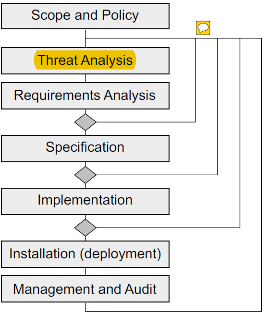
**IY5523 SBA**

Secure System Development Lifecycle

Feedback Loops – to go through threat analysis



**Scope and Policy**

**Scope**

- Purpose

- Main entities (users)

- Data

- Info transmission

- Main assets (can be staff, source codes, hardware)

**Policy**

- Set of rules how assets are managed & protected

At many levels of details:

- high level = general rules handling data & resources  
- detailed level = system specific policies describe rules for protection of system assets

**System Security Policy** = overall guidance for design for secure system

**Assets =** elements of system one wish to protect

Inc. data, hardware, software, procedure, ppl

\*part of scope = assets identified + listed

**Threat =** danger to asset’s CIA

**Attack =** realisation of a threat

= implementation of a threat from deliberate actions

NOT ALL THREATS => ATTACK (accidents)

**Safeguards =** mechanism, procedures used to protect assets against threats

e.g. authentication, access control

**Vulnerabilities** =weakness, absence of safeguards (exploited by >1 threats)

* In system, ops, safeguards

**Impact =** degree of damage by threat (seriousness)

Cost of safeguard VS cost of realised threat

**Risk** = seriousness of threat, + impact + probability

High risk = high impact X high probability

* Needs management, eg low risk != use money

**Risk Analysis =** identifying + assessing risk

**Risk management =** totality of measure = reduce risk

**Security Requirements =** define what safeguards

**Requirements Analysis =** refining the requirements

(high level security measures)

**Specification =** main objective > security requirements

Details of security req = derive from structure of sys

Hence = certain component, operate with security, also can define specific security-relevant subsystem

**Secure systems:**

**-** crypto funcs

- OS system sec functions

- hardware (smart card)

- physical (secure room)

**Implementation** = procure + combine with bespoke implementation

**Documentation =** system specifications, manuals, procedure definition, configuration, operations

**Testing** = confidence in correct operation

- design of set of test cases  
- done by third party, or supplier (review = best)

**Sec evaluation =** Different levels of confidence in correctness

- licensed, e.g. Common Criteria

**Installation**= procedures, how employees manage the ops. Size + complexity of procedures varies (depending on degree of human interaction)

From initial config -> day to day operations

**Procedures:**

**Contents:**

Roles = participants in defining procedures

Assignment of roles to individuals

Installation + initial config

Ops Procedure

Backup + Restore (disaster recover)

**Dual control** = no single individual has the power (e.g to access plaintext) **Separation of Duty**

**Dual control Mech :** >2 keys, multiple tokens to complete certain tasks

**Auditing Mech:** records of security related events

- Protected against tampering the system

- MAC on records, using key stored in physical subsys

WORM (write once, read many) drives

**Security management**

**-** secure sys = continuous management (operates correctly)

- upgrading system on new function, fix vuln

- important part of management

- Divided into:

* fault management
* config + change management
* accounting + audit management
* performance management
* security programme management

**Security Auditing**

- check security procedures = carried out correct = detect security reaches

- for root cause analysis (and responsibility)

- auditor = independent of ops role holders

- auditor != operational (separation of duties)

- auditor != experts, but can perform their function without advice

- defined as part of overall procedures

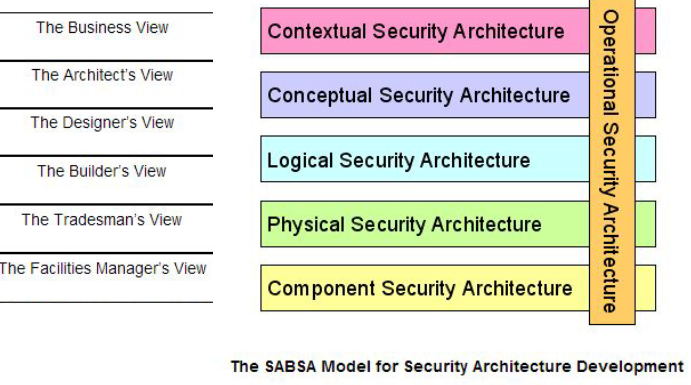
**Governance Risk Compliance**

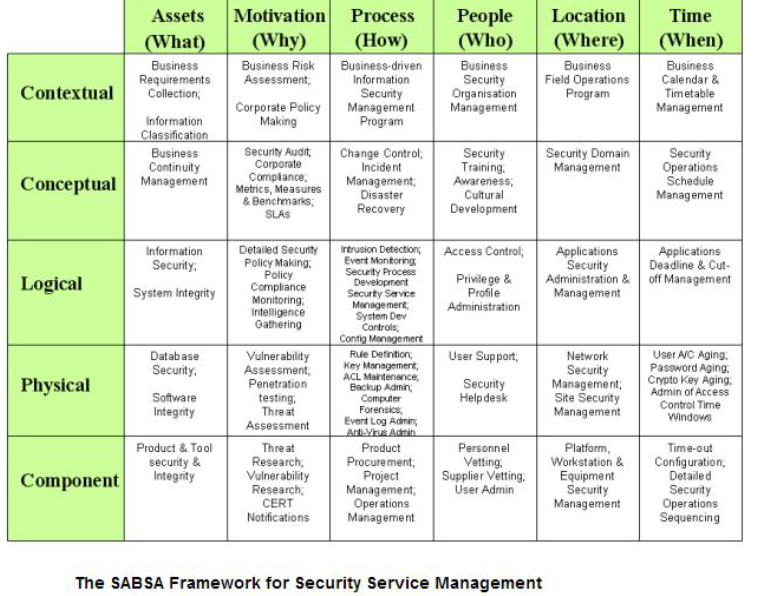
Benefits of Architecture:

- Common Language (^ comms, v ambiguity)

- Defines landscape (^ completeness, v gaps)

- Reduces Complexity (^ abstraction, ^ standards)





**Example of Contexts:**

Business Criticality

Threat Env

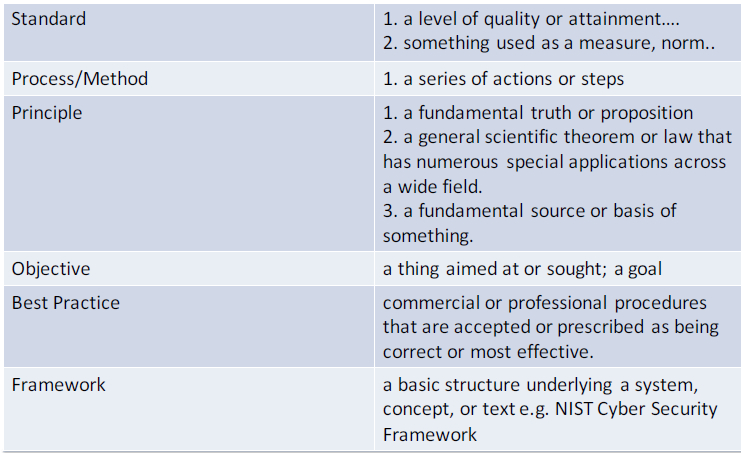
Usability Restrictions

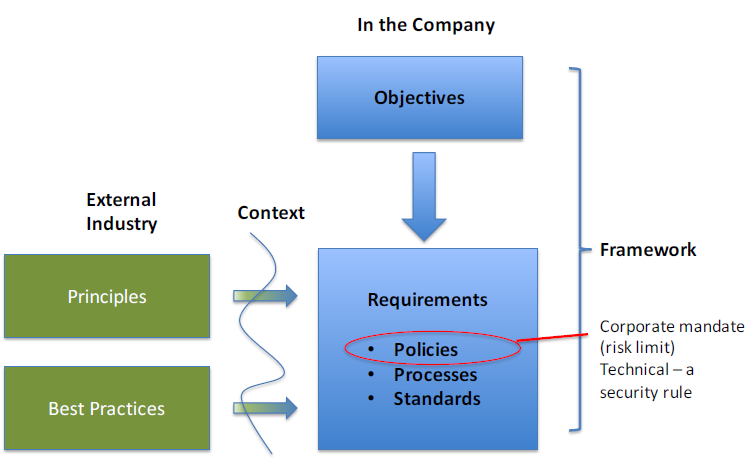
Restrict Scope to protect corporate network

Treat cloud services (outsourcing)

Focusing on protection, less on detection + response

Insufficient knowledge of security in new tech





**Gap between Board & Technical (Gov to breach it)**

- different expertise/language

- Breadth of view

- volume of detail

- frame of reference

**Cloud Governance issues:**

- Transferring control to someone else

- responsibility of data, assets

**Problem:**

- good risk management

- consistency (weakest link, overkill, interoperability, collateral damage)

**Alignment:**

- context, tools, expertise, data, motivation, sanctions

**Governance:**

Processes + structures implemented by board in order to inform/direct/manage/monitor activities of organization towards achievement of objectives

**GRC** (like umbrella, cover 3 areas of enterprise)

Areas of activities more aligned + integrated

**Diff types of Governance:**

**-** Corporate Gov  
(info tech gov, env gov, econ+finance gov, project gov)

- regulatory gov

(each type = >1 source(s) of guidance, similar goals, varying terms/techniques for achievement)

**Implementing Governance**

- Structure (frameworks/processes/models/methods)

- Codification (policy, risk appetite, apprved solutions)

- Capability (trained experts, decision gates)

- Data (Risk reports, matrix, risk position)

**Roles + Decision Makers**



**RACI Chart (Responsible, Accountable, Consulted, Informed)**

For roles/team- who is RACI

Responsible (actually doing it)

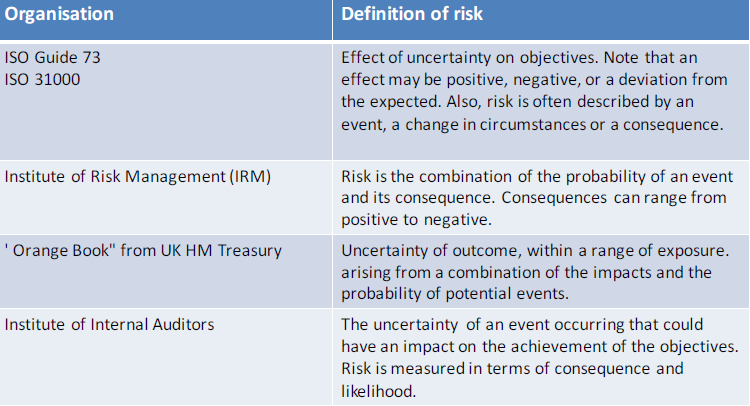
Accountable (decision maker, held to account)

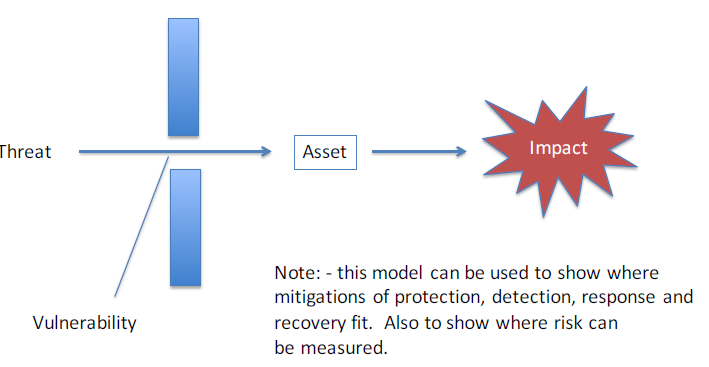
**Authorities + Delegations**

Who make risk decisions?

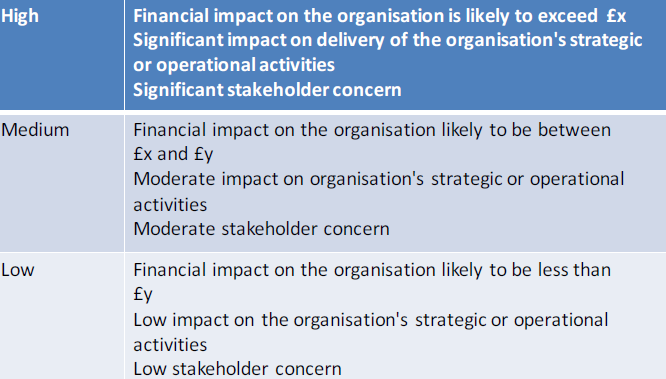
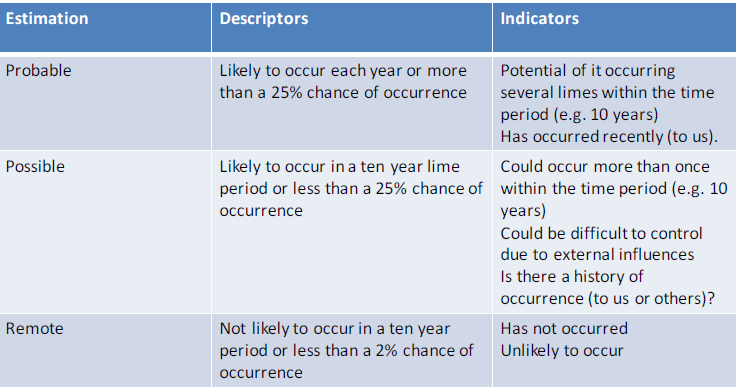
Who get authority?

What limits apply?

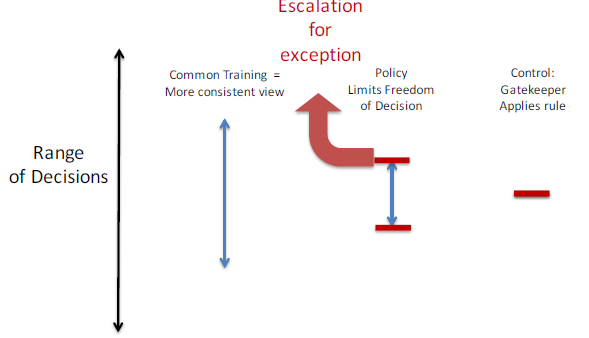




Risk Matrix

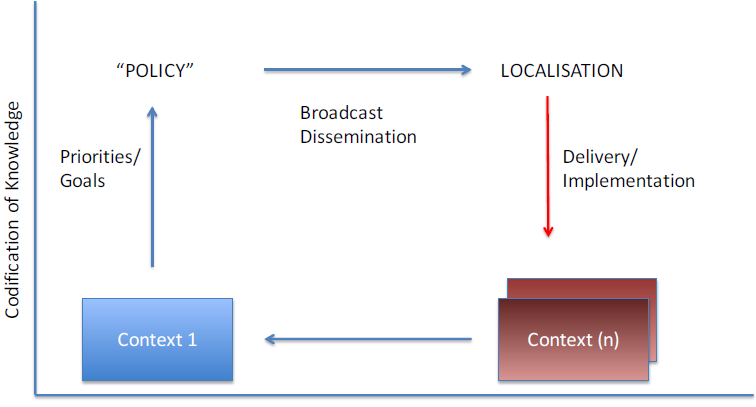


Balance = (Strategic goals, unacceptable lose ) VS (cost, operational opp)



Gatekeepers/Policies applied where it’s more critical

**Social Learning Cycle**



**Regulatory Gov**

GDPR, FCA, ICO, UK-NIS

Consequences:

- focus on lower risk, inhibit risk mitigation actions, set max standards

Standards VS risk judgement

Regulation = principles based OR rules based

(ensure data is protected) VS (Encrypt)

**Reporting**

1. Compliance Status
2. Capability Maturity
3. Risks (perf, improvement, targets, new risks, trends, aggregate)
4. Others (risk reduction)

**Dangers =**  different compliance rates differently

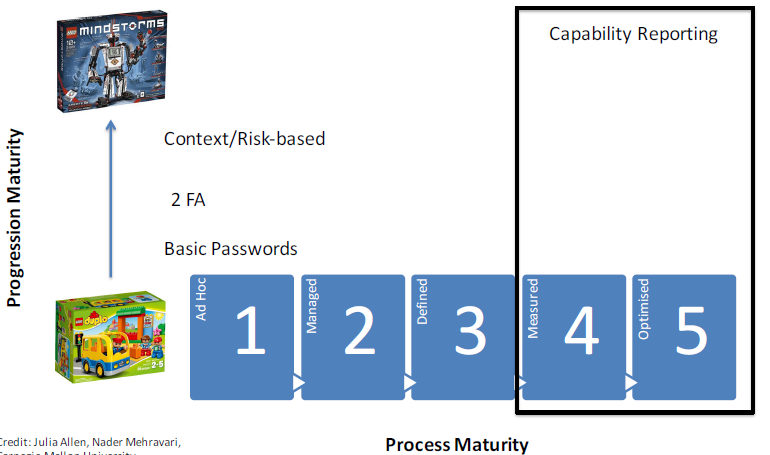
Compliance = easy to uds, BUT

- often defines max risk

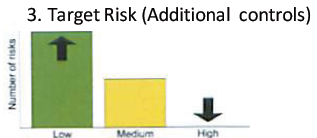
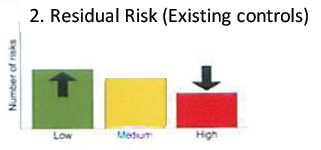
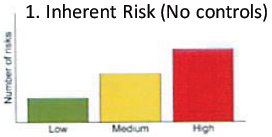
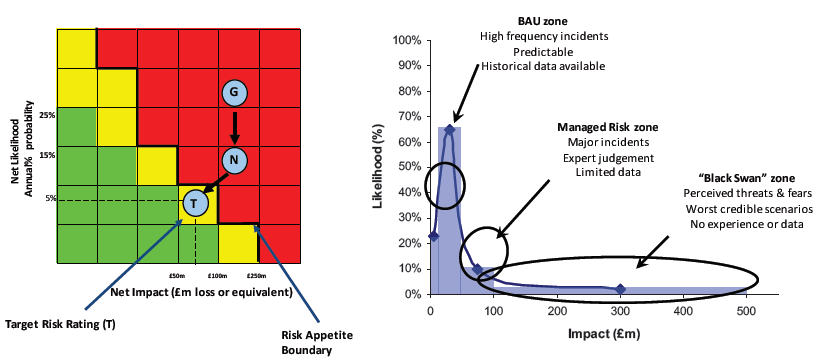
- always behind the risk

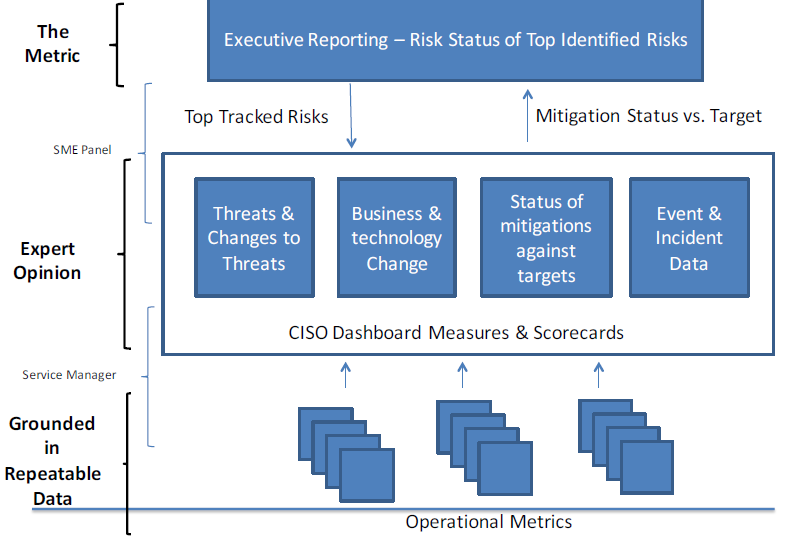
- can mislead on risk reporting

**CMM (capability maturity model)**

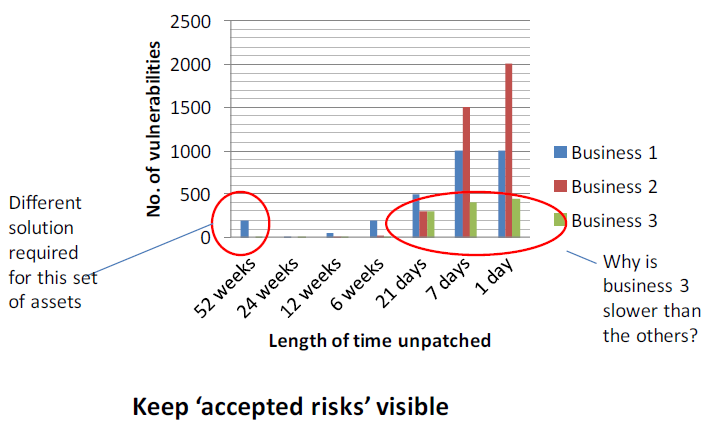


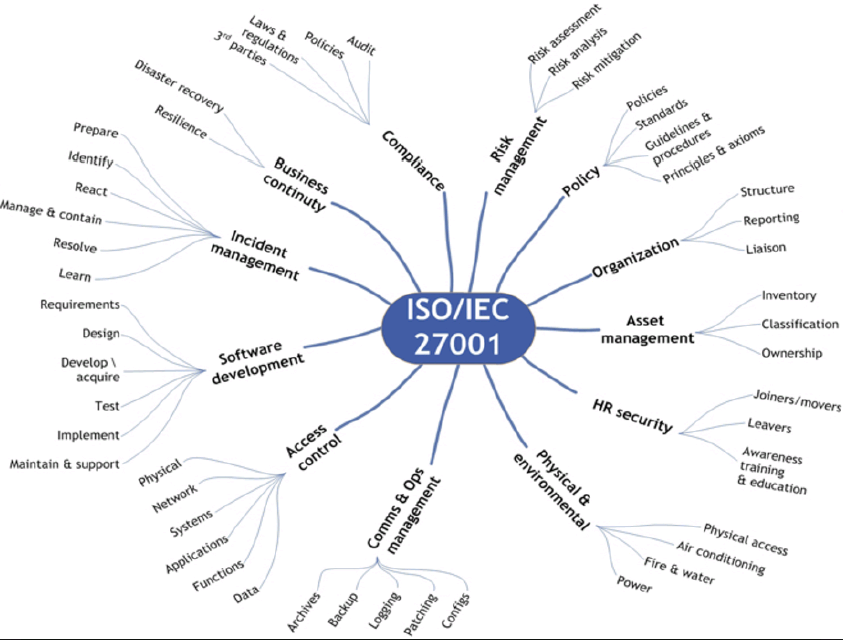
**Risk Reporting**





**Vulnerability Aged View**



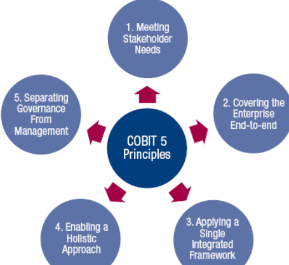


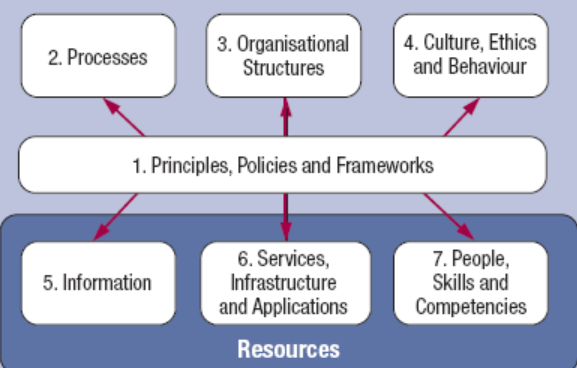


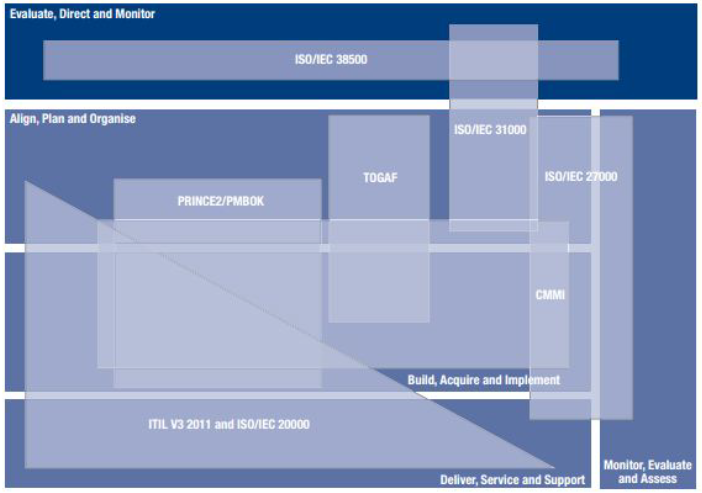
**Expanded to much more**



**COBIT**

Uses 5 principles to build effective Gov+management framework, based on 7 enablers





COBIT = Map standards back into corporate governance

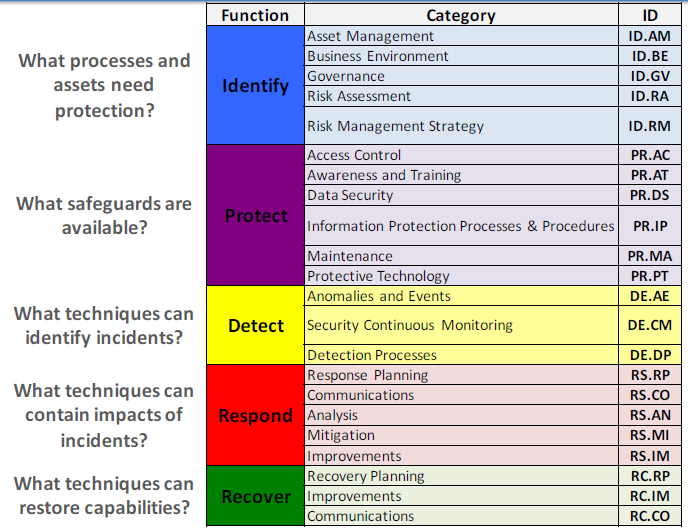
**Cybersecurity Framework (NIST)**

- standards/methodologies/procedures/processes that align policy/business/tech approach to cyber risk

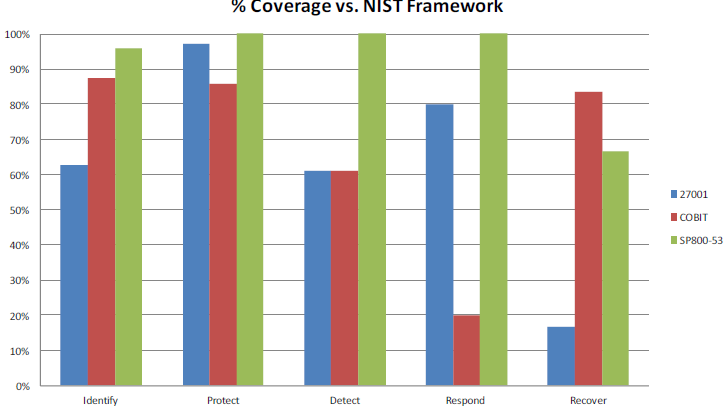
- prioritizable/flexible/repeatable/perf-based/cost-eff approach, with info sec measures+controls = help owners of CI, identify/assess/manage cyber risk

- identifies areas for improvements

- consistent with voluntary international standards



**Links back to international standards (like COBIT,ISO)**



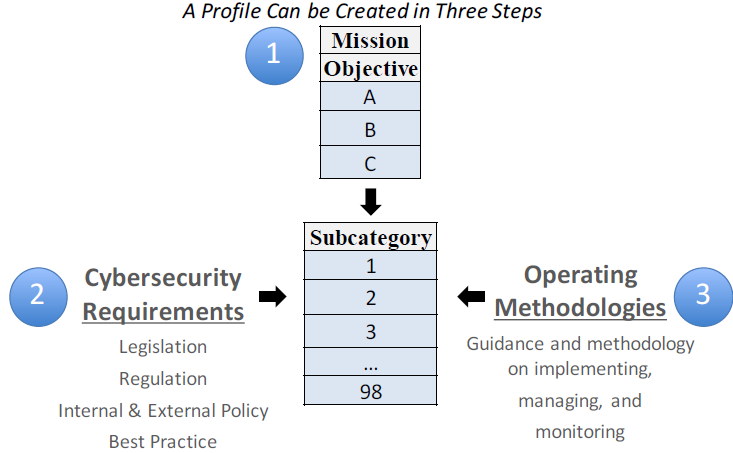
**Profile =** customization for sector/organization

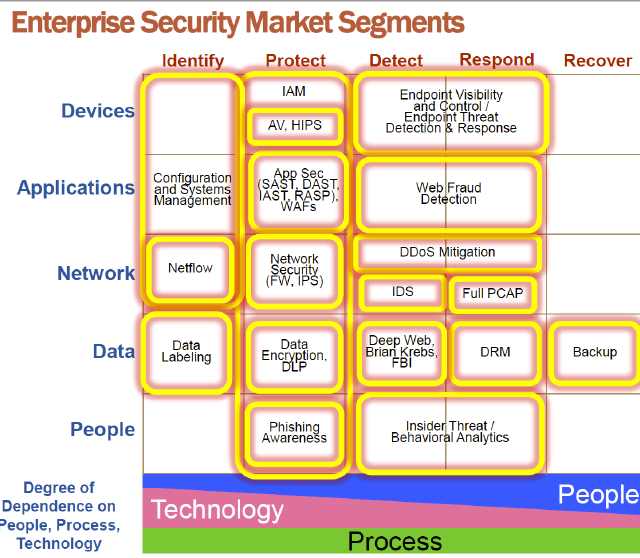
- fusion of business/mission logic and cybersec

- alignment of cybersec with ops

- basis for assessment + expressing target state

- decision support tool for cybersec risk management



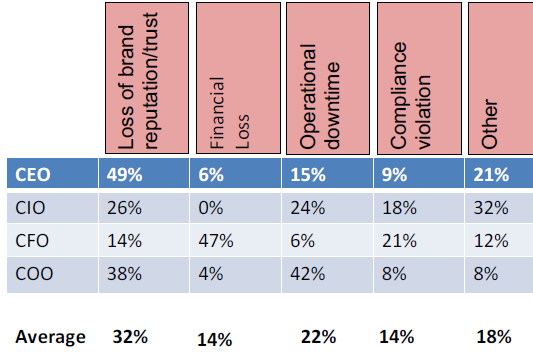


**Risk Appetite**

**Links** organisation’s **objective** to **risk** = allow for conscious decision, how to behave

**Define risk** an organization is prepared to accept (loss/disruption)

**Cost of avoiding** likelihood + impact + benefit



**Summary**

Architectural Concepts are fundamental to org sec

* Enable comms, setting code, Simply

Standards enable measurement (but there’s limits)

Codification needed cross organisation

* Needs context/localisation/understanding, skill in dev and usage

Adopting Risk Management Concept = for focus + relevance (requires understanding + practice to apply)

**Identity Management**

Define = set of processes + tools + social contracts for creation + maintenance + utilisation + termination of digital identity for people/systems/service = secure access to systems + apps

Define = set of info known about the person

Proof of Identity = (removable) tags + procedures

Jackal = use a dead child (birth cert) + apply passport

Infosec = CIA

WHAT is identity?

- **Attributed** **Identity** (name, DOB, place of birth, parents name, mother maiden name, birth cert)

- **Bio** **Identity** (edu, qualifications, where lived?, employment, interaction with structured society)

- **Bio** **Data** (any info combined = identify indiv)

- **Biometric** (diff types, accuracy, intrusiveness, tech, requires post-enrolment)

**Digital identity**

Dig identity = person’s identity in the dig world

(can have multiple)

Not exclusive for people (possible with services/systems/devices

Multiple identities = multiple tasks

(employee = org, citizen id = gov, ISP = services)

Req to PROVE identity

1. **Validity** = evidence to confirm name exists

- access wide **range/history/quality** of data

2. **Verification** = if applicant = subject/owner of valid identity ref.

- genuine person would know info   
(address, marital, employment)

**Electronic VS Doc Evidence**

- Credit Ref agencies prefer Electronic

**Doc is not robust as ☹**

- reconstruct visual check doc (photocopy?)

- Data = static

- Logistics of centralised checking process = high

- Documents = forged/bought

- Genuine doc easily obtained falsely

- doc used to breed other doc

Setting up multiple/corroborative/long term **electronic data = difficult to fake 😊**

**Registration + Enrolment**

= crucial important

= what are you trying to protect?

Registration = identify + enrol +…

Enrolment = binding u to the dig identity

Reliance on RESULTING system

High assurance registration + enrolment != scale

\*insider threats as well

**Req. for Biometric**

- secure enrolment procedure

- binding of biometric template to enrolee

- check template quality and matchability

Verisign = auth + verification procedure for SSL

Process for confirming

- still in business

- owns/has rights to use domain name, common name of cert signing request

- “corporate contact” works for organisation

- “corporate contact” aware of cert request  
- “technical contact” authorized to receive digital ID

Privacy = anonymity, pseudonymity, unlinkability

**Anonymous**

- free service = simple

- payment (requires anon payment sys)

- true/absolute anonymity = difficult to achieve, revealing IP addr = compromises it.

**Pseudonymity**

- lesser form of anon, reveals special type of identity

- generated regularly, short-lived

**Unlinkability**

- Property required to use pseudonyms

- Two pseudonyms are unlinkable if 3rd party cannot tell if it’s same user

- Often difficult to achieve, authorisation process = reveal info about user.

**De-identification**

- most common = process of removing/altering data in medical record (to identify patient)

- technique to allow research/training => use real medical data => not comprising patient privacy

- HIPAA

Patient = remove personal, de-localisation, record order scrambling, numeric items banded, extremes truncated, data reduced

**IDENTIFICATION**

User identifies themselves to trusted body

User = identifier

Identifier = given to authenticate the user

Authentication = confirms person producing identifier is the person to whom is was issued

**Security/Business Issues**

Send/receive valuable info

CIA of data

Identify ppl remotely?

**Why USE?**

**legal + audit + enable collab**

- moving away IAM, seen as protection commodity, deployed to deal with specific security

**Cost-saving + SSO**

- protection against identity theft (protect themselves from exposure, no more pw-based auth)

**Main use = identification + user auth + Id verification**

**Authorisation (Access control)**

**-** existence of auth process required

- decision to grant access request by process (based on security context)

Security context (id the user, any security group belongs) -> user that initiated

**Access Control** = specific security policy (org/statutory)

* Confidentiality (read) / integrity (write)

**Remote Working**

- to cut costs + better work/life balance

- finance benefit

- home internet = increased reliability+ availability

VPN = standard to connect to corporate network

Remote Access Server (RAS) used to manage AAA

Corporate Security Policy = amended to securely manage equipment, connection data

**Data Access**

- legal obligation (GDPR), impact IAM deployment

**VPN** = communicate confidentiality, protected network, internet = less trusted

Crypto protocols = confidentiality, sender authentication, message integrity.

* Extended geo connectivity
* Increase security (with encryption)
* Reduced costs (leased lines)
* Support users who wish to telecommute

Security implication   
= client side must be tightened + enforced

= Accessible corporate network from VPN = reduced  
= security logging on LAN

**SSO**

- auth to multiple sys = unpopular

- users = reuse same pw to avoid rmb diff pw

- once per session, forwards auth ID to other process

- strength of SSO <= strength of initial AUTH

- first AUTH compromised = quality diminishes

- not new, kerberos

**SSO and identity management =** synonymous/interdependent concepts

= basis of IdM

IdM no required for SSO

IdM = broad term, > than just provide auth service

**Business benefit of IdM**

* Simplification of admin, reduce cost
* Increased security, from strong auth mech
* Greater access to info (by partners/employees/customers)
* More transparent = SSO to hosted service
* Better regulatory compliance (security, audit, access policies)

**Regulations**

* HIPAA (privacy for health), Sarbanes-Oxley, Gramm-Leach Bliley Act (finance info), Basel II

**EU Directive**

- Data Protection (harmonise law of member states)

- Free flow of personal info

**European Data Protection Directive**

* Min data protection requirements

**Data Protection act 1998**

- implements EU Directive (8 principles)

- create civil/criminal for breach of act

- empowers information commissions = supervisory authority (responsible for UK policy, supervision, guidance, enforcement for data protection)

**GDPR** = regulation = implemented directly in law

- update (from previous EU directive + UK DPA)

- UK has same legislation = easier for UK to trade in EU after Brexit

NEW of GDPR

* Data Processor (on top of Controller)
* Right to erase
* Data Breach notification
* Data impact assessment
* Increase enforcement

USA

Industry – HIPAA, GLBA(finance),

State – California Online Privacy Protect Act, Security Breach notice

Federal – Telemarking Sales (Do not call), Electronic Comms Privacy Act

APEC (Asia Pacific Economic Cooperation)

Business

* Brand
* Employee Data Management (need localised)
* Increased Regulation (legal solutions for EU data trf, prev=Safe Harbor, model contracts)
* Customer Sensitivity (Lingual/Cultural)
* Extended Enterprise (R/L with partners)
* Technology Advances (Web based)

Identity Theft/fraud = wrongly acquires/uses person data, for own financial gain

Tech = steal mail, eavesdrop, steal personal info, infil organization, impersonating a trusted org in e-comm

**Identity Management**

**Deployment Models**

**Silo** (setup and operated by single entity for fixed user/resource community)

**Walled Gardens** closed community of org, single IDMS, B2B, specific operating rules for IDMS (like CC)

**Federated Identity**

* distributed model (open standards = OpenID/OAuth)
* no single entity for IDMS.
* Support multiple identity providers (IdP),
* distributed + partitioned store for identity info
* Strong end-user control + info dissemination
* Like passport system
* Allow multi org to exchange + link identity info across org (between partner/supplier/customer)
* Bridge between segregated silos of identity sys

Issues for Federated Identity

* Federated Vs Local
* Identities Change
  + Marriage, Multiple names
* Ppl move (update info, notify federator)

Drivers for Federated Identity

* (Service Providers) may wish to accept Identity from (Identity Provider)
* ORG extend employee identities to 3rd party
* Role/Credentials/Authorization Police assert from IDP to SP
* Multiple SPs may use auth of a single IDP
* Large ORG need to manage numerous security domain = internal federation across traditional silo
* Cross domain SSO without homogenize sys/auth approaches

Partners need to consider POLICY ADHERENCE

* Access policies (define lvls of access agreement)
* Privacy (industry + tech dev req)
* Logging, risk, liability….

IDMS Components

* Data Repo Components
* Security Components
* Lifecycle Components
* Consumable Value Components
* Management Components

Data Repo Components

* Deal with storage + management ID info
* API access to info
* LDAP/meta/virtual directory/db
* Policy govern access to info (stored here)

Security Componenets

* 3 categorys (AAA)

Authentication Provider (also IDP)

* Primary authentication of indiv
* Generates an auth token (smartcard,biometric,cert) app dependent

Authorization Provider

* Enforce AC when entity access resource
* Allow apps to make authorization + policy decisions

Auditing Provider

* Mech to track info in repo (create/mod/used)
* Analysis if circumvent policy controls

LifeCycle Components

* 2 categories

Provisioning

* Automation of all procedures (Creation, linkage to auth, setting+changing attributes/priv, decommission identity)
* Large sys = allow some self-service creation/management of identity

Longevity

* Historical record
* Allow examination of evolution of identity
* Allow attestation = ability to attest what actors had access to what resource in what timeframe

Consumable Value Components

* SSO (primary auth once), allow access of apps (part of IDMS environment)
* Personalisation (preference mgmt. tools) (allow apps to tailor user experience)
* Self service (enable users to self register to business service, manage profile info, allow auth cred management)

Management Components

* 4 categories

User management

* centralized infra for managing user profile/preference info
* decrease overall IT (user self service, directory optimization, profile synchro)

Access Control Management

* centralized infra for managing user auth/authorization
* allow automating access policies for employees/customers/partners

Privacy Management

* implement privacy + data protection

Federation Management

* establish trusted R/L between IDP

**Identity Management = tough**

Successful ID mgmt. = Kerberos, special purpose PKI (cc), Google ID

No global Schemes = no universal PKI

Identity = context specific (universal/global = unlikely)

**User Perspective**

Password policies = too draconian = compromising security

Security awareness training = biometric needs training = impt topic (tutorials, elearning, reminders)  
-> test if training = desired effect

**Legacy Problem**

Implemented KPI (with employee badge, integrate backend = difficult+ incomplete, requires OTP as well)

Factor in apps to support

**Cultural Difficulties + Difficulties**

* internal vein pattern scans of finger/palm = populat
* avoid fingerprint (too accurate) perception
* **facial != accurate, but comfortable**

**Ill design IDMS = more cost**

* time spent (staff logging on/auth to apps)
* time spent (admin managing dig ID in ORG)
* no. of PW resets
* data redundancy = associated admin cost

**Inability to function**

**Reduced security**

**Placement of liability**

**Inability to charge for service** (client make use of service without service provider identify them = provider cannot charge for service)

**Open Issues**

**Authenticity of ID** (determine accuracy + validity)

**Longevity of info** (track ID info over time, provide evidence to support historical investigation)

**Privacy, Identity Theft, Legal Structures**

**Process and Procedure Management**

1. **Enrolment**
   1. Issues with f2f/remote
   2. PKI lvl (lvls of identification/liability/algo str)
   3. Human Error + Procees
   4. Banking (KYC)
   5. HR = only authority
   6. Apply Federated ID, Dup checks
   7. HR add you, not remove you

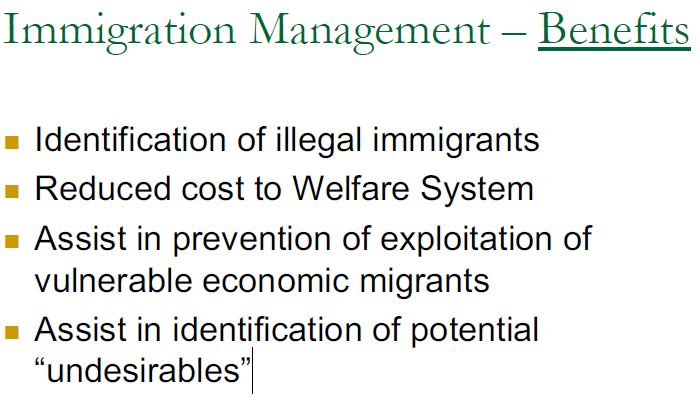
Verisign messed up

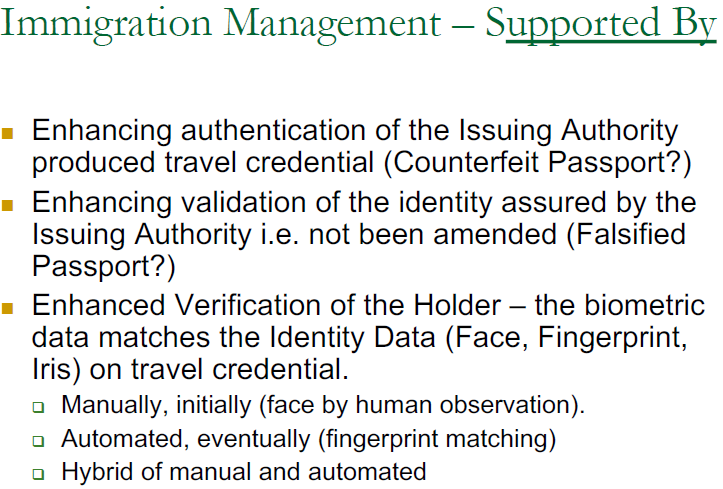
1. **Management of User Auth**
   1. IdM DB = Accuracy, Scalability, Extensibility(upgrad), Interoperability, Speed of implementation, solution complexity, data ownership, lifecycle management, provisioning, workflow, pw mgmt., selfservic admin, delegation
2. **Lifecycle Mgmt**
   1. ID life cycle = keep user’s entitlement current (moving department)
   2. Manual/automatic (changing of priv)
   3. Source of info feed
   4. timeliness of process
3. **Provisioning**
   1. Account provisioning
   2. resource provisioning
   3. Account de-provisioning (termination of access rights to sys)
   4. Authoritative Sources (HR, sys providing financial data services, directories)
4. **Workflow**
   1. Request entered, Routed, Path
   2. Passed to responsible creating the ID
   3. Process = consistent, audited (authorization)
   4. Automated = notify managers/admins (approvals), related to self service
5. **PW management**
   1. Considered weak auth
   2. But easy, no hardware, pw = stay
   3. Secure management = impt
   4. Establishing + managing PW policies
   5. Changing/resetting PW
   6. PW Synchro = updates/propagation
   7. Reduce PWs to rmb
   8. Update costs + admin overheads kept to min
   9. ISSUES = verification of PW change, diff PW policies (from silos)
6. **Delegated Admin**
   1. Group of indiv = admin
   2. Delegate permissions
   3. Partner ORG = manage own employee data
7. Self Service Admin
   1. Allow user to manage parts of identity
   2. Reduce admin costs + time
   3. Which fields = update/changed
   4. Validity checking
   5. Update= requires separate authorization

**Managing Tech to Business**

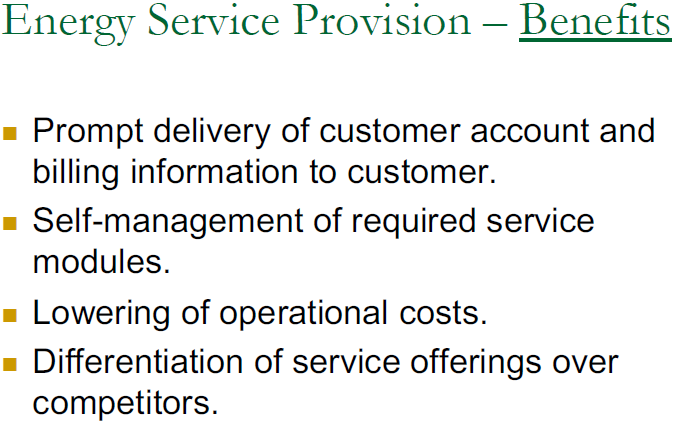
* Tech Dev Consideration (what can be supported, integration, diff techs)
* Architecture/Infra = offline/online, heterogenous platform, partner infrastructure/remote clients
* COST!
  + Cost of ownership
  + Rollout VS mgmt.
  + Size (manual V automated)
* Feasibility Study not the same
* Exponential Costs.

Sample Case Study









**Risk Assessment**

Using NIST SP800-30

Intro, Fundamental, Process

**Scope + Applicability of RA**

- Facilitate decision making at levels of risk mgmt.

Tier 1 – ORG / 2 – BusinessU /3- Info Sys

Throughout System Dev lifecycle

(Presys acq, sys acq, sustainment)

RA = No Specific Req (formal, lvl of detail, methodology, tools, techniques)

RA = not precise instruments of measure + reflect

* Limitations of specific assess methods
* Subjectivity/quality/trustworthiness of data
* Interpretation of results
* Skills + expertise of assessors

**Purpose of RA**

- inform decision makers + support risk responses

- Identifying:

->relevant threats or ORG

->Vuln (internal + external)

->Impact to ORG (from exploiting vuln)

->Likelihood of threat

Types of Harm

* Things to data
* Things to strategic/business

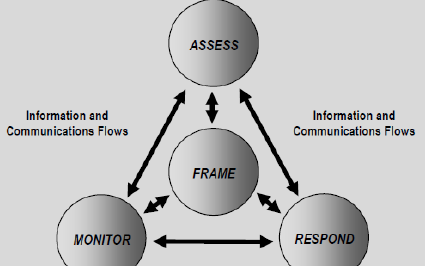
**Risk Mgmt Hierarchy**

Tier 1 + 2: systemic info sys security risks

(associated with ORG gov, Mission/Business process, Enterprise arch)

Tier 3: support implementation of risk mgmt framewk

(Security categorization, control selection + monitoring)



**RA in Context**

Part of ORG Risk mgmt. process

Framing Risk -> describe env

Assessing R ->

Responding R -> dev+eval actions

Monitoring R -> determine effectiveness of risk response

RA = support risk-based decision

* Dev of IS arch
* Dev of interconnection req for IS
* Design for security solutions for IS
* Modification of mission/business func

Why else might use RA

* Explore opportunity
* Identify B weakness/ shortcoming
* Drive change
* Eval hazards
* Budget planning
* Supply chain controls (biggest)
* Company risk Profile
* Compliance

**Risk** = measure of the extent to which an entity threatened by potential circumstance or event

**Risk A** = process of identifying, estimating, and prioritizing info security risks

**Threat** = any circumstance or event with potential to adversely impact ORG ops and assets

**Threat Source** = characterized as (i) intent + method targeted at the exploitation of vuln (ii) situation accidentally exploit a vuln

**Threat events** for cyber/physical atks characterized by tactics/techniques/procedures (TTPs) by adversaries

**Threat scenarios** = great events (with great specificity) + can be modelled/developed/analysed

**Threat Shifting** = response of adversaries to perceived safeguards and/or countermeasures

**Vuln** = weakness in info sys/ procedures/ internal controls / implementation = exploited by threat source

**Predisposing Condition** = condition exists in ORG, mission, which affects likelihood that threat events (if initiated) result in adverse impacts

**Likelihood** = weighted risk factor based on analysis of probability that given threat capable of exploiting vuln

(i) adversary intent (ii) capability (iii) targeting

(use historical evidence, empirical data, factors)

**Level of impact** = Magnitude of harm expected to result of consequences

**Risk Aggregation** = roll up several lower risk into high risk

**Uncertainty** = inherent in eval of risk

Why? = prev unseen, lack of vis of right info, lack of relevant data, changing regulations, lack of collab, lack of skills and capability, partnership and outsourcing, quantity potential dmg, diversity of process, lack of business maturity – poor process, lack of senior/board support

**Assessment Approach**

**Quantitative** = using number

**Qualitative** = non-numerical categories/levels (low, medium high)

**Semi-Quantitative** = uses bins/scales/representative numbers (role of expert judgement in assigning value)

**Analysis Approach**

Threat Oriented

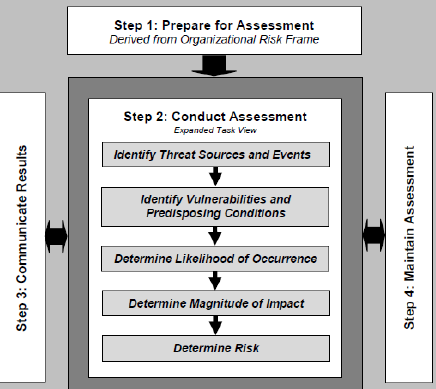
Asset/impact-Oriented

Vuln-oriented

ORG = can use single/multiple assessment methodology **(no one size fit all)**

* Time frame, complexity/maturity, phase of IS dev lifecycle, Crit/Sensitivity of Info + IS

**Process**



**Step 1: Prepare for Assessment**

**Task 1-1:** Identify **purpose** of RA

(Tier 3, RA support, decisions at sys dev lifecycle)

(Tier 2, risk A enable Org, (i) uds dependencies + ways risk are accepted/rejected/shared…)

(Tier 1, RA (i) support risk exec, (ii) key input to risk mgmt.)

**Task 1-2:** Identify **Scope** of RA

(ORG applicability, Effectiveness Time Frame, Arch/Tech consideration)

**Task 1-3**: Identify specific **Assumptions** + **Constraints**

- Threat sources, events, vulns, predisposing conditions, likelihood, impacts, risk tolerance, uncertainty, analytic approach

**Task 1-4:** Identify **information sources** (internal/ext)

Tier 1 = infosec gov structures, how ORG identify + prioritize crit functions

Tier 2 = info about business process, info flows

Tier 3 = design of tech used

**Task 1-5:** Identify **Risk Model** + **Analytical approach**

Quantitative/Qualitative/Semi-Qualitative

Threat Oriented, Assess/impact-oriented, Vuln oriented

**Step 2: Conduct the Assessment**

Task 2-1: Identify and characterize threat sources of concern

Task 2-2: Identify potential threat events, relevance of events and threat sources that initiate events

Task 2-3: Identify vuln + predisposing conditions

Task 2-4: Determine the Likelihood

Task 2-5: Determine adverse impacts from threat events

Task 2-6: Determine Risk (impact X likelihood) to ORG

(declaring uncertainty)

**Step 3: Communicate + Share RA Results**

Task 3-1: Communicate RA results

(exec briefings, RA reports, dashboards) formal/informal

Task 3-2: Share risk-related info

**Step 4: Maintain the Assessment**

Task 4-1: Conduct ongoing monitoring of risk factors

Provides crit info on changing conditions

Info can be used to refresh RA

Changes in: Threat Source, Threat Events, Vulns, Predisposing conditions, Capabilities + Intent of Adversary, Targeting of ORG ops, assets, or indiv

Task 4-2: Updating existing RA from results from ongoing monitoring

Sig. Changes: can revisit purpose, scope, assumptions, constraints

**PREV and NEW world**

Agility? IT env = dynamic, Infosec is not

Infosec Mgmt infra = assumes static entities

Social infra = cant take for granted

Working ENV = dynamic work force, no more job for life

Security tech are used (in staff control + ppl mgmt.) as much for data protection

Social media trends = enterprise more social, social media inclusion

Malware & stolen identities = more common

More virtualization, BYOD, mobility

Now = Multiple audience, adaptive, efficacious(productive + usable by Org), self-sustaining, complementary

Identification of assets, Analysis, Assessment

**New world**

Strength of countermeasure = resilience, solidarity of social network, speed of risk knowledge

Dependencies between physical, logical, social realms

Infosec problem = Multi-perspective problem (re-examine perspective) Physical//IT/Social INFRA

**3 Types of risk**

Perceived Directly (physical)

Perceived Through Science (pw cracking, crypto)

Virtual Risk (may be real/fake), (real consequences), science has no answer (APT, zeroday, quantum)

Risk Thermostat



**Cloud Computing**

**=** Cloud computing is a model for enabling ubiquitous,

convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

\* Defined at a high lvl to allow broad comparison btwn diff cloud services + deployment strat

3 Areas:

* **Essential Characteristics**

On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured service

* **Service Models**

SaaS (Software) e.g. email

PaaS (Platform)

IaaS (Infra)

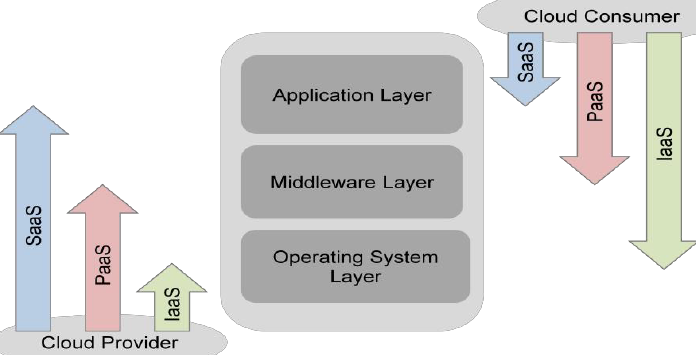
* **Deployment Models**

Private Cloud (exclusive use)

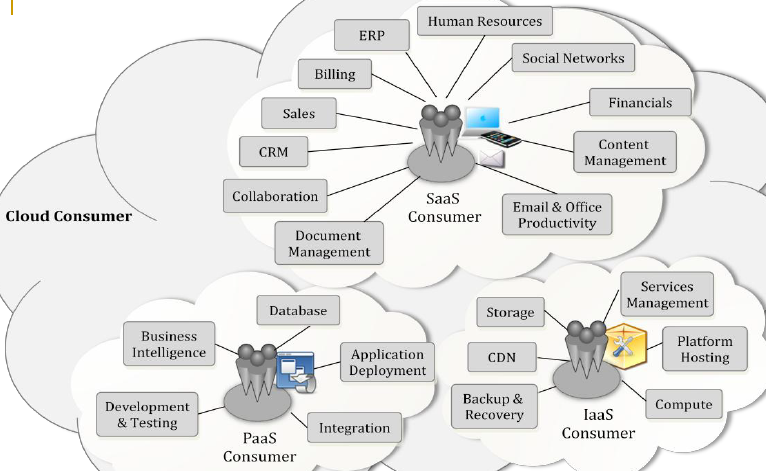
Community Cloud (specific community)

Public Cloud (anyone)

Hybrid (Composition of >2 cloud infra)

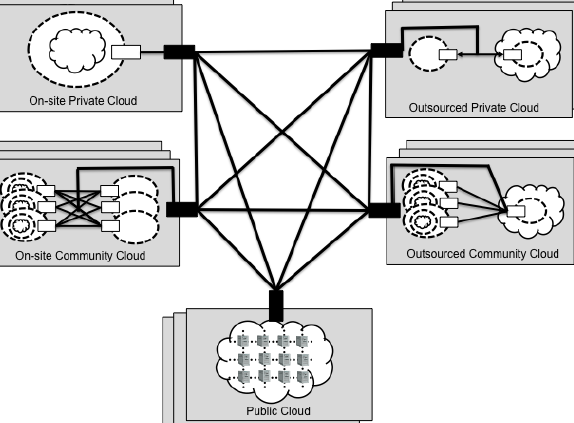


HyperV = inserts slim OS allows different instances of OS, thinking they have the having access to hw

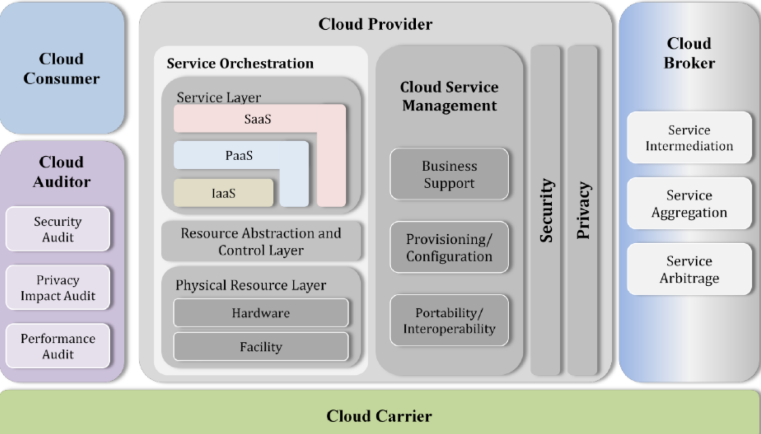


**NIST – Cloud Provider:**

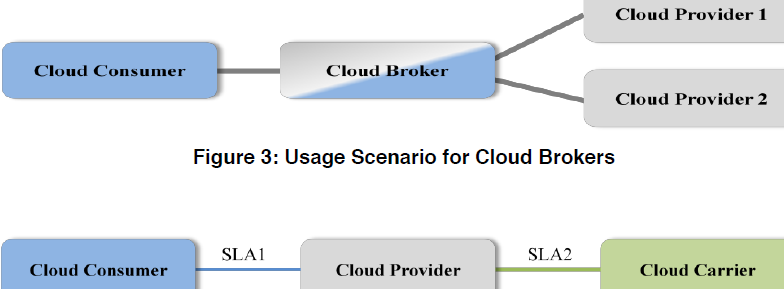
* Service Deployment
* Service Orchestration
* Cloud Services Mgmt
* Security
* Privacy



**Concept**



**Usage scenario:**



**Benefits**

Computing = represented as **Utility**

Reduces capital costs

Reduce need for infra

Focus on ORG core competencies

Agility by on-demand provisioning

Align IT req with business strat quickly

**Cloud Security Alliance**

* Top threats Working Group (collating + issuing guidance on main threats faced)

**Treacherous 12**

1. Data Breaches (confidential info compromised, loses control)  
   - Bitdefender, customer creds compromised due to vuln in cloud app
2. Insufficient Identity, Cred & Access Mgmt (no 2fa, weak pw)  
   - scrape Github looking for cloud service creds
3. Insecure Interfaces and APIs  
   - US IRS (internal revenue) exposed 300k
4. System Vulns  
   - heartbleed
5. Account Hijacking (new means of atk-ing victims using traditional methods, fraud, phishing)  
   - Code Spaces’s AWS acct compromised
6. Malicious Insiders (increasing lvl of access, segregating duties, effective logging)  
   - non cloud, like Edward Snowden
7. APT (extended periods of time, stealth, move laterally)  
   - carbanak attack, bank internal sys, 8M per bank
8. Data Loss (intentional/unintentional)  
   - 2011, AWS EC2 crash = significant data loss
9. Insufficient Due Diligence (exposes to commercial, financial, technical, legal, compliance risks if adopt too fast, designer not familiar with cloud)  
   - 2013, Nirvanix bankrupt and shut in less than 2 weeks, customer need to move
10. Abuse & Nefarious Use of Cloud Services (use for DDOS atks, email spam, phishing campaign, bruteforce of stolen cred db)  
    - Can get collateral damage  
    - DDoS can generate 100s of Gbps, bringing part of internet, services residing on targeted servers to halt.
11. DoS, DDoS (smoke screen for other atks)  
    - Feedly, Evernote, Deezer got DDoS
12. Shared Technology Issues (increased risk of having data + processes reside on shared platform, single vuln, compromise entire cloud)

- VENOM buffer overflow vuln = execute code in hypervisor’s security context

**Security Guidance for Critical Areas**

* Advocate use of risk-based approach
* CSA provides framework to eval initial cloud risks and inform security decisions
* Breaks down into 3 high level section, 14 diff domains

Identify the Asset

* Cloud assets = data, application/func/process
* Key use of cloud service = move info/trans/processing
* 1st step = determine what exact data/functions is considered for cloud

(prevent scope creep)

Evaluate the Asset

* Importance/sensitivity of data/function
* Assess CIA req of asset

Map Assets to Deployment Models

* Uds asset’s importance, assess which deployment model = appropriate

Evaluate Potential Cloud Service Models

* Degree of control (SaaS, PaaS, IaaS)
* Any other specific req.

Map out Potential Data Flow

* Btwn ORG, Cloud, Customers
* Essential to uds
* Identify any risk exposure

Section I: Cloud Architecture

Domain 1: Cloud Computing Architectural Framework

Section II: Governing in the Cloud

Domain 2: Governance and Enterprise Risk Management

Domain 3: Legal Issues: Contracts and Electronic Discovery

Domain 4: Compliance and Audit Management

Domain 5: Information Management and Data Security

Domain 6: Interoperability and Portability

Section III: Operating in the Cloud

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery

Domain 8: Data Centre Operations

Domain 9: Incident Response

Domain 10: Application Security

Domain 11: Encryption and Key Management

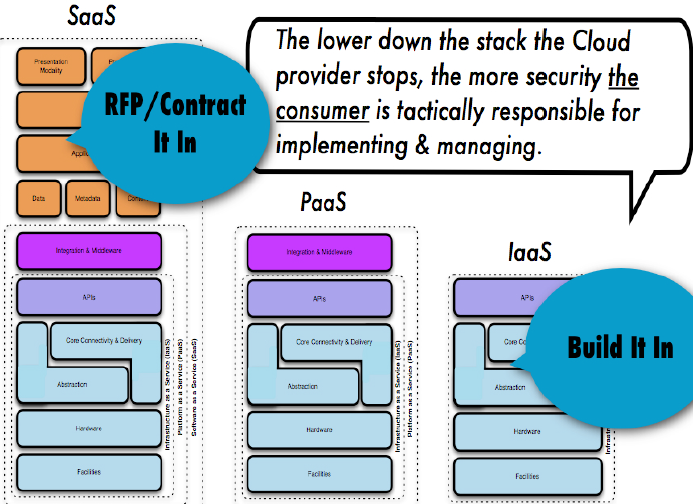
Domain 12: Identity, Entitlement, and Access Management

Domain 13: Virtualization

Domain 14: Security as a Service

Domain 1: Cloud Computing Architectural Framework

* Securing cloud apps + services
* Same as any other IT env
* Key diff = which model (SaaS, PaaS, IaaS)



Domain 2: Gov & Enterprise Risk Mgmt

* Extension of ORG overall corporate gov
* Development of agreement btwn provider and customer

Domain 3: Legal Issues: Contracts/EDiscovery

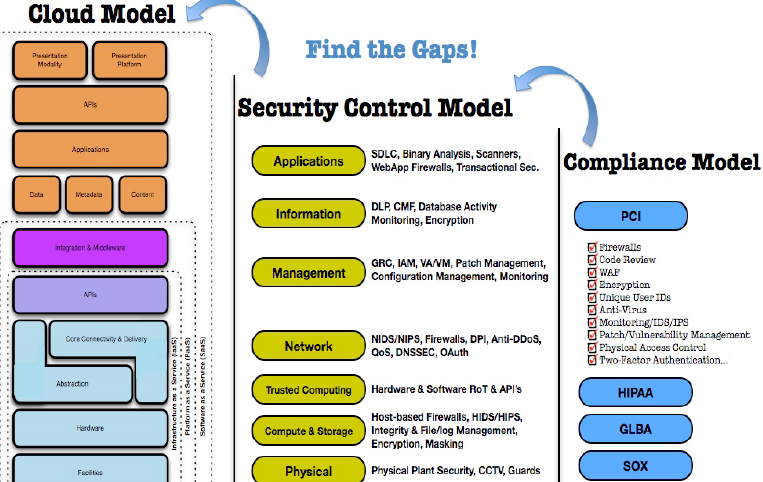
* GDPR, obligation to provide security passed to subcontractors

Domain 4: Compliance and Audit Mgmt

* Regulatory implications
* Assignment of compliance
* Capabilities for demo compliance
* R/L btwn customer/provider/auditor

Domain 5: Info Mgmt and Data Security

* Uds the cloud storage architecture = help to determine security risk + potential controls
* Data encryption = attention to key mgmt.



Domain 6: Interoperability and Portability

* Degree of interoperability = if u migrate to another CSP easily
* Use virtualization to remove hw lvl concerns
* Store unstructured data in established portable format

Domain 7: Traditional Security, BCP, DRP

* Identify physical security func, HR security func, BCP, DRP

Domain 8: Data Center Ops

* DC can be built around indiv “application misisons” (HIPAA or PCI)

Domain 9: IR

* Is level of incident response possible
* Efficient, and effective handling of sec incidents
* Depends on size of client

Domain 10: App Sec

* Security over the lifetime of app

Dev for Cloud = diff from Traditional Hosting

Domain 11: Encryption & Key Mgmt

* How these encryption processes work, Org manage their keys, using crypto service from another source

Domain 12: Identity, Entitlement and Access Mgmt

* Multiple sources of identity, related attributes = critical when cloud is public
* Federation based on open standards (SAML/OAuth) if possible

Domain 13: Virtualization

* Types of virtualization the CSP uses
* Should secure each virtualized OS, hardening software in each guest instance

Domain 14: Security as a Service

* Centralize security service (SecaaS)

**Security benefit of Cloud (by ENISA)**

European network and info sec agency

* 8 key areas = beneficial

**Security measures = cheaper = implemented on larger scale**

* Defensive measures, filter/patch/hardening
* Human resource + management + vetting (by large companies like Google/Amazon)
* Hw + software redundancy
* Strong Auth + RBAC

**Security as a Market Differentiator**

* Security = primary concern
* Choice based on security, CIA
* Strong driver for CSP to improve security practices

**Standardised Interfaces for Managed Security Service**

* Large CSP offers MSS
* Creates a more open/readily avail market for security service
* Can switch providers easily with lower setup costs

**Rapid Smart Scaling of Resources**

* Can reallocate resource for security purpose
  + filter, traffic shaping, encryption
* Increase support for defensive
* Limit effect on some attacks

**Audit + Evidence Gathering**

* IaaS support on-demand cloning
* Breach – can take image of live VM
* later forensics analysis, less downtime
* decreased cost of security incident
* cost effective storage for logs

**More Timely/effective/efficient update + defaults**

* can be pre hardened/updated with patches
* rolled out homogenously
* minimise window of vuln

Audit + SLAs = force better Risk Mgmt

* penalties in SLA = quantified, provide a motivation for more rigorous IA + risk assessment
* Frequent audit on CSP = increased exposure of risk

**Benefit of resource concentration**

* Increased benefit of reducing cost of physical permiterisation and physical access control
* Easier+cheaper of security policy

**PCI-DSS**

**DEF:** developed to encourage & enhance cardholder data security + facilitate broad adoption of consistent data security measures globally

**- Baseline of technical + operational req designed to protect cardholder data (min set of req.)**

- All entities involved in payment card processing

**Includes:** merchants processors, acquirers, issuers, service providers

Min set = 12 req (6 categories) + respective testing procedures = into a security assessment tool

**Additional** controls + practices (further mitigate risks)

Key Goal = compliance

**12 Requirements**

1. **Build + maintain a secure network & systems**
2. FW config
3. no default sys pw + others
4. **Protect Cardholder Data**
5. Protect STORED ^
6. encrypt transmission of data (over public/open network)
7. **Maintain a Vuln Mgmt Program**
8. Protect sys against malware, update AV
9. Dev + maintain secure sys + app
10. **Implement Strong Access Control Measures**
11. Restrict access to cardholder data by business NTK (need to know)
12. Identify + auth access to sys components
13. Restrict physical access to cardholder data
14. **Regularly Monitor & Test Networks**
15. Track + monitor all access to network resources + cardholder data (logging, 1 yr)
16. Test security systems + processes
17. **Maintain an Infosec Policy**
18. Infosec policy addressing infosec for everyone

Applies STORED, PROCESSED, TRANSMITTED

Account data = **cardholder data** + **sensitive auth data**

**Cardholder data** (CAN STORE, unreadable)  
- **PAN** (primary account number) = KEY!

\*PCIDSS applies to this, wherever it is

- cardholder name

- expiration data

- service code

\*Service = 3/4 digits on magstripe

**Sensitive Auth Data (CANNOT STORE)**

- full magstripe track data  
- CAV2/CVC2/CVV2/CID

- PINs/PIN blocks

**Various verification values =** verify possession

PIN & PIN block = used to authenticate (2FA)

PCIDSS !supersede local/regional law

**PCI DSS security req = apply to all system component**

**System component:**

* System that provide security services (auth)
* Facilitate segmentation
* Impact security of (DNS, web redirect) of CDE
* Virtualization components such as VM, virtual switch/applicance/desktop/hypervisors

**Cardholder Data Environment CDE**

* Ppl, processes, tech
  + Store/process/transmit cardholder data or sensitive auth data
* Network component
* Server types (web/app/db/auth/mail)
* App (all purchased/custom apps, internal/external)
* ANY OTHER devices/components to CDE

**1st Step = determine the scope**

- Identify all locations/flows of cardholder data

- Annually/Prior to annual assessment

- All cardholder data !exists outside CDE

**Network Segmentation**

* isolating CDE from entity != PCIDSS req.
* but, may reduce scope/cost of assessment
* reduce cost/difficulty of implementing+maintaining controls
* risk of ORG

No network seg = entire ORG network is in scope

Allows network seg = different physical/logical means

Effectively network seg = **Business Needs + Process for CD clearly understood**

Restriction of CDE =

* Elimination of unnecessary data
* Consolidation of necessary data
* Reengineering long standing business practice

Assessor need to verify seg = adequate

Wireless tech = allowed, but specific testing procedures (eval need for tech against risk, only for non-sensitive data transmission)

**3rd party/Outsourcing**

* Report on Compliance (ROC) documenting role of each service provider, identifying req. applies to entity/service provider

- Cloud/3rd party initially not accepted, now is OK

2 ways of validating compliance

1. 3rd party undergo PCIDSS assessment themselves, provide evidence
2. No own assessment, review service each customer’s PCIDSS assessment

**ROC:**

* **Executive summary**: aka description of business/network diagram
* **Scope of work and Approach**
* **Details on Reviewed Env**
* **Contact information & Report Date**
* **Quarterly Scan Results** (last 4 most recent scans avail, all externally accessible IPs)
* **Findings and Observations**

**Open Items**

* Non-compliances issues
* **Need to address, before validation**
* Allow continue of business, need pay fines
* **Assessor = need to reassess (validate necessary updates)**

**Main part taken by tables**

**3 tables**

* **PCI DSS Req**
* **Testing Procedures**
* **Guidance**

High level, **intent** of req. NOT IN EXAMS

12 Requirements

Criticism for PCIDSS

* PCI is a distracter from security & risk mgmt.
* Data breaches prove PCI DSS useless
* PCI is just security theatre
* PCI a dumb checklist

Compliance/Regulations forces companies to take security more seriously, sells more products/services

**BYOD**

**- business policy**  of employees bringing personally owned mobile device to work + use those device for access privileged company resources (email/files/db)

Trend

* Seen in reality in ORGs
* Improves productivity (for some)
* See company as flexi/attractive

Risk?

* Can result in data breaches
* Lose device = potentially lose data

Pros

* Reduced cost to buy High End Devices
* Better care (if own device)
* Take up new tech FASTER (than purchasing cycle)
* Choose own tech to use (not company standard)
* Exclusive control over device (some prefer)
* Can do BYO(App) – where app they find useful

Cons for companies

* Might not be as secure
  + Security experts labelled BYO(Danger/Disaster)
* Need to pay for employee’s service/tariff (inc personal use)

Cons for employees

* Company request certain control (to improve security)
* Expense = by employees, not company?
* Employee = responsible for repair (dmg at work)?

Mobility (on rise) + (more complicated)

Increase in Complexity = targeting complicated apps

* Bank account
* Corporate IP
* Personal Info

Mobile Malware ^ 155%

ORG = need for security/compliance policies

Survey on Mobile Devices in Enterprise Infra/Apss

9.1% complete, 3.9% = no idea

Biggest = LACK of awareness

BYOD policies = 49% too basic, insufficient

Complex Issues

* Legal/Policy = manage BYOD
* Device = compromised?
* Which App = allowed?
* Actions = taken? Removal from corporate? Device wipe ? (if leave company)
* Can company image the device ?
* Org = handle personal information ?
* Staff on corporate app = fired ?

Policies support BYOD = YES(standalone) 17%, YES (existing)24%, SortOf26%, No31%, DontKnow3%

Tools Used to manage risks

* Employee Education
* Logging + Mobility
* MDM
* Network access control
* Guest networking
* Config Controls
* Endpoint Integrity Checking
* Endpoint Malware Protections
* Endpoint Security Tools
* Application Controls

Mobile Policies (Topics)

* Access/Auth
* Acceptable Usage / Employee Education
* Email Acc
* Config
* Stored Data
* Malware Protection
* Apps
* Guest Networking
* SMS

BYOD as a Future

* Different employees, different platforms

BYOD Strategy Requirements

* LAN/WLAN
* MDM + security app
* Virtual Desktop Infra / Virtual Desktop = centralise secure software/apps/pref
* Data centre infra = support key virtualised & non-virtualised solutions
* Training = educate appropriate usage

**Key Benefits**

* COST EFFICIENCY (rapid turnover, employee = allowance, less time on procurement)
* CHOICE (more options, open/flexible) – network requirements = for diverse range
* MOBILITY (Hotdesk, diff sites, travelling)

**BYOD for Infosec**

* Prohibit personal device != solve problem
* WHO OWNS? (byod = user, past = company)
* WHO MANAGE? (company or user?)
* WHO SECURES device? (Accountability don’t go away, DATA is still company owned)

**CORPORATE DECISION = to allow BYOD**

**which Level = corporate culture + regulatory req.**

**\***IBM bans Dropbox and Siri

BYO(Software) – non-company, cloud SaaS to collaborate

* Data might fall into REGULATORY
* Eval how cloud provider transport/store data

Cost **Reduction/Increase (2012 survey)**

* > 2/3 IT professionals = increase costs
* < ¼ IT professionals = reduce costs
* 43% = virus into network
* 26% = concern about losing device
* 22% = concern about stealing data

WHOSE DECISION = BYOD

* Higher level than IT/infosec in ORG

Consumer grade = lack controls in corporate

No. of device management (n software) = **increase** costs

**Security Challenges**

* Mobile nature/lost devices
* Personal usage = RISKIER usage
  + Virus, hack
  + Shared device
  + Lack of security knowledge (config/patch/AV)
  + Riskier ENV (always admin rights)
  + Always in use
* Multiple device types & OS
  + Need to treat/config/secure different
  + Different Lvl of security risk
  + Constant change (new devices)
* Jailbroken/modded/rooted device
* BEYOND the device
  + Offsite data trf
  + Apps
  + Social media access/engineering/hacking
  + Device = portal to entire ORG network

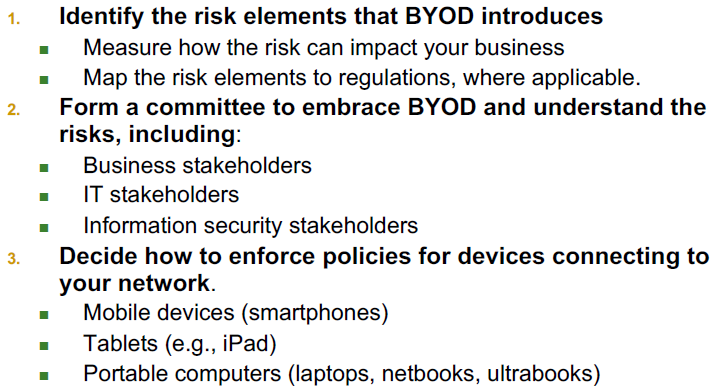
**Security Challenges – consistency/legal**

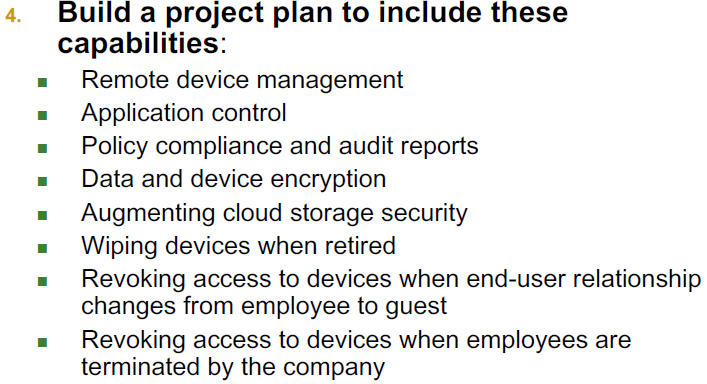
* Reasonable security factors
  + Sensitivity of personal info
  + Foreseeability of risks
  + Likelihood of damage
  + Cost of preventive measures
* Specific security controls = (by law/contract)
  + Mass personal info protection law
* Comply with own policies
  + Acceptable risk
  + Subjective reasonableness

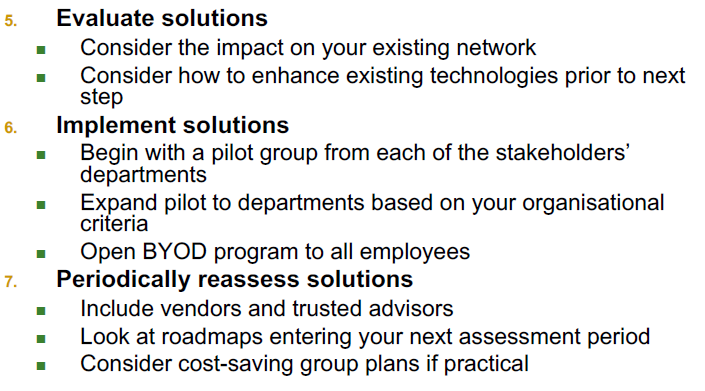
Securing BYODs – HOW?

* Same as devices on the network
* Strong passcodes
* AV protection, DLP
* Full disk encryptions, removable media, cloud storage
* MDM to wipe sensitive data if lost/stolen
* App control

**7 Steps of BYOD plan**







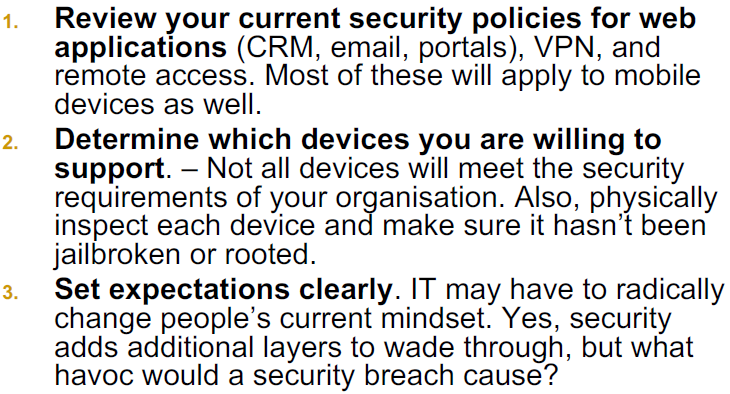
**2 categories security risks**

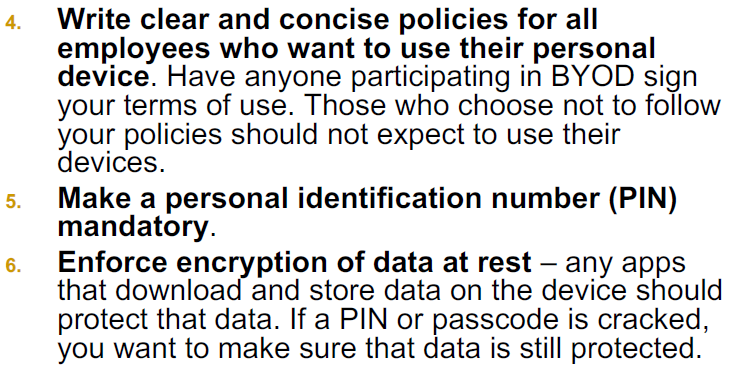
* **Device Risks** (new tech with local/cloud storage which ORG has little/no control)
* **App risks (**3rd party apps with corporate data, or own in house apps as well)

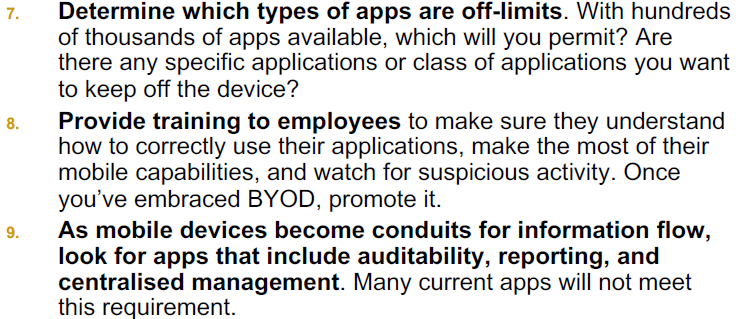
**4 Steps in securing BYOD**

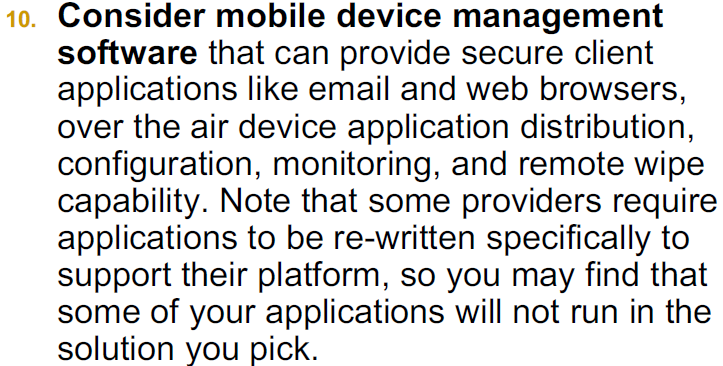


**10 steps to Secure BYOD Policy**









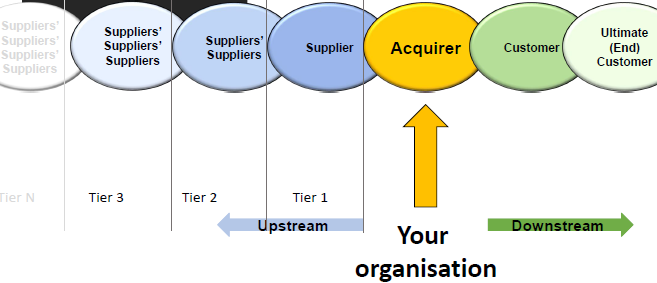
**Security & Supply Chain**

Supply chain = global

80% goods = ocean shipping

Process = complex

Produce smt very complex



**Physical** = network of ORG involved, through upstream + downstream linkages in diff processes and activities that produce value in form of goods & services in the hand of customers

**Information** = full set of elements (tech based, process specific, ORG in nature) that are necessary to:

* Collect info from discrete processes
* Transform information from data to knowledge
* Distribute info efficiently and in a timely manner to appropriate data consumers

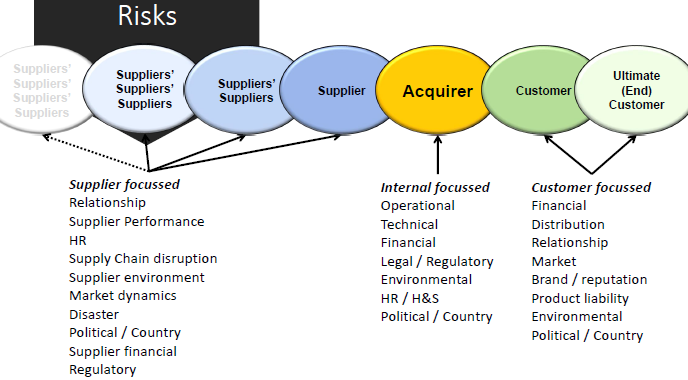
**Supply Chain Risk Mgmt**

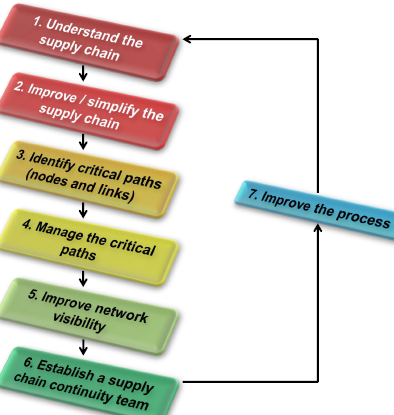
* Keep shareholders happy, disruptions to minimal
* 2/3 suffers from supply chain failures

= Avoiding loss of customer confidence, erosion of shareholder value resulting from supply chain disruption

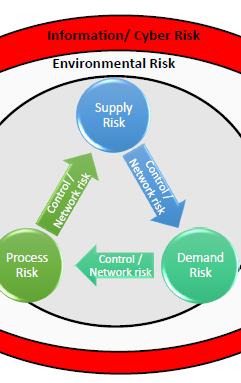
= Identification and mgmt. of risks within the supply chain and risks external to it, through a coordinated approach amongst supply chain members to reduce supply chain vulnerability as a whole

**Risk** = possibility + hope of gain, depending on context, significant gains expected from taking a risk. Risk cannot be defined a negative OR unwanted expectation



**Supply Chain Risk Mgmt Process**

**\***Not stuff, ppl also



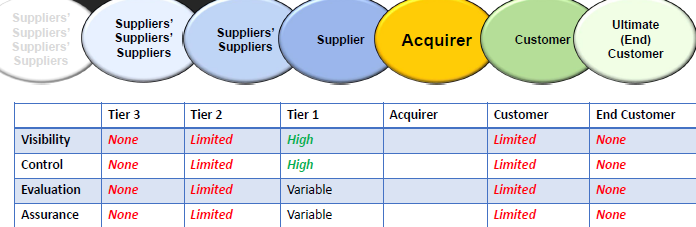
Demand risk = how to know forecast is correct

Env Risk = trade links, floods, fires, laws

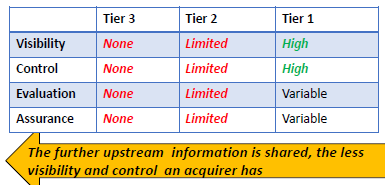
Information/Cyber Risk = CIA

**Supply Chain Information Security Issues**

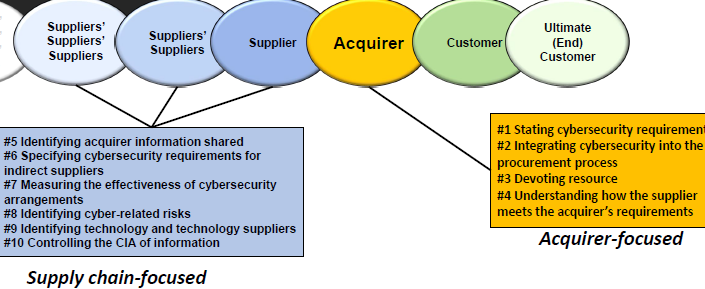
* impt stuff like Intellectual Property



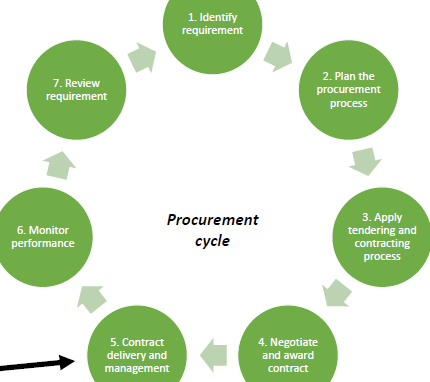
e.g. Blueprints send down from Acquirer to Tier 1, then Tier 2/3. No control/sight = blueprint becomes “public”

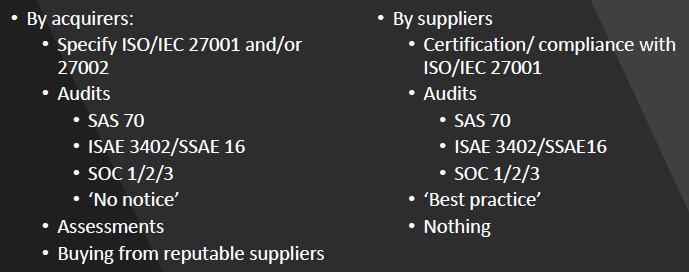
a

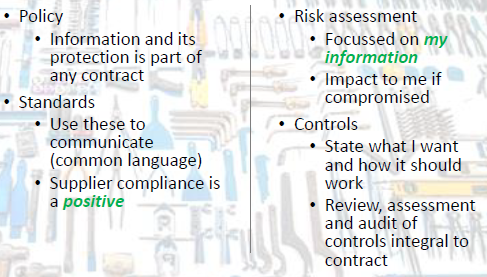
ORGANISATION/Acquirer



Information Security = inside 5.Contract Delivery and Mgmt

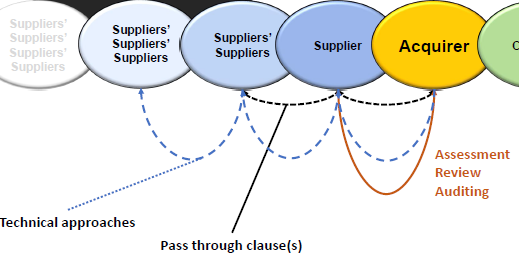






Typical Protection Approaches

* Assessment Review Auditing
* Pass Through Clauses
* Technical Approaches

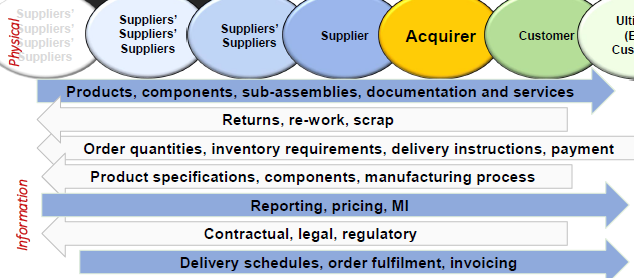


New Approach = Follow the INFO

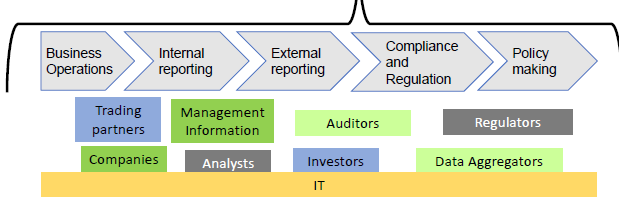
* Supplier centric = difficult (even when small numbers) – 100s to 1000s of them = impossible
* Information is the most impt (asset, value)
* Info = shared for supply chains to work
* Targeted by (criminals, hacktivists, competitors, nation states)
* Protecting SYS not enough

Share info = Who, What, When, Why, Where, How

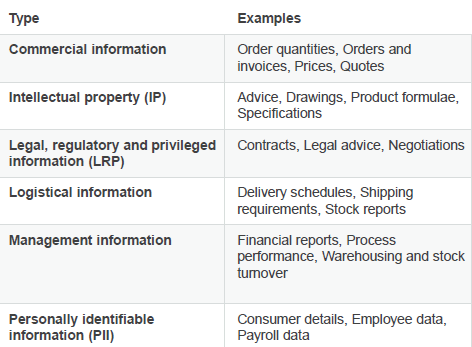
* ALSO = How much access to info?
* ALSO = how is shared information PROTECTED by those who receive it?



ORG info in supply chain



Types of INFO in supply chain (use these information to categorize protection, and plans)

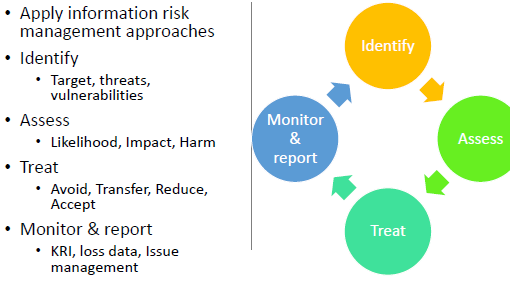


Info Centric Approach

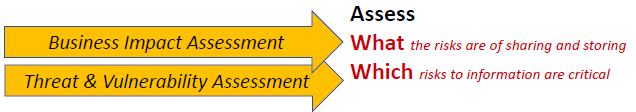


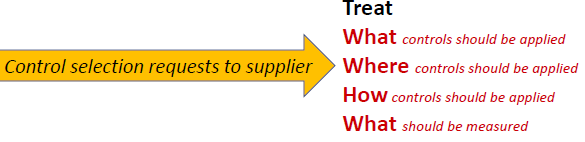
MOST IMPT= WHAT info is shared

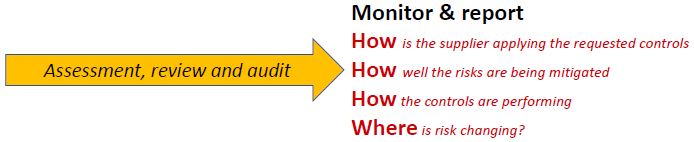
Risk Mgmt = Follow the information









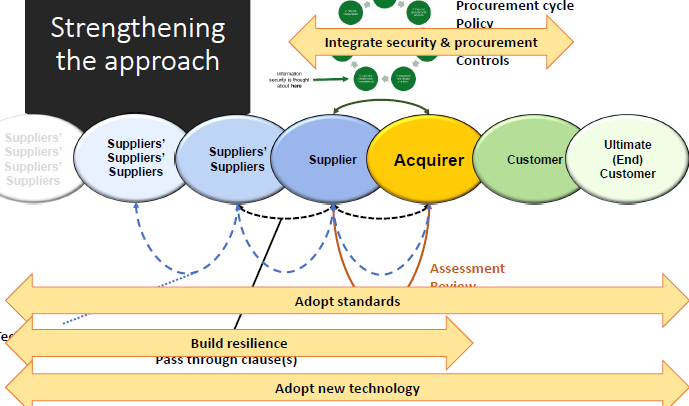


**Benefits**

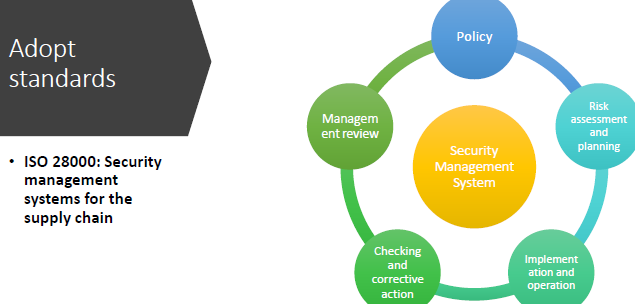
* many suppliers do not process/store/access/transmit/handle very sensitive/critical supplier info
* Info + info risk = can categorize suppliers
* Info risk = focus resources on suppliers and info that high risk

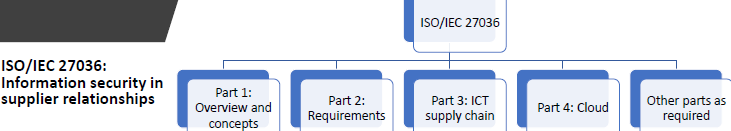


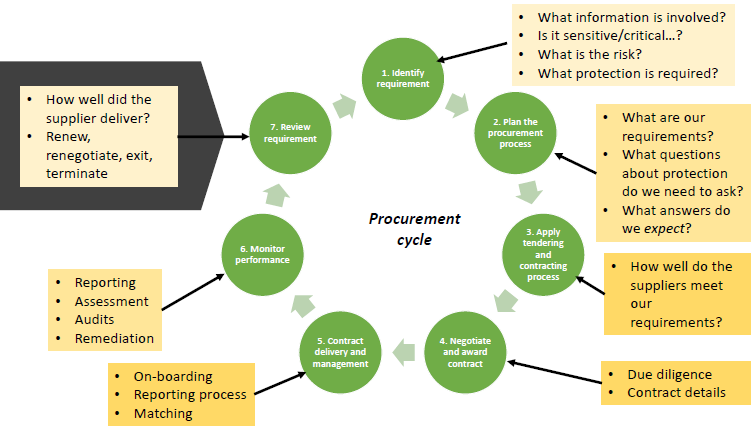
* For existing contracts
  + Build on/align with current business process
  + Focuses effort on info that causes high impact if compromised
  + Filters/breaks up ORG contracts into manageable chunks
* New Contracts
  + Select info security arrangements driven by risk
  + Sets a consistent approach in selecting and measure infosec arrangements
  + Defines terms + conditions upfront



Standards:



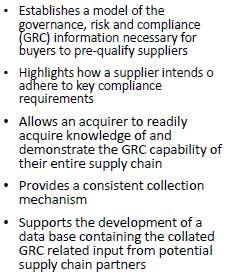




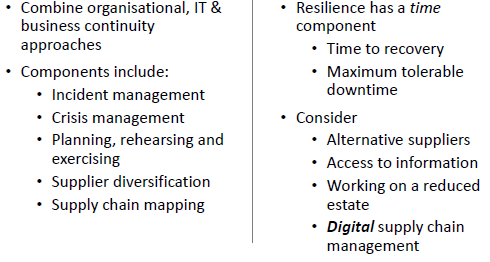


Can match controls/risk treatment TO RISK – logical flow

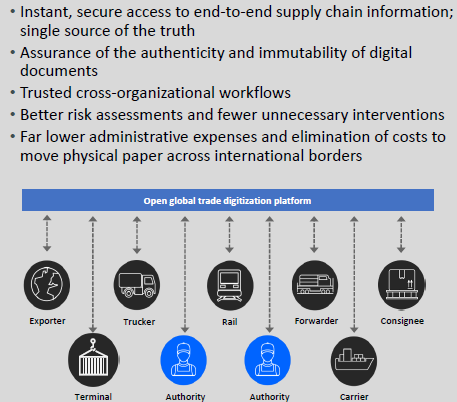


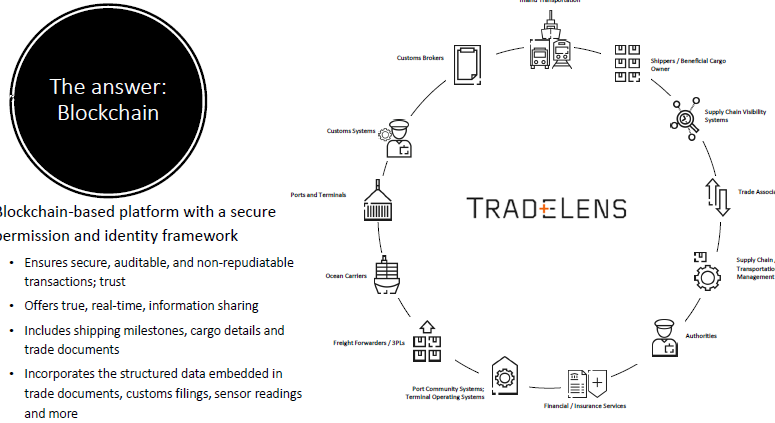
**Know your suppliers**  


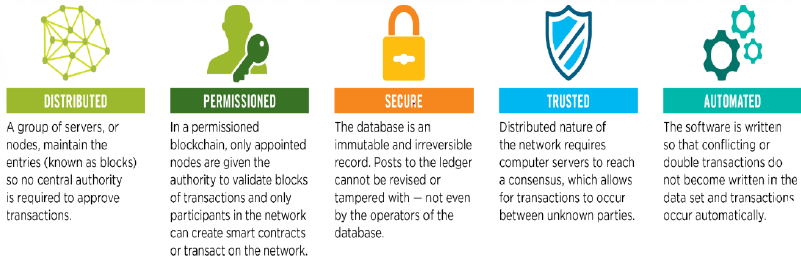
**Resilience Approaches**



New:

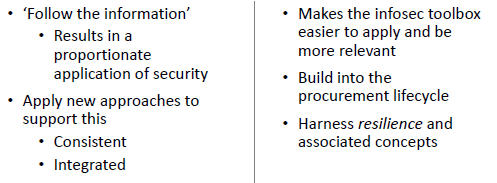




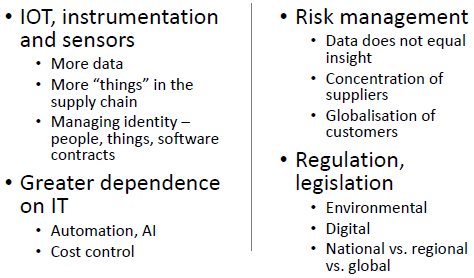


CISO need to focus on the WHOLE supply chain

**Summary**   
supply chain = IMPT  
2 key components (phy + info)  
Supply chains HAVE risks  
Info + protection = under-appreciated risk (difficult to know where to start, current tech = limited)



Challenges for FUTURE:



**Big Data, As a Security Solution/Problem**

A lot of data, in social media, communication, web-based

**Challenge**

= not possible to store all data

90% = unstructured

**Observation**

RDBMS (relation db mgmt. syst) = challenged to scale

Big data = when size of data becomes part of the problem

Big data tech = new gen of tech and archi, designed to extract value from very large volumes of wide variety of data, enabling high-velocity capture, discovery, and/or analysis

Big data = **VOLUME, VARIETY, VELOCITY**

**3V**s

**Volume** – lower cost of e-channels = collect 10x quantity of data

**Velocity** = point of interaction speed, pace data used to support interactions & generated by interactions

**Variety** = no greater barrier to effective data mgmt will exist than variety of incompatible data formats, non-aligned data structs, and inconsistent data semantics

**Veracity (4th)** – Act upon info (if you don’t trust) ? Establishing trust in big data = huge challenge as variety and size grows

**Value (5th)** = Provides user with insights or useful value, something to use

**Variability (6th)** = initial struct and content of data change over time, similar data from diff sources can exhibit wide variability in struct and format, allows org form, and transform for analysis

**Structured** = easy to model, enter, store, query, process, visualize

**Semi-Structured** = in a format (XML/JSON) but not rigid model

**Unstructured** = free text, books/articles/docs/emails/media

NoSQL (Not only SQL) – Non-relational approach

Power = for specialised solutions (faster/scalable)

V = generally less querying power than SQL

Able to handle semi-struct and un-struct data, horizontal Scalability

May Complement RDBMS = can hold vast amt of less valued + less-struct data

Big Data (Composition of data in 1 large source, less work for hackers) = RICH targets

Security Data = Source of Big Data Repo (Logs, IPS/IDS DB)

Big Data has designed without security

MORE security controls in RDBMS than NoSQL

* SQL security = config, MFA, data classification, encryption….
* NoSQL = cell level access label, Kerberos, Access control lists

**5 Security Issues for Big Data**

* **Cyber Security –** could help identify zero day attacks (using data collected)
* **Data in the Cloud** – attractive way to harvest and places more demand on business to get secure cloud sourcing strategy. Cloud = removal of permissions or confidentiality restrictions on original data
* **Consumerization** – metadata, the use of the tech/device. BYOD= security vs productivity. Use Big Data Analytics tools to identify any misuse/unusual access (suspicious activities)
* **Interconnected Supply Chains** – coordinating the contracting + provisioning of business relationships, including outsourcers, offshores,supply chain. Losses control of IP/PII, can use Big data to analyse high risk data
* **Privacy =**  how to demo to regulators on what is collected. If hold foreign data, may fall under foreign rules. Help identify where PII is stored/protected

**BIG Data over** infosec

* Combination of explosion of data, evolution of regulation = change of information gov
* Focus more on information protection
* Infosecurity teams= content aware
* Too much data for ORG to take a blanket approach.

**Security + Privacy challenges for Big data**

* **Random Distribution** (hard to know exact location)
* **Privacy** = assign sensitive data with special priority (now has no such stuff), that will do encryption/blind processing
* **Computations** = extract useful insights by performing specific computations, need to secure + protect these computations to avoid any risk.
* **Integrity =** ensure validity + trust of data
* **Communication** (between nodes/clusters, can extract valuable info)
* **Access Control**

Ways to protect Privacy

* **Rules + Legality –** carefully choose storage + processing location
* **Encryption** (Storage, computation, communication)
  + **Computation** = blind processing or homomorphic encryption. HOMOMORPHIC = process it when it’s encrypted.
* **Authentication (control access to resources)**
* **Metadata + Tagged Data =**  will possibly treat private info different when processing
* **Unstructured Distribution =** separate data from individual related info, prevent extraction of useful insights (in some nodes)
* **Anonymization =** data perturbation + data swapping technique = to protect association of indiv to crit info
* **Tracing Activity =** to protect/supervise stored data = mandatory to log activity performed over Big Data

Big Data VS anti-competitive = if data protection and privacy issues should be assessed in proceedings

* Merger control (Facebook + WA)

Google + DoubleClick = deprive privacy choices

**Big data focus on** making sense on data sprawl and managing data as a whole to support business

Leveraging Big Data in INFOSEC program

“Shelf-life” of data = important

Access to info = real time = as close as possible

Security Policy on Big Data?

* Using Big data tech to aid security
* Protection of Big Data

Data protected at rest? In motion? In use?

Who gets Access? DATA? Analytical OUTput?

Existing policies unlikely to cover new situations

Big Data Security Analysis

* Modern attacks counter traditional security analysis

1 way = Big Data help scanning events on network and servers to find advanced threats. Possibly by scanning network for abnormal events = deviate from baseline

* Need to aggregate data
* Analysing logs, to performing correlation

Use of Big Data = Prevent-Detect-Respond technique (PDR)

* Requires improved techniques for detection
* Where Big data and analytical techniques comes in
* Big data analytics = in infosec+fraud detection
  + 13% knows how to big data, 25% perform big data security analytics

Benefits from Big Data Security Analytics = HIG

Best in class companies = wide range of tech = those companies use a broad range of security tools

= used automated controls = (key aspect of solutions)

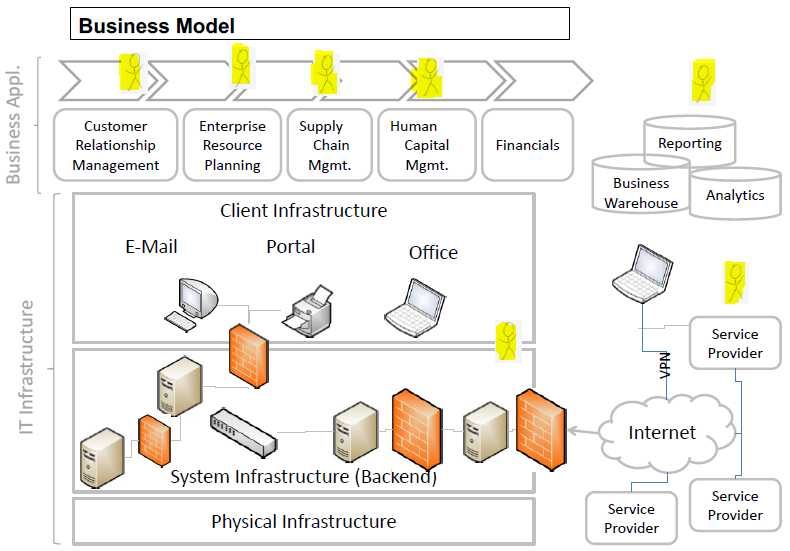
Good security solution =

* how you implement, and for what purpose
* what environment

Security in a business environment

Apps, Process, Analytics

* Business Apps
  + ERP, CRM, Supply Chain, HRM, FI
* Business Processes
  + Order to Cash, Maintenance Process, Complaints Mgmt
* Business Analytics
  + Financial Reporting, Profitability analysis, Fraud detection



What is impt to business?

– Availability, now also security

Security = needs to **explain** to how it helps the business, not to overdo it, at different levels

Security Perspective = Different Roles/Views

* Auditor
* IT Security (Responsible)
* Vendor
* Business/Product Owner
* Hackers
* CEO (KPIs)

Security Requirements

* Derived from business + compliance requirements
* Uds real assets
* Basis for risk assessment
* Need to enforce in complete infra

How to translate BUSINESS req to Security at ALL lvls

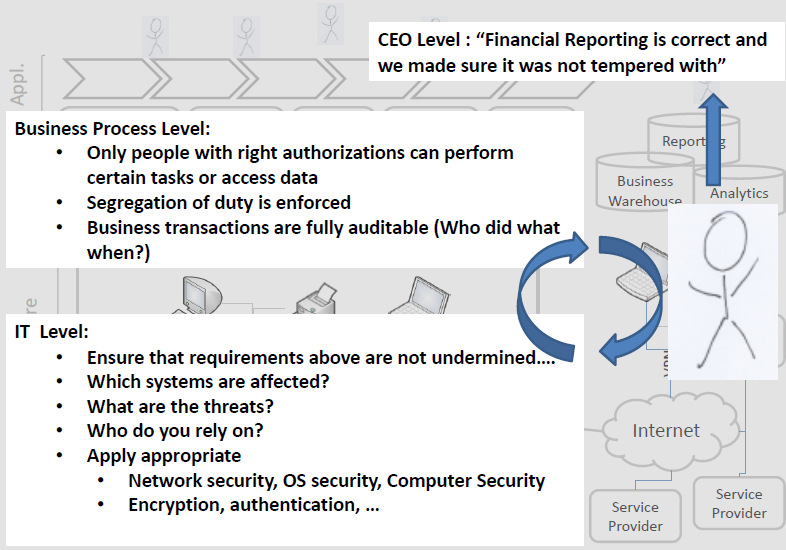
How to ensure END-to-END Security

How much risk is someone willing to take?

Vulnerability Mgmt (person did not communicate)

Equifax = affected by the vulns in APACHE-STRUTS

Needs to work with the Business ppl to solve security problems (not even know the systems are there)



Protection of business ASSETS + COMPLIANCE of rules/regulations = DRIVES business investments

* Needs to justify costs
* According to business plans

COMPLIANCE

* Have to legally = SOX/HIPAA/PCI-DSS/Data protection/GDPR/industry specific
* Show/proof security = ISO27k, Common Criteria
* Clearly structured blueprint
* WHO NEEDS? ORG? or product/service?

Business Process & Application Level

* Design authorizations, roles, identity mgmt.
  + IAM
* Business entities (sales orders)
* Needs audit?

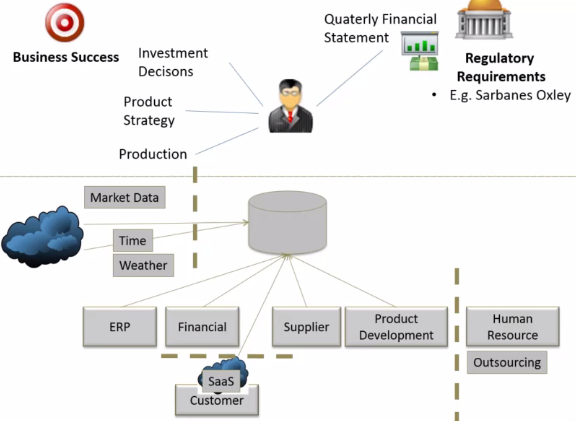
\*Requires uds of app and process

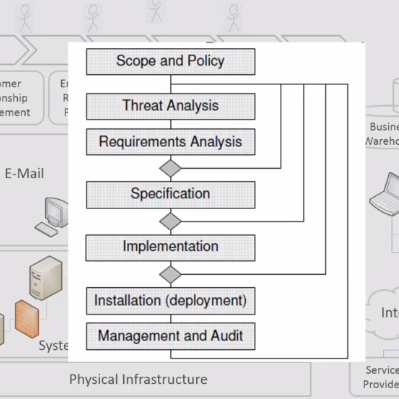
Compliance + Security

* Regulatory
  + Drives business security investments
  + Help uds business env
  + Help identify assets + critical sys
  + Need to consider threat + req analysis
* Complete risk+threat analysis still needed
  + Value of assets for ORG

Basis for Success in Information Society = Right + Accurate information at RIGHT time.

* Helps solve problem
* Helps make decisions
* Allows compliance
* When u need it
* In Real Time
* Ahead of competition





Key Topics

* Challenge for security expert
  + UDS the business context of ORG, operate in compliance, asset, risk assessment
  + UDS security threats, mech, dependencies in all lvls
  + UDS security measures
* Combine 2 into consistent security design
* COMMUNICATE with tech experts + business experts

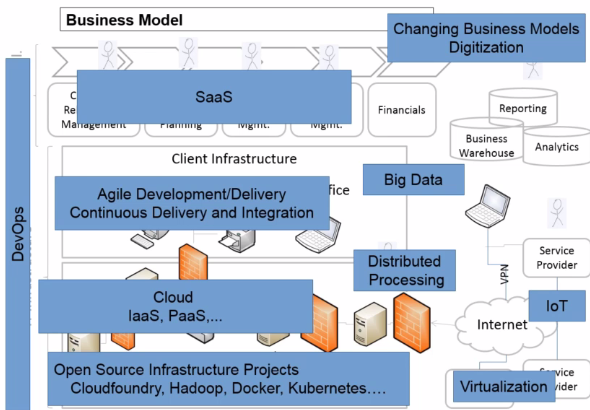
**Impact of current trends**

Deal with changing ENV

* Change in regulations
* Change in tech
* Change in business model
* New trends (cloud/mobile)
* Deal with new threats

UDS impact of changes on security

Security solutions to enable secure adoption



Moving to cloud, - cncf.io

Targetting ORG = APT

* Targeted attack at certain business or ORG
* Hack critical part of security infra
* Use knowledge to atk target
* E.g., RSA/Stuxnet/Diginotar

Do you know you are attack?

Do you know what the DMG is?

Do you have 2nd line of DEF?

Heartleed = high vis, easy to exploit, very difficult to detect.

Fixing bug != sufficient, need replace keys/cert/pw

Revocation != reliable

Y do cars needs brakes? – so can go FASTTTT

What is then a SUITABLE break?