2nd = PLAN + PREPARE for IR

* Dev of guidelines to ^ confidence in Org readiness to respond

BC = can continue operating after major inc/disaster

* Can outsource to service provider
* Backup = part of BCP

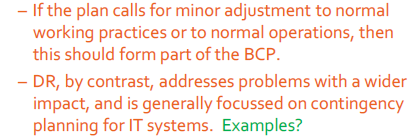
BCP = maintaining BC

* problem still happens, problems affect ops
* can be serious (power failure)
* can be better if tried/tested plan in place

DR = major, normal ops = damaged/disrupted

* most serious problem
* key = risk assessment (some so unlucky = not worth planning)

BCP vs DR

* SCALE of steps involved
* 
* Magnitude of financial consequences

Example

* Main = loss of service, ensure all records are backup offsite, no need complex DR plan
* ORG = rapid cash turnover, main = loss of finance

OPS env of ORG = impt factor

Developing plans:

1. Complete RA, consider unlikely events
2. Consider possible impacts (cause not impt, impact & likelihood)
3. Address major eventualities
4. Mgmt decides which parts of DR
5. Size of problem, duration, operational impact

How far = plan?

* Scope = not obvious
* Plan not far enough sometimes (months no access, due to bomb scare)

Lack of access = MAJOR issue overlooked

* Problem outside of ORG, cordoned off
* How to address in BCP?

Need for planning

* Requires detailed + careful planning
* A document !enough
* Awareness + education prgm = staff aware and importance

Documentation and availability

* Doc = vital, documenting expected actions + procedures = not enough, needs to be available
* If put in office, no access to office = GG
* Readily available, kept secure, (sensitive info)

Outsourcing DR = a lot more, easy with cloud

Testing = everything needs to test, with different testing strategies (full enactment)

A lot of backup fail when used

ISO/IEC: 27002:17 : Info Sec aspects of BCM

2 controls

1. Infosec continuity EMBED in ORG’s BCM
2. Info processing facs implemented with redundancy sufficient to meet avail

Is BCM/DR part of ISMS

Planning infosec continuity

3 controls

1. Planning Infosec continuity
2. Implementing infosec continuity
3. Verify, review, eval info sec continuity

1 planning info sec continuity

* ORG should determine **REQUIREMENTS** for continuity in adverse
* Check if it’s inside BCP/DR (should be inside)

2 Implementing

* Establish, doc, implement, maintain procedures and controls to ensure required level of continuity in adverse situation
* ENSURE:
  + Mgmt. struct in place (mitigate and respond)
  + IRT with necessary responsibility/authority/competence
  + Documented plans/response/recovery dev + approved
* Technical
  + Security controls
  + Processes
  + Compensating controls (cannot be maintained during adverse)

3 Verify, review, eval continuity

* ORG should VERIFY it works
* Org/tech/procedural/process changes = lead to change in infosec
* Verify by testing everything

17.2 Redundancy = 1 control

Info processing facs implemented with redundancy sufficient to meet availability

* Cannot guaranteed, redundant component/architecture considered
* Should be tested

**PART 8: STAFF MGMT**

Recruitment

= nature of task, necessary to vet staff before employment (for high sensitive tasks)

* Vetting = history + criminal record checks
* Contracted to 3rd party specialist

Security culture

* Attitude towards work/employees
* Care about if things works
* Aware of danger (positive security culture)
* ISMS fails if security culture is poor

DEV a security culture = VERY TOP

* Signed by CEO, needs to exist
* Statement not enough
* Mgmt. needs to lead by example, if mgmt. ignores rules = so will everyone
* >50% caused by inappropriate actions by staff (accident>deliberate)
* Effective security culture = reduce number of incidents

Security Awarness

* Vital component of security culture
* Staff UDS real threats
* Part of staff induction
* Include laws/regulations
* Include real life examples
* Not such C, IA as well
* Records of who is trained and when…
* Evidence of due diligence (legal)

Employment contract

* Impt = legal status
* Defines terms/conditions/responsibilities/obligations

Key areas

* Acceptable standards
* Ownership of IP
* Use of corporate assets
* Grounds of Disciplinary
* Adherence to laws/regulations
* Duty of care
* NDA

Service Contracts (3rd party)

* Commit to nature of service (including policies/procedures)
* Commit to meet perf levels (guarantees)
* Contracts = share risk = provision for compensation (if fail)

Codes of Conduct (for infosec CIA)

* Also ethics (like gifts, and offering gift)

Acceptable use policies

* How employees an use ORG info/sys
* Part of employment
* ORG accountable for employee’s action (reduce liability)
* Protect staff from harassment/malpractice
* Specify Level of seriousness

Segregation of duties

* Divide authority = perform sensitive tasks
* Prevent too much power on 1 user
* Prevent over-dependence on 1 user
* Risk to ORG & INDVi
* Manage risk of collusion & fraud

Separate sys admin/user/auditor/dev/test/ops

* Regulations might require time

3rd Party Suppliers

* Obligations to keep personal data confidential (and accurate) = accounted when subcontracting
* Needs to include and ensure legal obligations
* Risk sharing.

User Auth = why?

* Access to resources = CIA
* All users must have individual accounts
* Robust method of user auth
* Ensure user ACCOUNTABILITY (ppl are held responsible for actions), needs correlate to user

HOW?

* PW (known shortcomings)
* Others = tokens/biometric
* 2fa

Identification VS auth

* Act of learning a claimed identifier
* Act of verifying that person claiming identifier is its owner
* Username = identification, pw = authentication
* Biometrics =? Both ?

Authorization

* AKA access control,
* Means of limited rights of users to perform actions, based on identity
* OS implement access control to permit access to files/apps to be controlled
* RBAC (or indiv apps) implement access control

Access control administration:

* Permissions needs to be managed,
* Time consuming + often neglected

(when users leave)

Data classification (paper/electronic)

* All requires protection (given value based on RA)
* Classification that needs a mark (hard to remove)
* Secret/confidential…

Rules

* Needed to govern how doc handled at each lvl
* Each lvl = corresponding dmg (if disclosed)
* Highly confidential = kept in safes, distr limited

Security Training

* Anyone needs comply with infosec policy/procedures
* Helps indiv uds security responsibilities
* How ORG can be put at risk (Y is it impt?)
* Rules/how can be avoided

Lvl of training = lvl of access to corporate info

* Can carry out security procedures, uds how to use securely
* Coverage of acceptable use policy

Content = consistent with enterprise goals

* What need to know? Y?
* What is the current uds? What else after trg?

(implementation != as designed)

Approaches to training

* Specific infosec trg   
  *(goal = increase competency in specific area)*
* Raising awareness of infosec

*(aim to change user behaviour, influence perception of risk)*

HR Security

* Prior to employment
  + Screening (Bg check – verify with accord laws/regulations/ethics)

- avail of good char ref  
- confirm of qualificaton  
- independent identity verify (Passpo)

- credit/criminal

* + Terms + conditions of employment

(ORG’s respon for infosec)

- NDA, responsibilities  
- actions taken (if not comply)

* During employment
  + Mgmt Responsibilities

(briefed, guidelines, motivated to fulfil sec policies, infosec awareness, conform to terms, have appro skills, educated, anon whistleblower chnl)

* + Info Sec awareness/edu/trg

Account employees’ roles

* + Disciplinary  
    start checking after infosec breach, should be fair, allows responses based on impact/ first offence / trained ?

- used as deterrent

* Termination/Change of employment – infosec resp. and duties still valid (defined, communicated to employees/contracted + enforced)

ISO27002 – CLAUSE 9 (relevant)

* User access mgmt.
  + User access mgmt., provisioning
  + Mgmt. of privileged access right
  + Mgmt. of secret auth info (pw)
  + Review of user access rights
  + Removal/adjustment of access rights
* User responsibilities
  + Use of secret auth info

**Procedural Issues**

Procedure = established/official of doing smt, series of action conducted in a certain order/manner

In ORG = many procedures (un)written

Y document procedure?

InfoSec Procedures

* Creation/Storage/modification/Processing/Deleting
* Info processing mgmt.

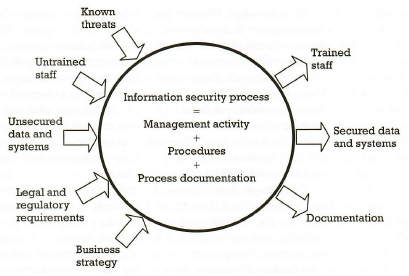
E.g. Backup, new release, incidents, new user, sys config, procedures for access mgmt

Procedures = TYPE OF CONTROL

* Some will be how to use other controls
* Not security related = but huge impact for security

Major of ISMS = processes

* Processes = transform inputs (untrained staffs) to outputs (trained staff)
* Key processes= documented



Getting it right!

* BALANCE with usability + security
* Lvl of doc = risk + difficulty
* Unreadable != used

ISO27002, 12.1 = ensure correct + secure ops of info processing facilities

12.1.1 = documented operating procedures (com startup, shutdown, backup, maintenance, media handling, computer room, mail handling)

Some OPS = delicate! (not perform correct = not objectives met) = need documented right

* Backup wrong, critical data not copied, = vuln
* Incorrect Access control =inappropriate access

Correctness = covers all (most impt tasks) (when + who?)

Consistency + recording = (still correct/consistent when performed by another staff)

* What records needs to be kept (e.g. logs)

Accountability

* impt ops done by appr staff
* segregation of duties
* appropriate records are kept (who? when?)

Contents of procedures

* precise = corporate standards, style of authors, **skillsets of audience (to be usable)**
* list of roles, segregation of duties, equip/data needed, **SEQUENCE OF STEPS** to carry out, what to record

Importance = highlight importance of defined roles + responsibilities in ORG (sec sensitive ops by authorised staff)

ISO27002 clause 6 = ORG of info sec

* establish a mgmt. framework to initiate and control implementation and ops of infosec

6.1.1 = info sec roles and responsibilities

- who accept residual risk

- delegation of security task (but still accountable, and needs to ensure correctly performed)

- indiv responsibilities = specified

6.1.2 = segregation of duties

- no 1 person can access/modify/use assets without authorisation/detection

- event inititation SEPARATE from authorisation

- collusion possibility (when design)

- small org hard, then use other controls (monitoring/logging/supervision)

Example (Backup)

* important = preserve availability of info
* can use a lot of ways (cloud)
* roles involved = chosen carefully
* freq, timing, scope = specified

1. obtain storage media
2. selecting data
3. copying data to storage media
4. appropriate protection to data (enc/integrity)
5. store in remote site (with physical sec)

* req. to record details of backup

(name, datetime, problems, identifiers of media)

Other procedures = (restoring, audit, checking)

Obligation to delete PII? But impossible to delete, impossible to find out

Example (Production Signoff)  
- new version of software, sign off by person  
- authorisation culmination of checks (in procedures)

(extensively tested)

1. successfully tested
2. system documentation with rules
3. timing of release no conflict
4. record the authorization

Other possible procedures

* production testing/documentation/defects

Example (Staff induction)

- security critical for security recruitment

1. Correctness of major claims on CV

2. criminal checks

3. taking up references  
4. Sign of contract + acceptable use policy  
5. Staff induction training  
6. Corporate security policy  
7. Providing necessary access to info systems

Other related = staff termination/ disciplinary actions

Example (incident reporting)

- all IT staff = briefed on security incidents and procedures (to capture as much info as possible)

1. Date + time

2. describe incident as much details  
3. Describe any actions taken  
4. Name + contact details of reporter

ISM (in real world)

* basic methodology are the same
* security has no edges (crosses boundary)

Fundamentals

* infosec = (info is the flow of everything) = not an option, necessary
* Ecommerce = made it a consumer issue (once a security, now fundamental)
* Boundary blurred, external threats = likely, where’s the extended enterprise ends?
* History = use fear/uncertainty/doubt to do it (wont last long, must let them uds)
* Align with business, no free rides
* Not only protection, but cost+ops as well

Importance of Infosys = almost every relies on it

* Cant have sys failure/ info loss. (manual != feasible)

Changing = LAST time = centralised, remote access from known locations, only accessible to internal ppl.

Value of information = ? (increased now)

**WHY?**

Technology mech = part of solution

PPL , the ORG, procedures >= impt than the tech they support

PPL, PROCESS, TECH

Security = strongest as the weakest link

Proper ISM maybe be overlooked = weak link in the chain.

Not always external attacks! (accidental as well)

Good control != (always) working

Pure technologist = need to uds business context



**IT** vs **information** vs **Cyber**

Logical = IT sys

ORG security = Risk

Cyber = high end threat space

Good Infosec func = spans ALL to protect enterprise

Physical Security ?

* Just as impt as any other aspects
* Data theft (reputation, high profile, news)
* Loss of laptops
* Physical Security incident OR infosec event?
* Disk Transfers ?
* Loss of Media
* Removable Media (USB? Phone?)
* Alarm sys/sensors? – installed by external firms (outside of IT gov)
* Cameras (usage of bandwidth)
* Social Engineering (talk your way)

Who takes care?

* Cable room, comm rooms
* Unlocked, used for storage, no record keeping
* DoS waiting to happen

Theft (stealing of data?) Copying (but original copy is still there) – more difficult problem

- Stealing used to be depriving someone else of smt

Unauthorised Entry

* Robbery/burglary = crime
* Electronic world = evidence of intrusion = fw log, event log

Security Goals

* Adequate protection of ppl, financial, info, infra from deliberate/accidental dmg, disruption/loss/misuse

Guiding Principles

* Secure the business (not the secure tech)
* Matter of UDS-ing appetite for risk

Risk = Threat\*Vulnerabilties\*Impact (any = 0, risk = 0)

Threat = unwanted event = result in harm to asset, exploits >1 known vuln

Vulnerability = susceptibility of an asset to attack

Impact = magnitude of potential loss/seriousness of event

Assess Risk = not just threats

PROTECT business, not technology

Cost of Security

* Never get the funds you want
* Never be secure
* What is “SECURE” in context of business
* Pragmatic (sensibly, realistically)
* Know when compromise achieves nothing = waste money

Threat Landscape

* Virus = constant battle with new variants, rate of emergence = ^
* Worms = ^ problem (facilitate other atks, DDOS, identity theft)
* Spyware = who’s watching?
* APTs?

Identity Theft

* Impersonation
* Auth
* Verification
* Phishing/pharming
* Spoof websites
* Social engineering
* Multi channel approaches
* Physical forgeries
* Account takeover

DOS (esp DDOS)

* Multiple atk sites
* Unwitting accomplices who fail to secure own tech
* Defences rely on rapid filtering at boundaries and rapid reconfig
* Business = reliant on open networks
* Bandwidth helps, but for simple atks
  + More on filtration issues
  + Amplified atk = 100X atk capability
  + IOT as botnets

Threat actors

* Individuals
* Hacktivists (Ashley Madison)
* Criminals
* Competitors
* Intelligence Agencies
* Military Forces

Resistance to Cyber Crime

* Effective controls/ perimeter def = deflect majority of attempts to enter sys
* Strong access control, monitoring = contain insider malfeasance
* Cyber espionage, state actors = impossible to prevent

Nation States (China, Russia,…)

Cyber Crime Threat = no. of organised criminal and political atks ^ skills + sophiscation ^

Political volatility = use of cyber warfare

Threat is big enough for boardroom agenda for UK

APT = slow/patient attack

* Originated by Organized crime, state sponsor
* Variety of attack vectors
* Capabilities ! underest.
* Atks = persistent, remediated sys continue to be targeted
* Substantial resources (manpower/malware) in terms of atk sys, well versed in IT mgmt.



Shamoon = 30k computers useless, and needed replace

Exfiltrate data, and erase harddrive

* Copycat of Wiper

Real use of Cyber Warfare (Russian invasion of Georgia 2008)

* Took down banking and gov sites
* Take over TV, radio, newspaper
* Same kind of strategies

Infosec Function

* Policy and Gov
* Incident Mgmt (Investigation and Forensics)
* Consultancy (Advice/Assurance)
* Architecture & infra
* Awareness
* Operations

Corp Gov = means of which companies are directed/controlled

* Accountabilities of corporate boards and directors (performance/legal/ethical)
* Area of high visibility
* Major issue for regualtors
* Control + integrity = impact on security
* Legal + regulatory req = valuable tool for persuasion
* Which infosec is directed and controlled within a company
* Administrated via TOP level steering comm (not alone)
* CISO = assurance = both board+regulators

Assurance

* Compliance
* Audit + Controls Testing
* Board level issue (not in boardroom unless smt is wrong, expected to be done)

Policy

* Should not spell out the details
* High level, outlining resp.
* Mandatory, no dispute
* Derive from ISO27002

Standards

* How we do it
* Policy INTO reality
* Env or Tech
* Inherit the authority of policy
* Should permit a range of solution (appropriate to assessed risk)

Ownership

* Critical to ensure accountability of policy issues
* Identify owners (infra, apps, processes, info/data)
* IT don’t OWN everything

Guidelines

* Good Practice
* Not mandated
* May represent emerging tech (standards not there yet)
* Why waste time for alternative solution?

Procedures

* Add ORG controls to provide end=-to-end security for processes
* Nothing left to chance
* MUST inc installation, init, ops, support

Metrics

* Cant measure = Cant measure
* Metrics = not easy
* Most measure what they can RATHER what they need

Training & Awareness

* Security = everybody issue
* Failure to educate = weaken disciplinary/legal redress
* Increasingly it is necessary to educate public (phishing)

Incident Mgmt

* When (and Will?) sys are attacked
* IMPT to have processes to allow managed response
* Planning is preferable, Generic than specific
* Essential to keep SENIOR mgmt. by escalation process
* Investigation = needed (after incident, requires computer forensics)

Consultancy

* Assisting business + IT dep to interpret policy
* Uds threat and Vuln
* Centre of Excellence
* Mix of TECH + security analyst (speak both technical + business lang)

Conclusion

* Information = highly valuable asset + info processing sys = critical to business
* Information assets = effectively protected + risks = understood and managed
* Effective info sec != saying “No”
* No Magic Bullets
* One size no fit all
* Secure BUSINESS then tech
* Infosec evolves, infosec mgmt = needs to evolve

Failures And Mistakes

* Mistakes with Tech
* Mistakes with People
* Mistakes in Management

**Mistakes with Tech**

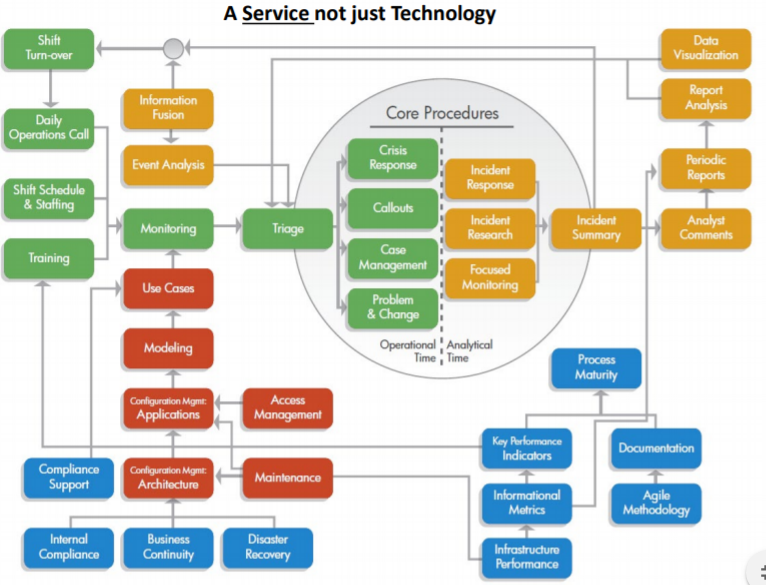
* Poor adoption
* No Service view
* Poor manageability
  + No tools/processes
  + Goals not achievable
  + Underestimated deployment effort

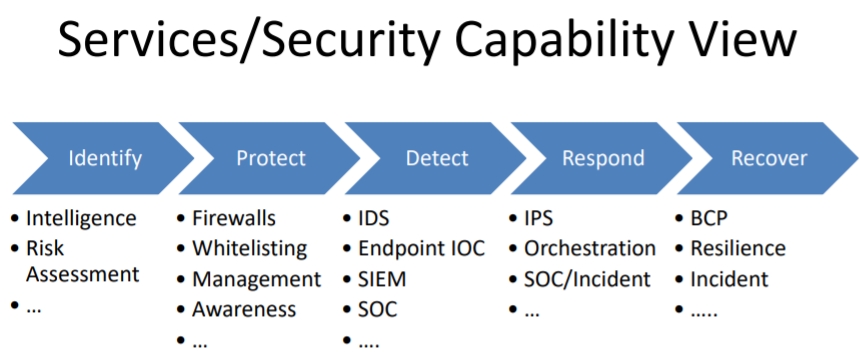
Shelfware = owning/license software you don’t actually need/use

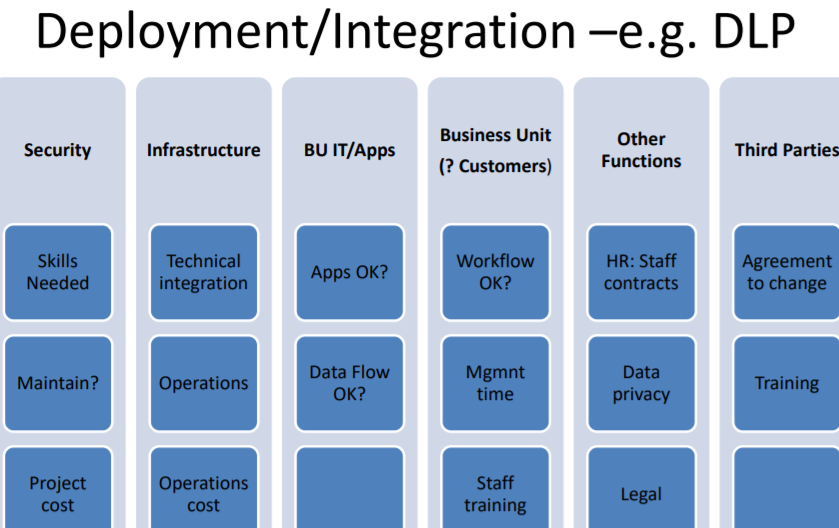
Finding the businesses unit (in a org)

* Those without money
* *Those with the greatest need – more risk (worst)*
* Those who follow corporate direction
* **Those who are friends – there’s trust**
* Those who don’t care (exec)

Technology is there







**Mistakes with People**

* Poor cultural understanding
* Bad approach to security awareness
* Underestimating the need for personal trust

**User Awareness**

Security Awareness or Cultural Change

* Dig -aware = Gen Y & Mill
* Users are not enemy
* Usability of security solutions
* Tools help the security aware
* Who reads policy books ?

Failures in info sharing

* Success factors
  + Trust in ppl who sharing
  + Value of info you are sharing
  + Effort needed to share
  + Rewards you expect from sharing

**Mistakes in Management**

* Communication & engagement
* Financial
* Expertise
* Programme
* Groupthink
  + Wrong scope/risk/solution

Engagement using technical jargon

Engagement using Fear, Uncertiainty, Doubt

Engagement using mgmt. analogies (prev)

Engagement using boardroom misunderstanding

* Ciso should sit on board?
* Ask the board for money?- board don’t allocate funds
* Inconsistent/confusing comm
  + Terms, diff presentation of risk/metrics

Risk decisions != common sense

Good Risk Mgmt != common sense

(Delphi Technique, Good workshop facilitation is essential)

**Poor Finance Planning**

* Failure to follow planning cycle
* Failure to warn others abt financial planning implications
* Poor project spending
* Investment budget but insufficient

Activity Based Costing Mistakes

* Pay for policy
  + Voluntary?
  + Taxation
  + Who benefits ?
* Pay for security services

Payment for policy /monitoring should not be voluntary

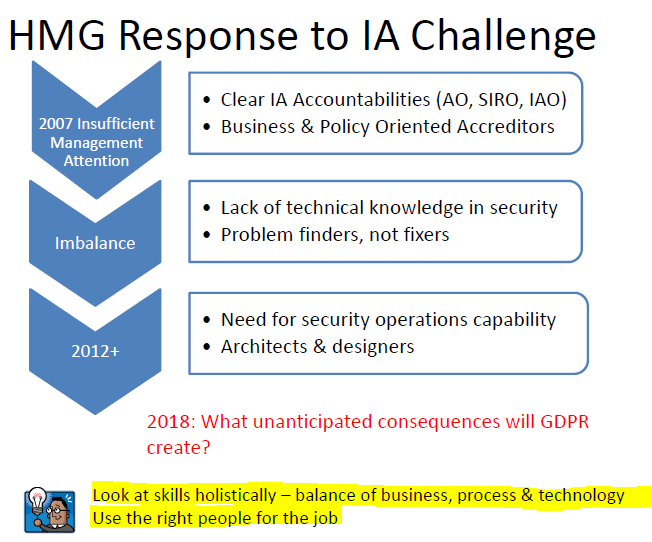
Wrong expertise

(not using professionals)

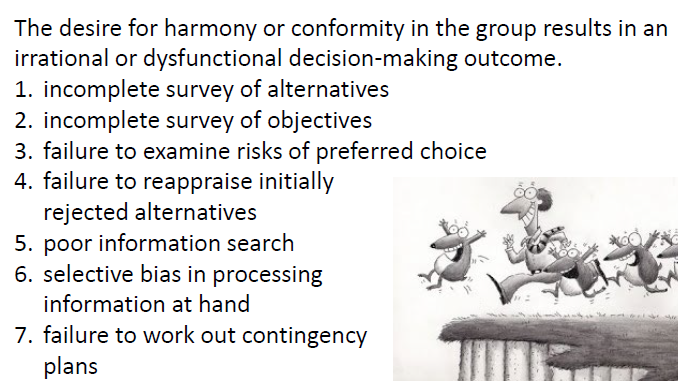
* Poor use of time
* Amateur comms
* News article lawyers

(lack of security knowledge)

* Experience of PCs at home
* Inflight magainze advice
* Out dated knowledge
* No external comparator
* Insufficient breadth of skills (policy > tech)



Group think



Sunk Costs

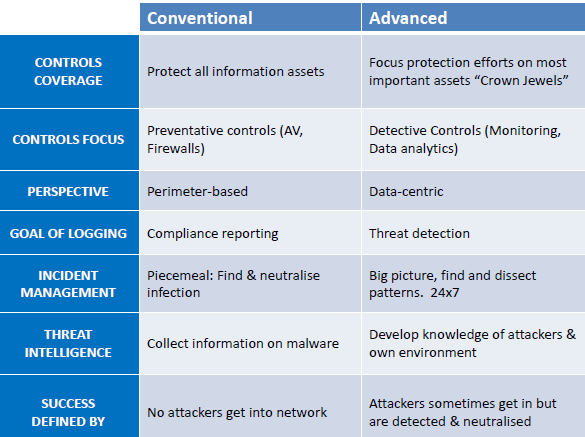
* Making choices in a way that justifies past/flawed choices

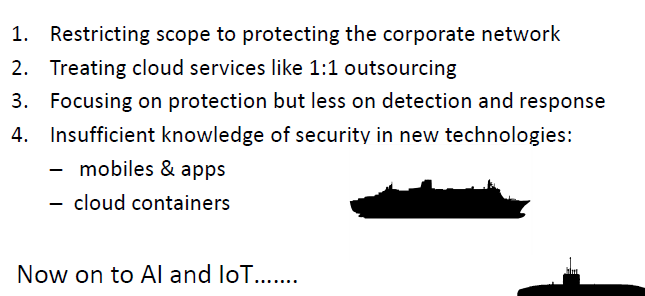
Solutions

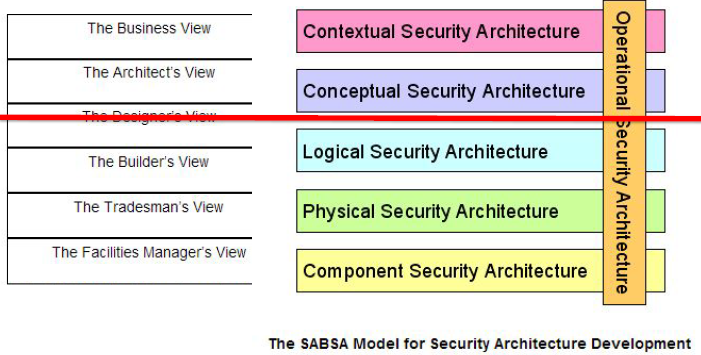
* Get views of ppl not involved in decisions
* Remind yourself that even best managers make mistakes
* Don’t encourage failure fearing

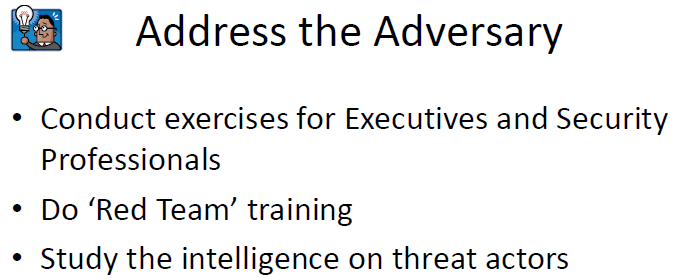
Risk of Compliance Reporting

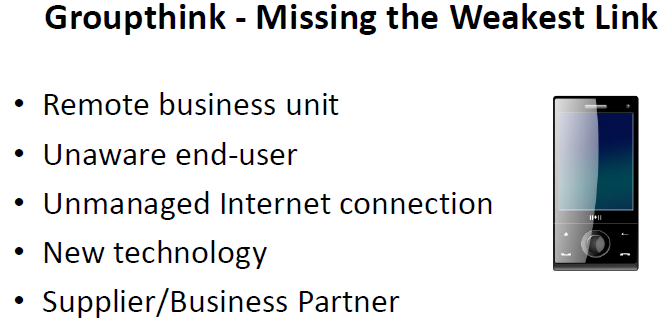
* Jumping on red

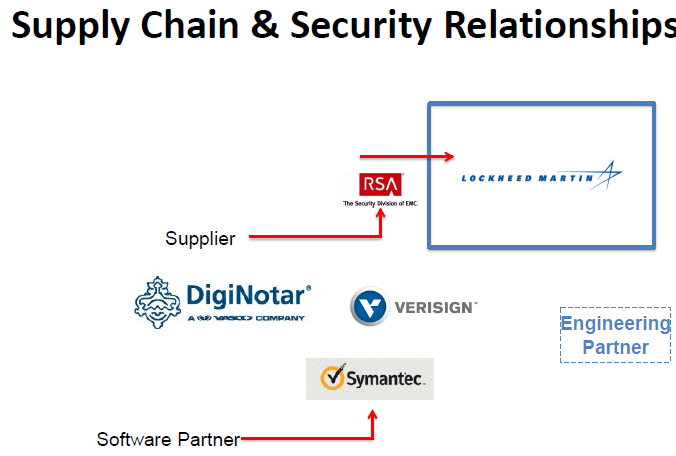


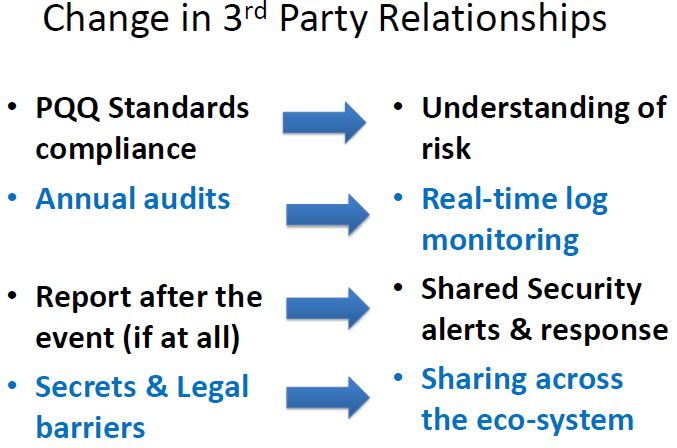


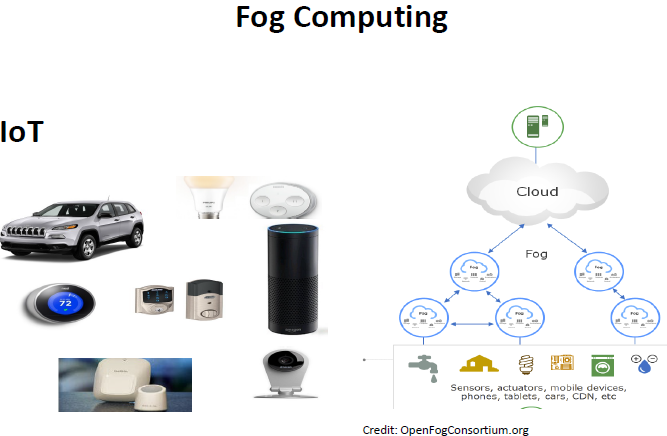




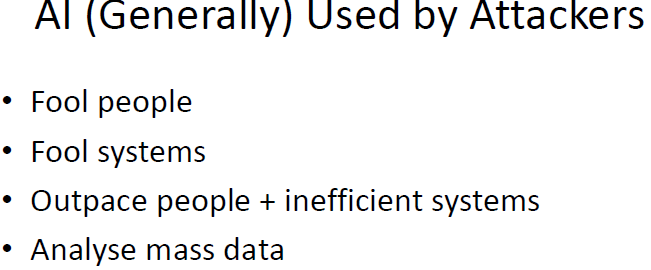


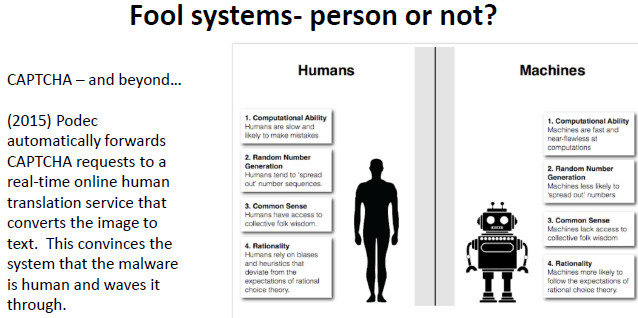


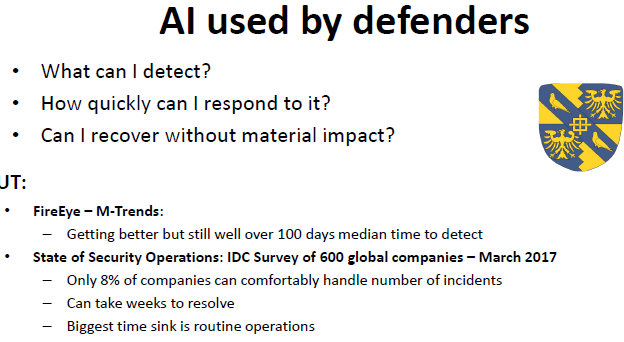


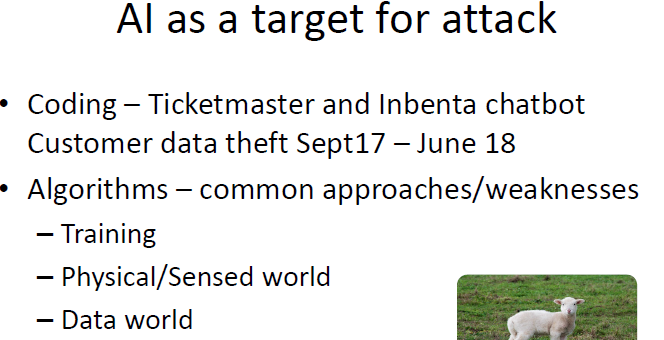


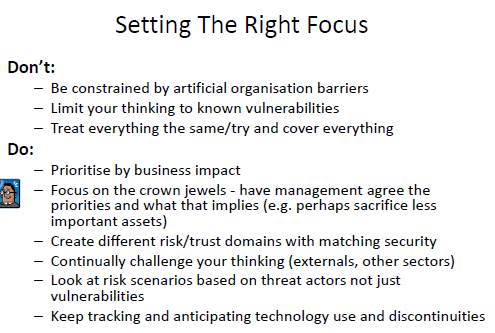


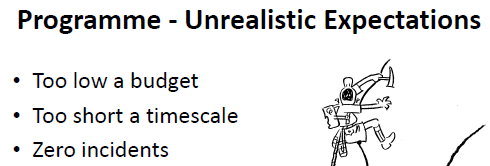


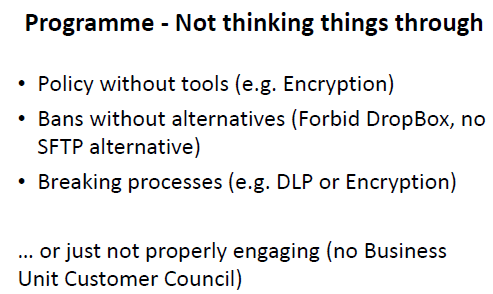




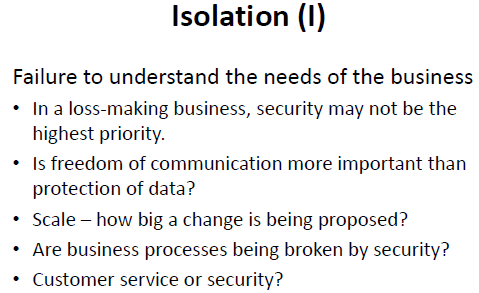


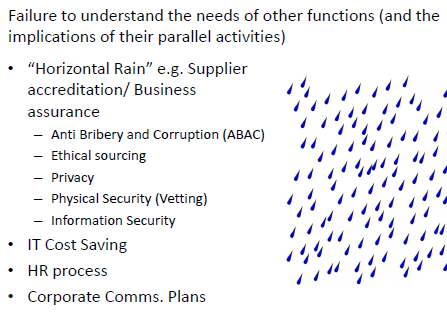
Images can be trained to recognize wrongly 

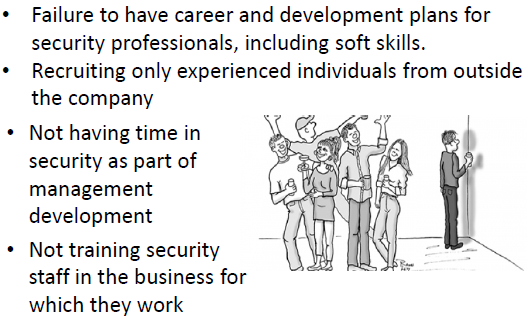


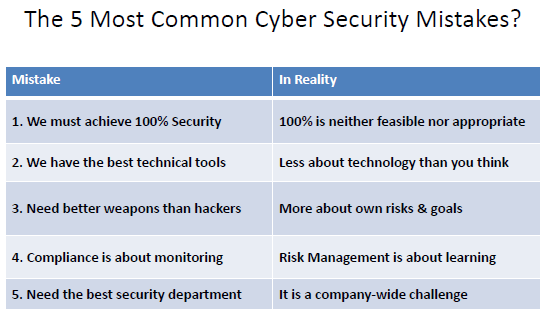


BIGGEST TAKE AWAY = WORK WITH OTHERS, DONT ACT IN ISOLATION









**Failures of ISM**

Objectives:

* Look at examples
* Uds why failures
* Learn lessons

Why look at failures:

* Avoid errors that caused failures
* Common (often not reported)
* Can look at which areas are more data (historical/statistical), and focus more VA

Breaches (may) not be simple failure

* New attack vector found/exploited
* Think beyond known vulns

Security = needs to be reactive

* Able to detect + react
* Protective controls (necessary), not enough

Though controls/staffs are good, breach can still occur

NIS: online business need to notify if impacted

**TalkTalk Case Study:**

Oct 2015, DB compromised

* Large set of customer info (156,959 cust)
  + 15,656 bank acct
* Talktalk didn’t know how BIG
* Big fine in the end
* Exploited vuln in 3 websites   
  (gave access to info)

6 days to aware = network slowness

* SQL injection atk (identified shortly)

Next day = report to ICO, public, email customers

Next day = headlines, (4mil reported, not true)

* Post update on company site
* Warns customers
* Ransom message in email to MD

Next day = fraud happened, stole cash, used to buy goods

25 Oct = website, not core systems, no credit card details

26 Oct = Talktalk confuses public (sequential atk)

* 15 yo arrested

30 Oct = extent of data accessed, sig less than suspected

31 Oct = another person arrested

6 Nov = reveals actual scope of atk, payment cards obscured (cant use for fraud)

11 Nov = 30-35 mil for data breach, free stuff for cust

20 June 2016 = Inquiry, never remove/secure webpages that enables attack on website+DB

DB = outdated, bug enabled attack

No monitoring to discover buln

SQL injection = common attack (known defense)

2 prev attacks, not much actions

Impact mixed

* Nov 15 = 30 -35 mil lost
* Feb 16 = Lost 101k customers, half mil took up free upgrade
* May 16 = lost 100k, more than 40mil
* Jun 16 = 400k fine

Lessons

* Talktalk should have known, 2 prev attacks, no actions, software outdated = FAILURE in Risk mgmt.
* Must learn from Talktalk security fails = can cost business, must honour info customer entrust to you = NO EXCUSE

**Moonpig** (greeting cards)

* 2 separate breaches (Jan 15, Jul 15)

Jan 15 = millions of customers vuln to atk

* Frustrated, released on blog
* API has no auth, can just place orders on customer’s account, card info, addresses, orders
* Easy as not rate limited, cust ID = sequential
* Aug 13 = initial, chased on Sep 14, released on Jan 15
* Disabled Mobile APP

Fixed by have same creds on API calls, used 9 digit Acct num, unencrypted. (resend request with 9 digit number)

Impact = DMG-ed reputation, top10 uk security breaches  
Jul 15 = email, pw, acct balances = public

**Mumsnet** (2 public atk)

* April 14, heartbleed (unknown amt compromised)
* Aug 15, large scale DDoS atk, released 3000
  + Someone hacked into admin
  + Reported to police, confident user pw not accessed
  + Forced pw change
  + Likely result of phishing attack
  + Promptness + clarity + detail = praised

Impact:

* Inconvenience, but well treated = won praise

Lessons:

* Not to be blamed for Heartbleed, but responded really well

**Facebook** = fined 500k for Cambridge Analytica scandal

* Failed to safeguard user’s info
* Failed to be transparent how it’s harvested

2014 to 2015 = allowed an app to harvest 87m user profiles (used by Cambridge analytica in 2016 president + referumdum)

* Warning letters to 11 political parties (notice to agree to data protection audits)

Conclusion

Summary

Infoseurity = preservation of CIA of info + info processing resources

ISM = set of processes procedures and ppl to ensure infosecurity

Themes

* Implement security to meet business needs
* Use business needs to underlie risk assessment process
* Select + manage controls based on risk assessment
* Make sure staff buy into processes, can perform them while doing their job (most impt!)

Use ISMS to enable ISM

Definitions of basic concepts of ISM and ISMS in ISO27000

* Consideration of req. of **27001**
* Security controls in 27002 (not really in exam)
* (req. of 27001 = consider controls for possible adoptions)
* Concluded with detailed 27005 (risk mgmt.)

Operations of ISMS

* Legal + regulatory issues
* Audit
* Incident mgmt. + disaster recovery
* Staff mgmt.
* Procedural issues

Real World ISM issues

* 2 leading practitioners from real life ISM
* Failure from ISM

ISM = balance between ideal + what can achieve

Resources != infinite, priority of most important asset, most efficient

Enough to be MORE secure than peer ORGs (unless major target)

EXAM = MAY 2019

* 3 out of 5, 2 hours
* Examples of old papers (3rd time taught course, don’t expect same style for exams before 2017)

REVISION LECTURE = APRIL 2019

* Q&A style or go through topic
* Can send questions in advance