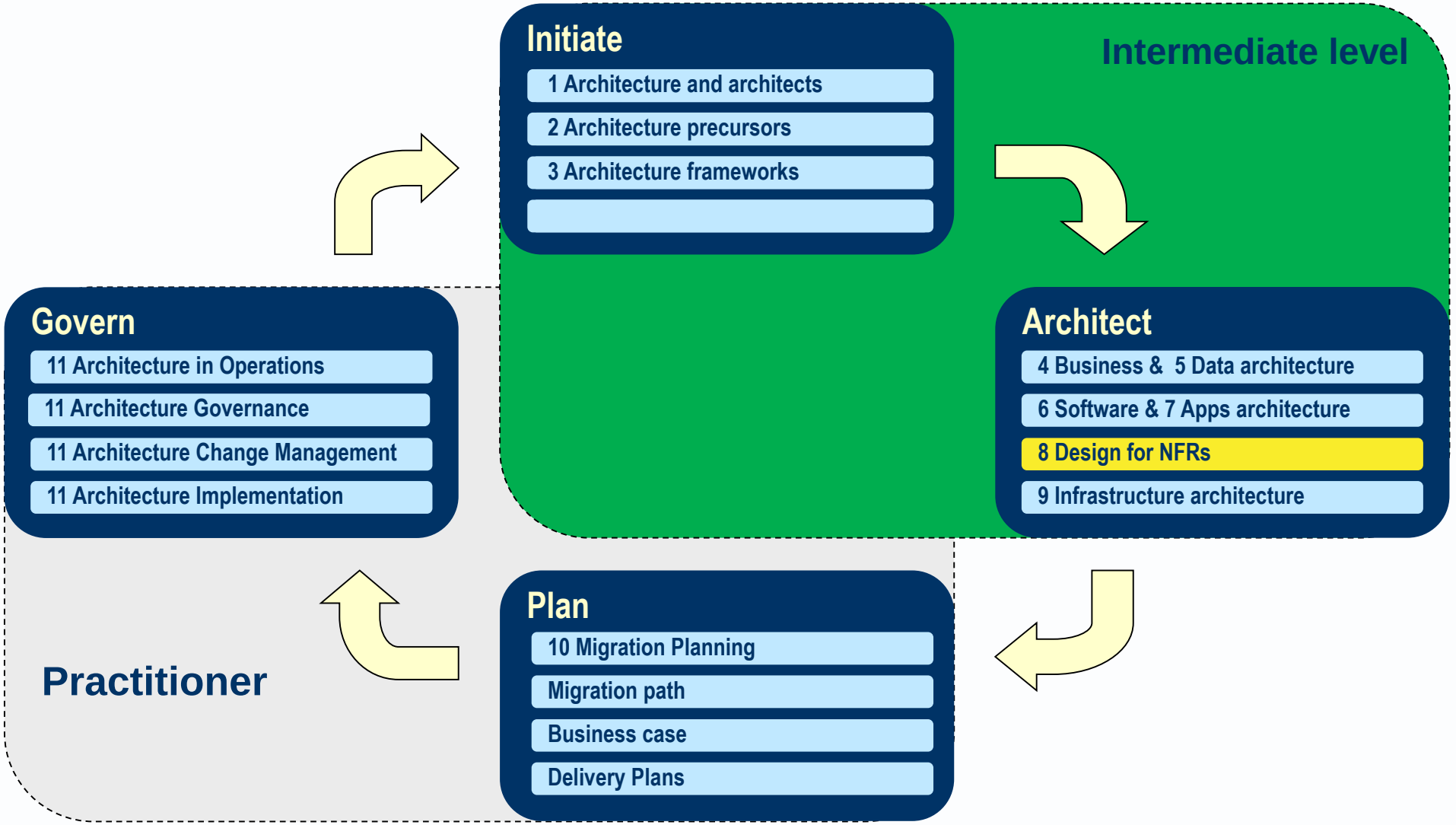
Avancier Reference Model

Design for Qualities / NFRs (ESA 8)

8. Design for NFRs

Avancier



8: Design for Qualities (NFRs)

- This section contains a selection of measures and common techniques that could be relevant in answers to exam questions.

8.1: Non-functional requirement types (NFRs)

- **PARRISSS**
- **UMPIE**

Performance

- [a requirement type] that is subdivided into two measures.

- Throughput: volume or number of services performed in a time period.
- Response or cycle time (aka latency): time taken from request to response or completion.

- Sometimes, improving one measure damages the other.

PARRISSS

- **Availability** [a requirement type] the amount or percentage of time that the services of a system are ready for use, excluding planned and allowed down time.
- Possible measures include MTBF / (MTBF + MTBR), which usually refers to availability at the primary site, excluding disasters.

- **Reliability** [a requirement type] the ability of a discrete component or service to run without failing.
- Possible measures include mean time between failures (MTBF).
- Aside: The measures above are sometimes applied only to platform applications, ignoring faults and failures in business applications.

- **Recoverability** [a requirement type] the ability of a system to be restored to live operations after a failure.
- Possible measures include mean time to repair (MTBR). Usually refers to disaster recovery using resources at a remote site.

PARRISSS

- **Integrity** [a requirement type] a term with four possible meanings defined under “Data Integrity”.
- **Scalability** [a requirement type] the ability for a system to grow with increased workloads.
- **Security** [a requirement type] the ability to prevent unauthorised access to a system.
- **Serviceability** [a requirement type] the ability to monitor and manage a system in operation.

UMPIE

- **Usability** [a requirement type] the ability of actors to use a system with minimal effort.

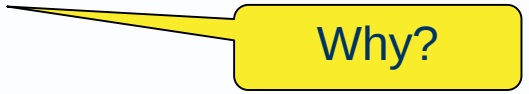
- Aside: Measures include PLUME.
  - Productivity; tasks completed in a given time.
  - Learnability; how much training to reach a proficiency level.
  - User Satisfaction; scores given by users.
  - Memorability; how long to forget how to use the system.
  - Error Rates.

UMPIE

- **Maintainability** [a requirement type] the ability to analyse, then correct or enhance a system.
- **Portability** [a requirement type] the ability to move a system from one platform to another, or convert it to run on another platform.
- **Interoperability** [a requirement type] the ability for systems to exchange data using shared protocols and networks.
  - It may embrace also “integratability” - the ability of interoperable systems to understand each other, which requires either common data types or translation between data types.
- **Extensibility** [a requirement type] the ability to add new features; a kind of maintainability.

8.2 Design for speed or response time

- **Remove bottlenecks**
- The general advice is to look for bottlenecks and tackle them one by one.



- **Remove what slows things down**
- General techniques to minimise or remove:
  - distribution of processors and network hops
  - database accesses, discs (replace by solid state drives)
  - security overheads such data encryption.
  - middleware

Data access optimisations

Caching

- [A technique] that copies persistent data nearer to the user than the original data source.
- Generally good for response or cycle time; can raise data integrity and security concerns.

Database indexing

- [A technique] that creates a list of pointers to stored data elements.
- Some disable indexes during the day to optimise on-line update processes, and enable them at night optimise batch input and output processes.

Analysis of database access paths

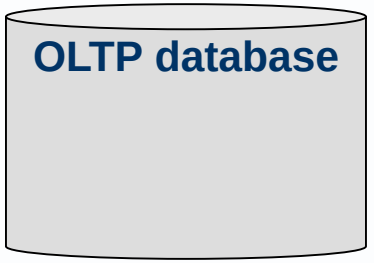
- [A technique] that studies the route of a process through a data store structure.
- Since, a SQL programmer often does not know the access path their procedure takes through a database, it is advisable to use access path analysis and/or employ highly skilled SQL resources for critical database access programs.

Separation of update (OLTP) and reporting (OLAP) databases

Avancier

Normalisation

- Relational data analysis.
- A technique for defining a data store structure that assists data integrity by storing each fact once.
- It also optimizes update processes by minimising redundant data storage.



Denormalisation

- A design technique that optimizes input and/or output processes by structuring a data store structure to reflect the most important input or output data flow structures, at the expense of duplicating some stored data.

Other

Archiving of old data

Throttling of throughput (e.g. 90 customer orders at once)

- To prevent servers being overloaded.

8.3 Design for throughput or capacity

Parallel processing

- [A technique] to increase the amount of processing done in parallel.

Scale up

- [A technique] that increases the power of one node.
- Usually by adding resources, processors or memory.
- Generally good for speed and throughput.

Scale out (aka clustering)

- [A technique] that increases the number of parallel nodes, e.g. adding more nodes to a cluster.
- Usually requires a load balancer to distribute service requests between nodes in a cluster.
- Generally good for throughput; not always good for response time.

8.4 Design for availability (reliability and recoverability)

N+1 design

- [A technique] to add an extra server to a cluster, to insure against failure.

Defensive design

- [A technique] to
- 1. Design a client component so that it does not fall over if a server component does not work properly; typically using asynchronous invocation.
- 2. Design a server component so it does not depend on input data being valid. This means testing input data and preconditions before processing (the opposite of “Design by Contract” as promoted by Bertrand Meyer.)

Backing up

- [A technique] to copy a data store for use if the original fails.
- Or to restore individual files that have been deleted or corrupted.
- Typically the last line of defence, and can be inconvenient to use.

Failing over

- [A technique] that automatically switches over to a redundant or standby system, upon the failure or abnormal termination of the previously active system.
- Failover happens suddenly and generally without warning.
- Procedures must address “fail back” to normal operations.

Design for recoverability

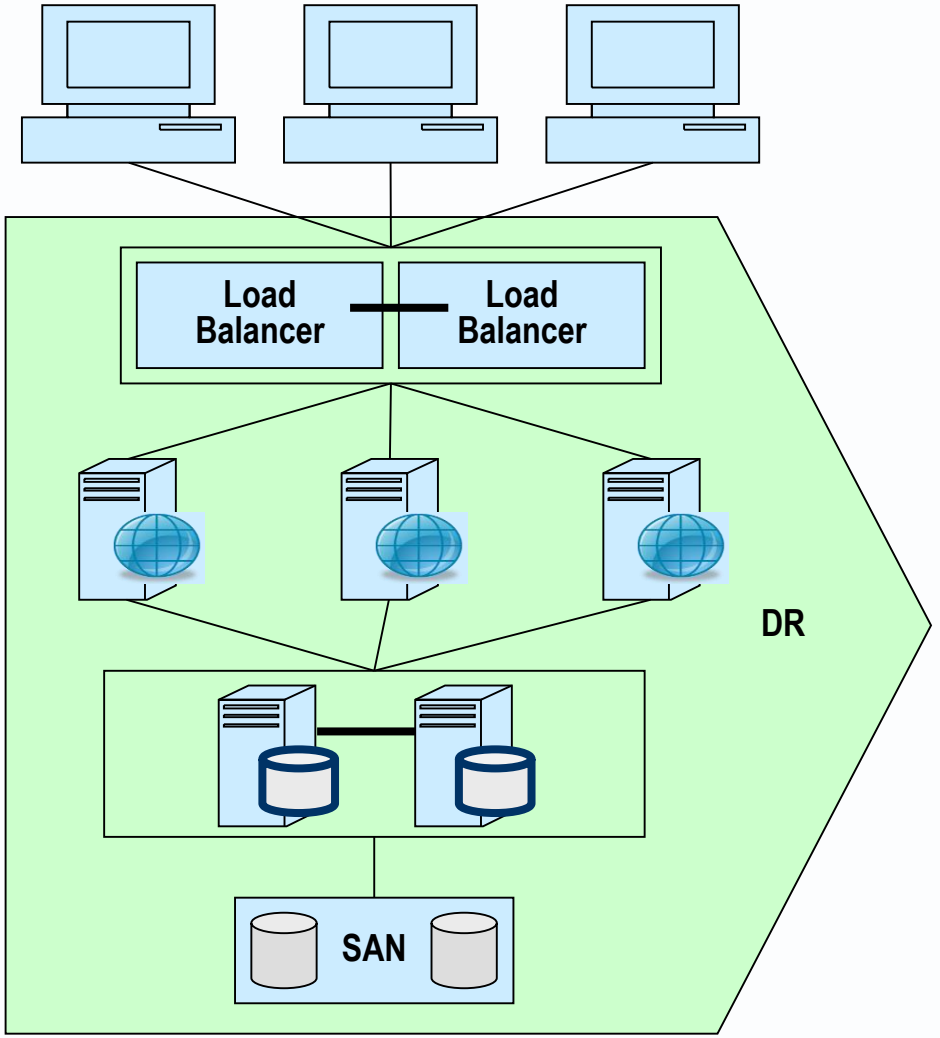
Avancier

Synchronous replication

- replicates data storage in real time
  - needs high bandwidth and low latency
  - limited by distance 150K?.

Asynchronous replication

- replicates data storage off-line
  - makes and keeps copies of data at a remote site
  - operations can be resumed at the remote location using a remote copy.
  - not subject to distance limits.



Design for integrity

- [a technique] such as
  - reducing data replication,
  - normalising stored data,
  - switching on automated referential integrity checks,
  - applying transaction management to update processes,
  - removing caches, and
  - consolidating distributed databases.

Design for serviceability

- [a technique] to instrument applications so that they report on what they are doing, and how well they are doing it.

- Report *business events/transactions*
- How many sales made per minute?
- How many NHS consultant appointments booked by GPs per minute?

8.5 Design for security – business-oriented concerns

- Design of human organisations to protect business systems from unauthorised or malicious access, to maintain the data qualities of confidentiality, availability and integrity.

Design for human and organisational security

- [A technique] defining anything that can be done outside of IT systems to secure business information, such as
  - security guards,
  - locks on doors,
  - passes
  - definition and roll out of policies and procedures.

8.6 Design for security – data-oriented concerns

- Design to protect business data from unauthorised or malicious access, to maintain the qualities of data confidentiality, availability, and integrity.

Data security

- [A concern] that may be defined as **c**onfidentiality alone.
- Or as a combination of Confidentiality, Integrity and Availability.

	Confidentiality	Integrity	Availability	Security Level
Customer	**High**	Moderate	Moderate	**High**
Order	Moderate	**High**	Moderate	**High**
Product	Low	Moderate	**High**	**High**

Data security concepts

Avancier

Information domain

- [an entity] a uniquely identified set of items with a security policy that defines the rules that constrain access to data within the domain.

Security policy

- [a document] that defines which actors have access rights to which data objects in a given information domain – and which security processes or properties are used.

Identity

- [a property] one or more data items (or attributes) that uniquely label an actor. E.g. passport number or user name.

Data security concepts

- **Encryption** [a process] to encode data items (in a data store or data flow) so that they are meaningless to any actor who cannot decode them.

- **Checksum** [a property] a redundant data item added to a message, the result of adding up the bits or bytes in the message and applying a formula. This enables the receiver to detect if the message has been changed. It protects against accidental data corruption, but does not guarantee data flow integrity, since it relies on the formula being known only to sender and receiver.

- **Digital signature** [a property] a cryptographic device that simulates the security properties of a handwritten signature. More secure than a check sum, it is said to guarantee the data flow integrity of a message, since the signature is corrupted if the message content is changed.

8.7 Design for security – application-oriented concerns

- Design to protect business applications from unauthorised or malicious use.

Identify management system

- [An application] designed to ensure only authorised entities can access applications.
- It ensures identification, authentication and authorisation of entities against permissions granted them.

- Consider
  - how the user is informed of their responsibilities associated with using the application, given a copy of the access agreement,
  - how the user can change password, call for help, etc.

What is the right sequence for these 4 actions?

- **Identification**
  - [A process] via which an actor supplies their identity to an authority.
  - It is usually followed by authentication.
- **Authentication**
  - [A process] to confirm that an actor is trusted
- **Authorisation**
  - [A process] for giving access to a trusted actor, based on that actor's known access rights.
  - It is usually followed by access.
- **Access**
  - [A process] that locates data or processes of interest and retrieves them for use.

Authentication

- [A process] to confirm that an actor is trusted - is the entity to which an identity was given. It produces one of four results:
  - true positive
  - true negative
  - false negative (which leads to wrongly-denied access), or
  - false positive (which leads to unauthorised access).
- It is usually followed by authorisation.

Three-factor authentication

- [An authentication] that checks what users remember (e.g. password, mother's maiden name) and carry (e.g. credit card or key) and are (using biometric data).

8.8 Design for security – technology-oriented concerns

- What is done at the infrastructure technology level to protect business application systems from unauthorised or malicious access, to maintain the required data qualities of confidentiality, availability, and integrity.

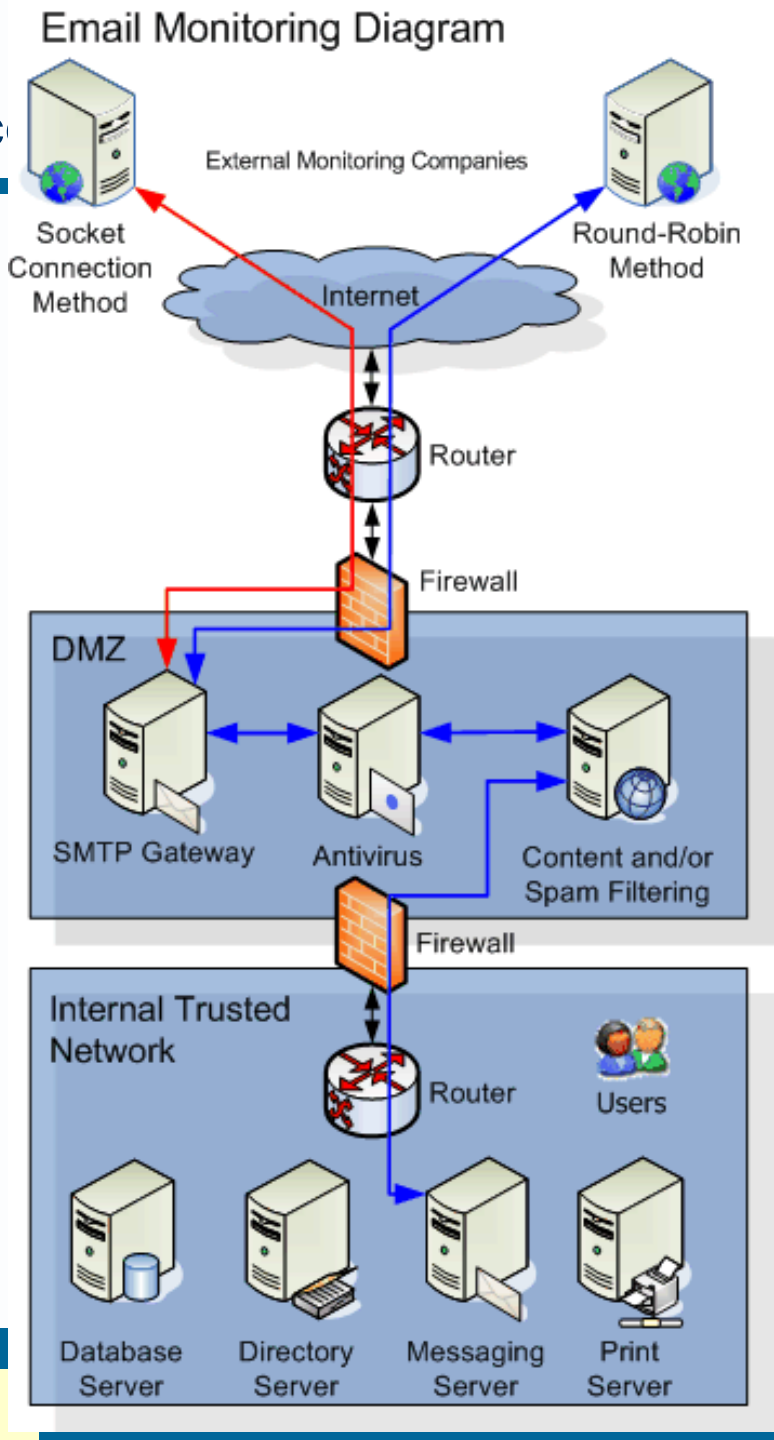
- **IT service functions related security**
  - Identity & Access Management
  - Continuity Management
  - Security Intelligence
  - Digital Forensics
  - Security Analytics
  - Audit, Network Monitoring
  - Compliance Management
  - Training & Awareness Programs, etc

8.8 Design for security – technology-oriented c

- [a technique] for protecting client and server computers from malicious access.

- **Firewall** [a component] at the boundary of a network that can detect, filter out and report messages that are unauthorised and/or not from a trusted source.

- **DMZ: De-Militarised Zone** [a component] of a network, usually between the public internet and the enterprise network.
- It uses firewalls to filters out messages that fail security checks.
- It contains servers that respond to internet protocols like HTTP and FTP.



HTTPS

- [a process]
- a normal HTTP interoperation over
  - an encrypted Secure Sockets Layer (SSL) or
  - Transport Layer Security (TLS) connection.

- This ensures reasonable protection of data content from those who intercept the data flow in transit.

- (Aside: If an HTTPS URL does not specify a TCP port, the connection uses port 443.)

SSL supplanted by TLS
SHA1 supplanted by SHA2

Web site security

- [a process] whereby, for example, a web browser checks the public key certificate of a web server at the other end of an HTTPS connection.

- The aims are to check the web server is authentic (who it claims to be) and that messages to/from with the web server cannot be read by eavesdroppers.

FOOTNOTES

Design for NFRs - Security

Avancier

Design for security	Design for security is addressed elsewhere in this reference model under the headings of business, data, applications and infrastructure architecture..
ISO/IEC 17799	Information technology: Code of practice for information security management.
ISO/IEC 24762:2008	Information technology — Security techniques — Guidelines for information.
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements.

Security: Public key certificate

Avancier

Public key certificate

An electronic document that enables a web server to accept https connections, or [a client?] to verify that a public key belongs to an individual.

It incorporates a digital signature to bind together
a public key with
an identity (the name of a person or an organization, their address, and so forth).

Encrypting File System	Encrypting and decrypting documents.
File recovery	Recovering encrypted files if the EFS certificate is accidentally deleted or damaged.
Server authentication	Verifying the identity of a server to computers that are connecting to it.
Client authentication	Verifying the identity of a computer to a server it is connecting to.
Secure e-mail	Encrypting and digitally signing e-mail.
Code signing	Verifying the publisher of a program. For example, if you download an ActiveX program, its digital signature verifies that it is published by the organization that is listed as the publisher.

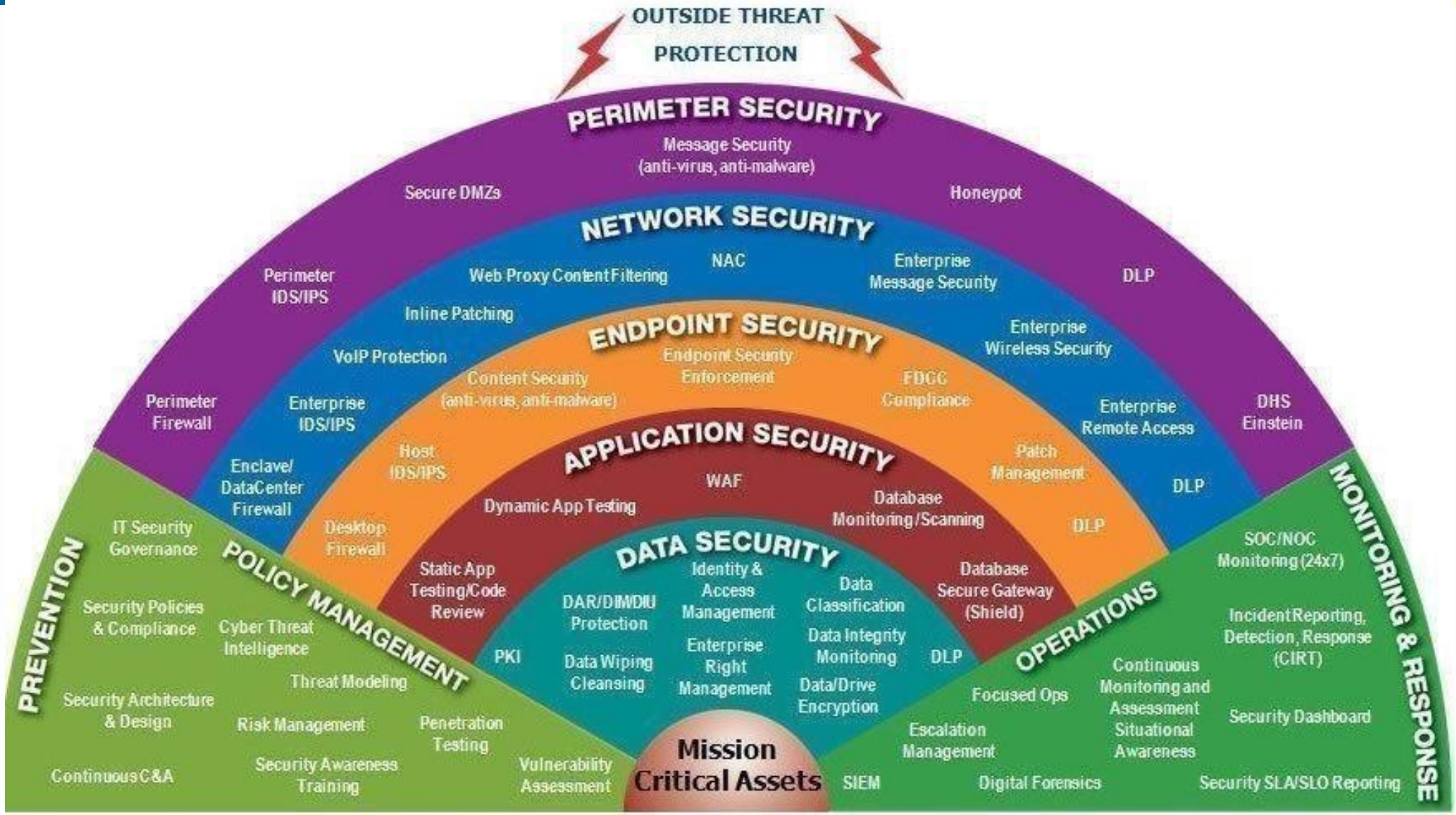
Security: Certificate authority

Avancier

Certificate authority	The web site administrator must get a public key certificate signed by a certificate authority. This signature certifies (authenticates) that the certificate holder is the entity it claims to be. Web browsers are generally distributed with the signing certificates of major certificate authorities, so that they can verify web-server certificates.

“A Layered Cybersecurity Approach” (Infographic) from the Cyber Security Hub

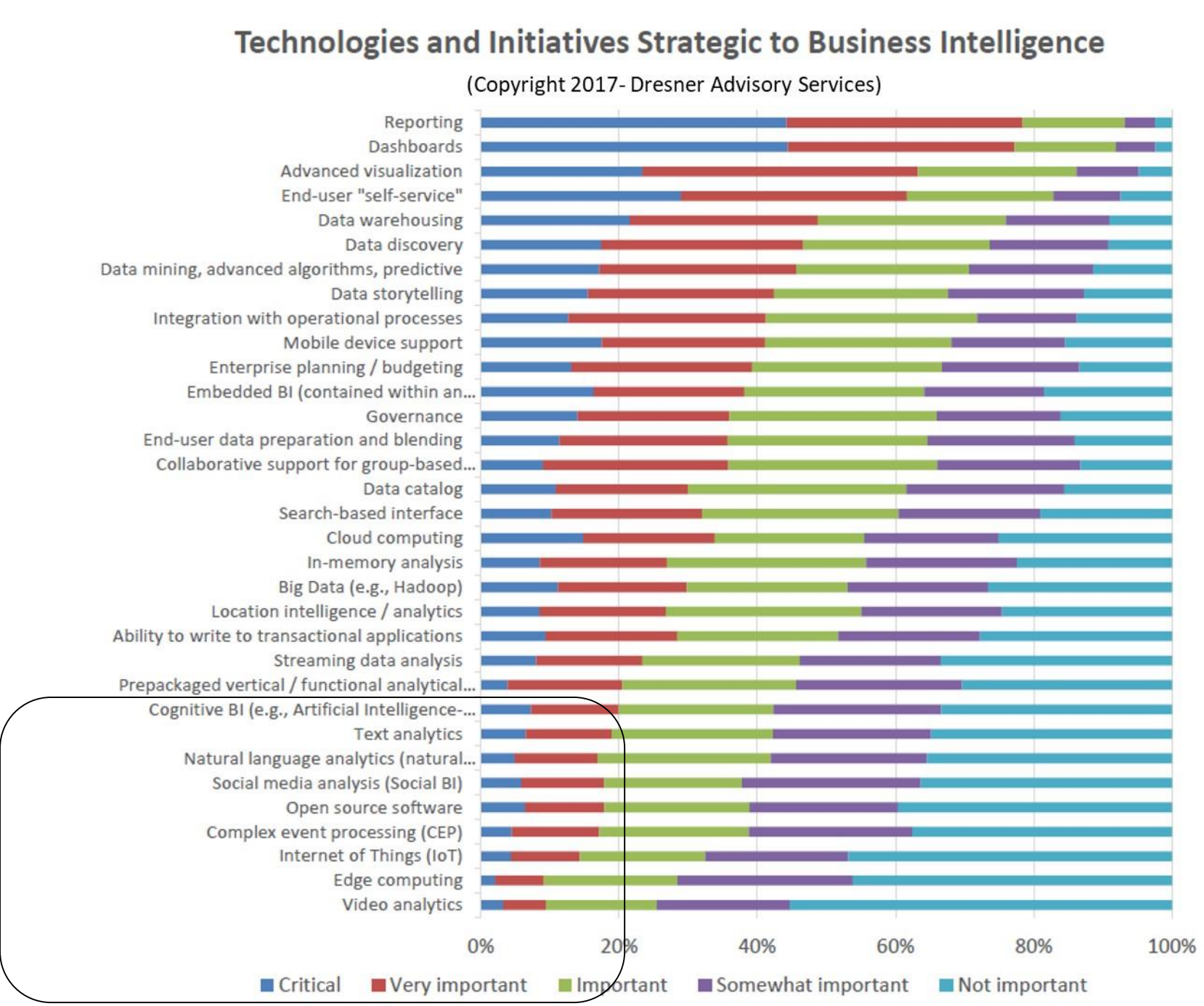
Avancier



Industry 4.0?

- 99% of businesses are not internet giants like Amazon or Google.
- Given transaction numbers in the UK, it looks to me that
  - all credit card transactions
  - all faster payments
  - all Argos web site visitors
- could each be supported by a regular DBMS with SDDs.

- EA is about the whole application portfolio.
- Most apps can be supported by an ordinary DBMS or document store
- Design for extreme scale is the exception rather than the norm.
- And IoT is still considered important by only tiny minority.



See https://blogs.forbes.com/louiscolumbus/files/2017/12/Figure-5-Core-Business-Intelligence-Technoloigies.jpg

FOOTNOTE on GDPR

- http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

1. The first global data protection law?

- The EC is extending data protection regulations to any company that works with information relating to EU citizens
- [Will USA and China resist?]

- One supervisory authority rather than one for each EU state.
- Fines up to €20m or 4% of group annual global turnover.
- EU citizens can approach any data protection authority to lodge complaints
- Any European data protection authority can take action against organisations, anywhere in the world

2. Wider definition of personal data

- data usable to identify an individual as personal data includes, for example
  - Genetic
  - Mental
  - Cultural
  - Economic
  - Social information.

3. Tighter rules for consent to and use of personal information

Avancier

- Organisations need to
- use simple language when asking for consent to collect personal data
- be clear how they will use the information
- prove clear and affirmative consent to process personal data
  - (silence or inactivity no longer constitutes consent)

4. Certain organisations require a DPO

Avancier

- What matter is the number of data subjects not the number of employees

- DPO is needed when
  - “core activities” require
  - “regular and systematic monitoring of data subjects on a large scale” or consist of
  - “processing on a large scale of special categories of data”.

- The DPO must ensure personal data processes, activities and systems conform to the law by design

5. Mandatory privacy impact assessments (PIAs)

Avancier

- All projects involving personal information must work with DPO and conduct PIAs.
- Data controllers must conduct PIAs where privacy breach risks are high

6. Tighter data breach monitoring and reporting

- Organisations must
  - monitor for breaches of personal data.
  - notify the local data protection authority of a data breach within 72 hours of discovering it.
- This implies internal data security policies, promotion and training

7 Privacy by design from the start

- Data minimisation and the right to be forgotten
- Organisations must
  - hold data no longer than absolutely necessary
  - get fresh consent before changing their use of data collected.
  - delete any data at the request of the data subject

- [I’m not clear what deletion means
- Completely erasing data can be very, very difficult
- And proving it is impossible]

<http://involve-beta.e-rm.org/articles/1477/36421/1352470/content.aspx>

Data Removal Experience (IS5)

Avancier

- Our Brief "deinstall equipment, recycle the IT kit, securely destroy data on all media, provide certificates for audit and all regulations ....."

- We looked at the volume, sensitivity and effectiveness of destruction
  - Hard disk drives (servers, laptops, PCs)
  - backup tapes
  - digital cameras,
  - devices with SD cards,
  - mobile phones,
  - PDAs (eg Blackberry)
  - ID cards with magnetic strips or simply with a photo.
  - Photocopiers have large hard drives with images of potentially sensitive documents .
  - Many large printing devices now have hard disks inside.

- Currently non-magnetic devices
  - USB Sticks,
  - SD cards and machines with flash memory
- should be physically destroyed as the technology for erasing them is not currently effective.

Data Removal Standards

- DoD 5220.22-M
- NIST 800-88

8. Liability extended beyond data controllers

- Not only company data controllers
- But all organisations that touch personal data.
- Even service providers

GDPR talks to

- **the 'principle of proportionality'**
- - in other words, if reasonable organisation and technical measures have been applied, then any case against you will take into account measures you have taken to protect the freedoms and rights of data subjects as set out in your privacy impact assessment.

- **the cost of implementation**
- - so, if you can successfully demonstrate that the effort is disproportionate to the risk of varying likelihood and severity for the rights and freedoms of natural persons, then this will also be taken into account.

Read more about the GDPR

Avancier

- The European Parliament's official publication of the General Data Protection Regulation means it will become enforceable on 25 May 2018.

- The GDPR is about enabling organisations to realise the benefits of the digital era, but it is serious about enforcement for those that do not play in the rules, says UK information commissioner.