DRAFT - ICT Project Guidance

Security View

Version:

0.1

Author:

Sky Sigal, Solution Architect

## Purpose

To document the Security Aspects of a system.

## Synopsis

<TODO>

## Contents

[Description 1](#_Toc154927865)

[Synopsis 1](#_Toc154927866)

[Contents 2](#_Toc154927867)

[Purpose 3](#_Toc154927868)

[Background 3](#_Toc154927869)

[Outcomes [Objectives] 3](#_Toc154927870)

[Options [Considered & Selected] 3](#_Toc154927871)

[Constraints 3](#_Toc154927872)

[Assumptions 3](#_Toc154927873)

[Dependencies 3](#_Toc154927874)

[Decisions 3](#_Toc154927875)

[Deliverables/Outputs 3](#_Toc154927876)

[Heading Level 3 3](#_Toc154927877)

[Heading Level 4 4](#_Toc154927878)

[Appendices 5](#_Toc154927879)

[Appendix A - Document Information 5](#_Toc154927880)

[Versions 5](#_Toc154927881)

[Images 5](#_Toc154927882)

[Tables 5](#_Toc154927883)

[References 5](#_Toc154927884)

[Review Distribution 5](#_Toc154927885)

[Audience 5](#_Toc154927886)

[Structure 5](#_Toc154927887)

[Diagrams 6](#_Toc154927888)

[Terms 6](#_Toc154927889)

# Service Security View

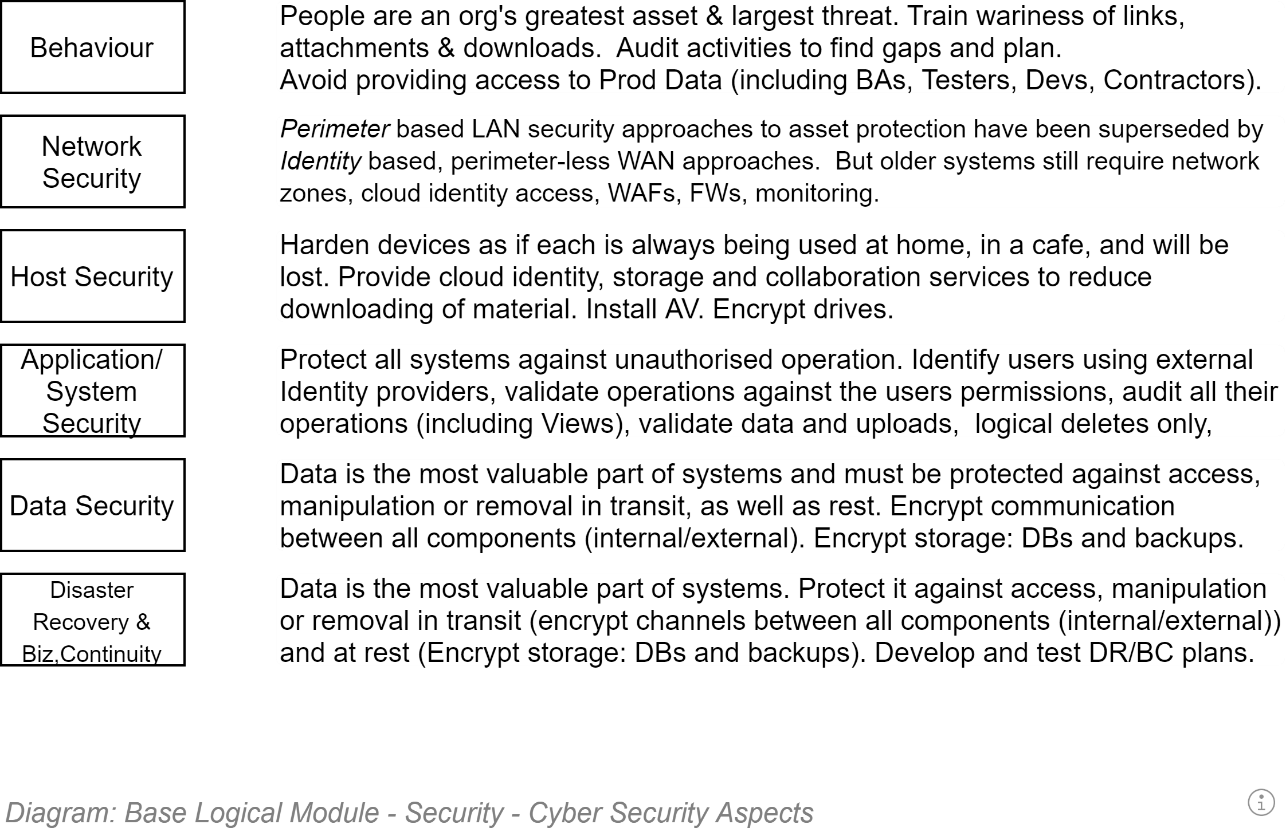
This section describes the security risks and controls used to mitigate risks within the processes and services of the solution.

## Section Synopsis

Security of a system does depend in part on the system’s technical design – but it is only one part of a system’s security.

### Overview

Security starts with people.



## Behaviour

### Non-Access to Production Data

Irrespective of the data classification[[1]](#footnote-2) of the data, production data is entrusted by end users to information systems in the belief that the data is not accessible by others without specific consent.

Based on the above, only the automated delivery pipeline’s security principal is given access to production data – whether it being live production data or backed-up production data (which is still *production* data, just only slightly out of date).

Traditionally Testers, DBAs and other technical Specialists who have had access to production data on other projects, complain vociferously about not knowing how to work when this security restriction is implemented.

Their complaints are addressed by:

* Continuously performing exploratory tests to find new failure points
* Use the found failures to inform the continuous updating of test data, to use in automated tests performed by the deployment pipeline (in order to never have to repeat those tests physically).

## Production Tools

The tools provided to Production personnel to communicate and develop a solution impacts on the behaviour of team members, and therefore the security profile of the solution.

* **Web based team collaboration and wiki services**: Easy onboarding of collaborators (e.g.: using AAD, which allows for inviting Guests) to a system accessible from anywhere at any time improves collaboration (e.g.: using Teams) over secure channels (HTTPS), decreasing the feeling that there is a need to transmit information by another channel outside the provided system (e.g.: using Email, which is -- by default -- an insecure channel).
* **Web based ALM Services**: complete suites offer mature build services that are already integrated to secure credential stores, removing the perceived need to persist integration credentials into source code.

## Physical Environment Security

The physical environment used to host the service must meet ISO-27001 Stage 2+[[2]](#footnote-3).

ISO-27001 ensures the data centre that hosts production data is assessed as having many security controls in place, including the following:

### Confidentiality

N/A

### Integrity

* Physical perimeter hardening (CCTV, alarms, patrolling, etc.)
* Security trained personnel
* No access to hosted devices unless requested, approved, logged and accompanied by a second person observing their actions remain within the scope of the approved task.

### Availability

* Automated Backups, Fallback & Recovery capabilities
* Power, traffic and access monitoring and alerting
* Optionally, remote self-service administration capabilities

## Network Security

If the device is within a LAN, the LAN’s perimeter is hardened, uses a firewall to close unnecessary ports, uses traffic monitoring and alerting.

Even if within a LAN, Communication between Devices must be secured, as if the system were not protected by a LAN’s perimeter defences. Specifically, communication between all components and services should be secure. Refer to *Security in Transit*, and *Security at Rest*, in the next section.

### Azure Cloud Service Network Environment Characteristics

TODO: Copy from BASE

### Amazon Cloud Service Environment Network Environment Characteristics

TODO:

## Host Security

TODO: Clarify

### Azure PaaS Characteristics

TODO: Copy from BASE

### Azure Container Characteristics

TODO:

## System Information Security

Several data specific controls are used to secure the system’s information.

### Confidentiality

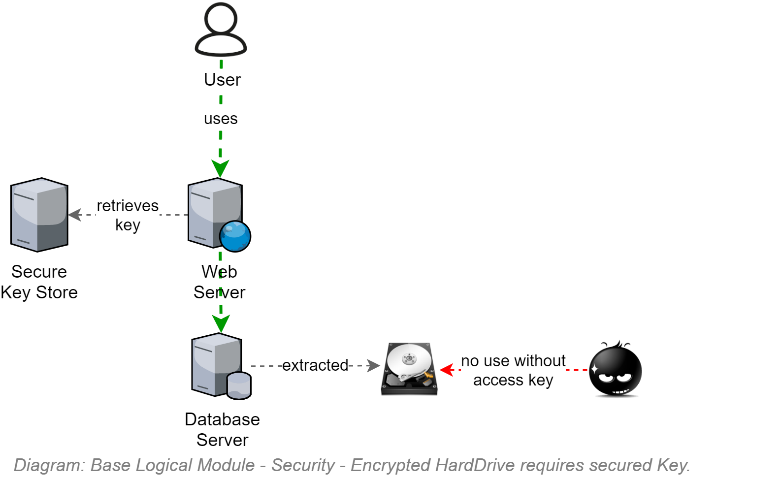
#### Security at Rest

Protection of the data at rest is accomplished at several levels, as shown below.

##### Encrypted Hard drives

The hard drives used to persist the production data on must be solid state (for performance) and encrypted.

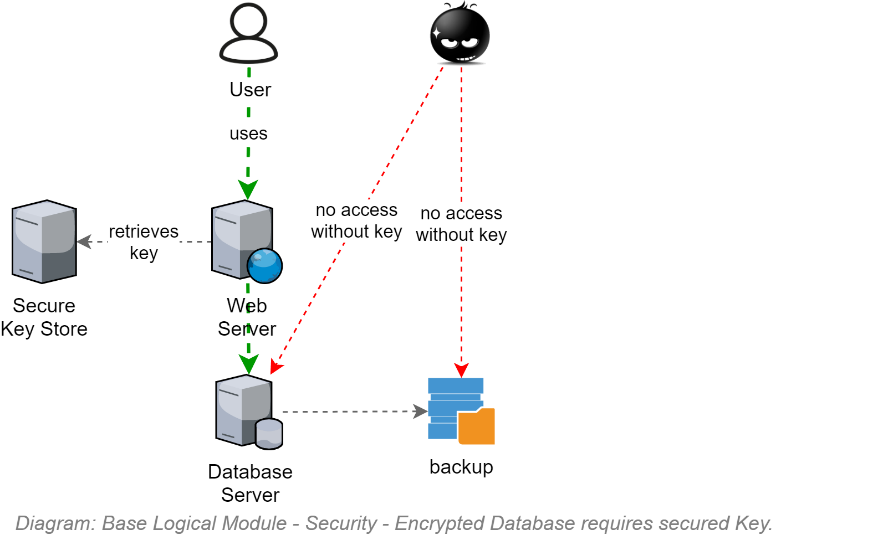
By using encrypted hard drives, if the disk drive is replaced, or disposed of without being wiped first, the database on the drive remains inaccessible.



##### Encrypted Databases

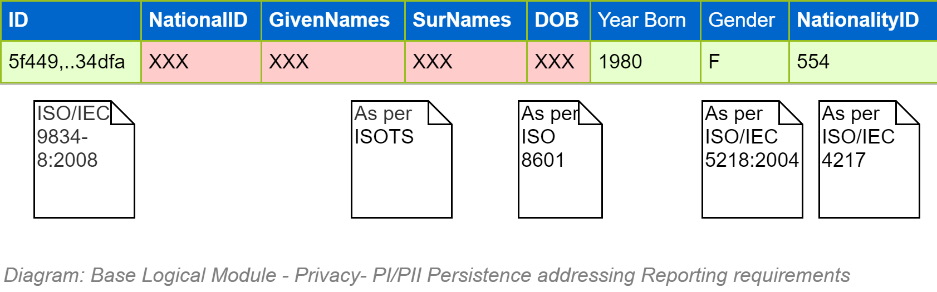
The databases created on the hard drives are created using a cloud service provided key.

By encrypting the database, if it downloaded via Remote Desktop Protocol (RDP) or similar, the database remains inaccessible even when removed from a secure backup environment.



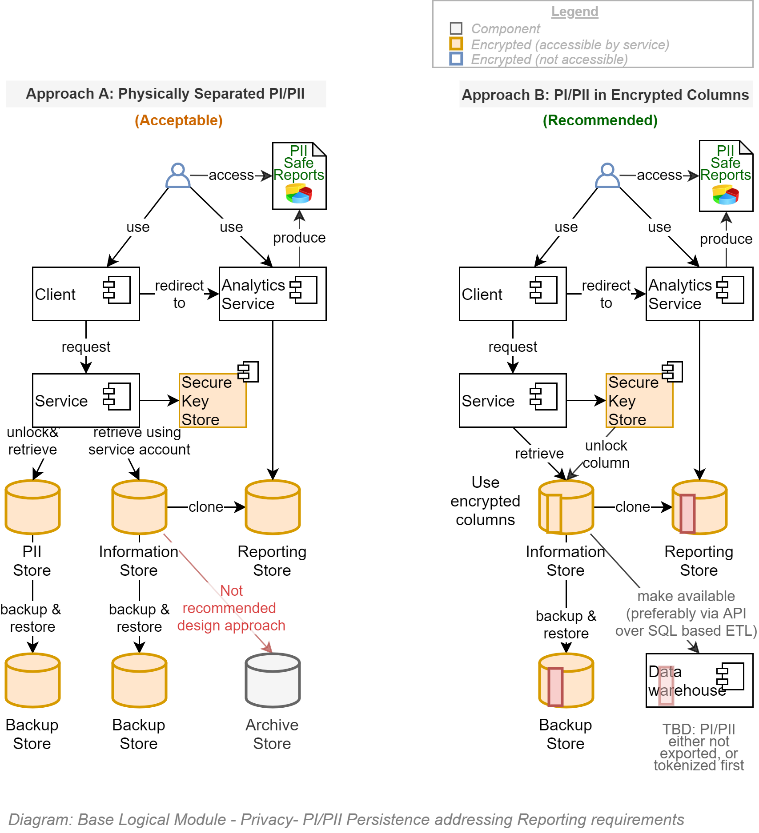
##### Encrypted Database Columns

The columns of the tables containing the Personally Identifiable Information of Users are encrypted using a key, persisted in the environments key vault in such a way that the cloud provider’s database service can access it.



By encrypting the columns containing PII information the database can be cloned for analysis and reporting by others with less of a chance of disclosing sensitive data via the analysis and reporting tools.

Information  
**Note:**  
Not all database engines can deliver encrypted database columns. This is one of the reasons why we stipulate the use of certain database engine types (e.g.: SQL Server) as opposed to accepting other recommendations.



##### Limited Database Access

The only service accounts that are given direct access to the database are:

* **The deployment pipeline’s service account**, used to create the database, update its schema, seed its reference data, and develop and restore backups.
* **The information system’s host’s service account**: the service’s ORM component uses this account to the same as above, as well as read/write additional data.

Limiting the accounts that can access the system’s data to only two system service accounts is another way of ensuring Users (Testers, DBAs, Specialists) do not have unaudited access, nor know credentials that they may inadvertently commit to the code repository or transmit over a system.

#### Security in Transit

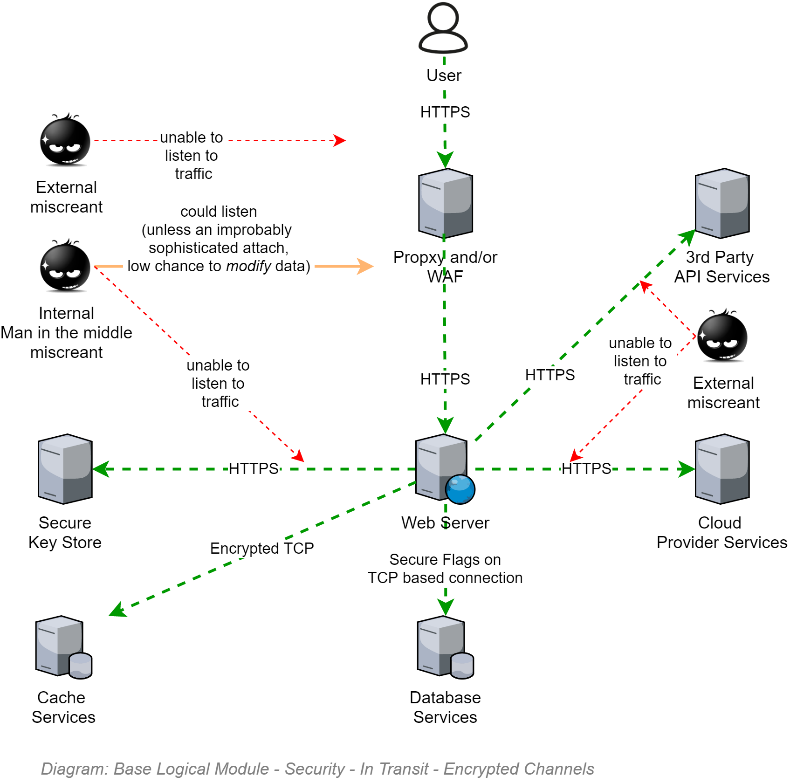
Security in Transit is met primarily by using appropriate encryption of channels between devices.

##### Encrypted Channels

Communication between Components and Services must be secured by encryption where-ever technically and reasonably achievable.

For example, HTTPS, using the latest TLS specification, is always used over HTTP channels. Connections to relational databases use security flags where they can be implemented[[3]](#footnote-4).

ed in this solution.



###### Redirection

If a user specifically requests communication over an insecure channel – ie, they type <http://myapp.tld>, instead of <https://myapp.tld>, the web server issues an HTTP 302 Code, redirecting them to the same URL, but this time over https (i.e.: <https://myapp.tld>).

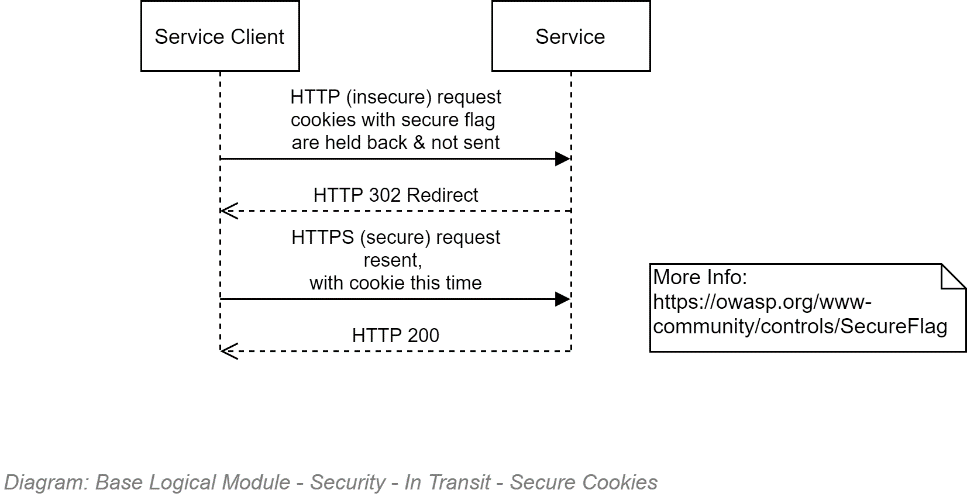
Note: Redirection is not an application setting: it is a server setting that is put in place via Infrastructure as Code (IaC) instructions issued by the continuous deployment pipeline, prior to the software package being deployed to the web server.

###### Secure Cookies

An important aspect of secure communication is ensuring that secure objects are not transmitted over unsecure channels.

If a user specifically requests communication over an insecure channel (see above), the service client (i.e., browser) MUST NOT send its SessionId cookie over the cleartext channel.

The way to stop that is ensure that cookies developed to roundtrip the session id between service and service client and back again, is decorated with the secure=true flag. This tells the browser that the cookie can only be transmitted if the channel is deemed secure (i.e. encrypted).

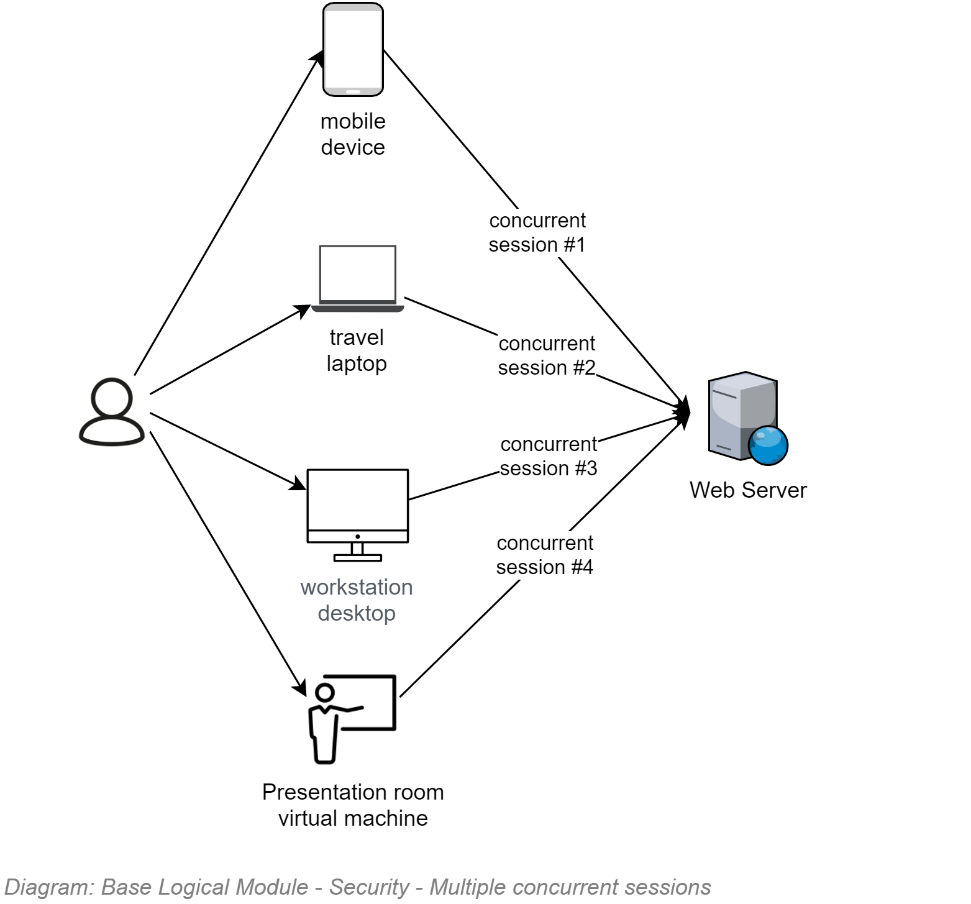


##### Encrypted Messages

Not required.

### Integrity

#### Sessions



Bullseye  
**Requirement:**  
Sessions must be permitted to be as long as possible, while being short enough that their security tokens cannot reasonably be decrypted by brute force before they expire.  
The rationale is that in order to make the service user-friendly, the service must not force them to re-enter their credentials more times than required.

#### Session Operation Auditing

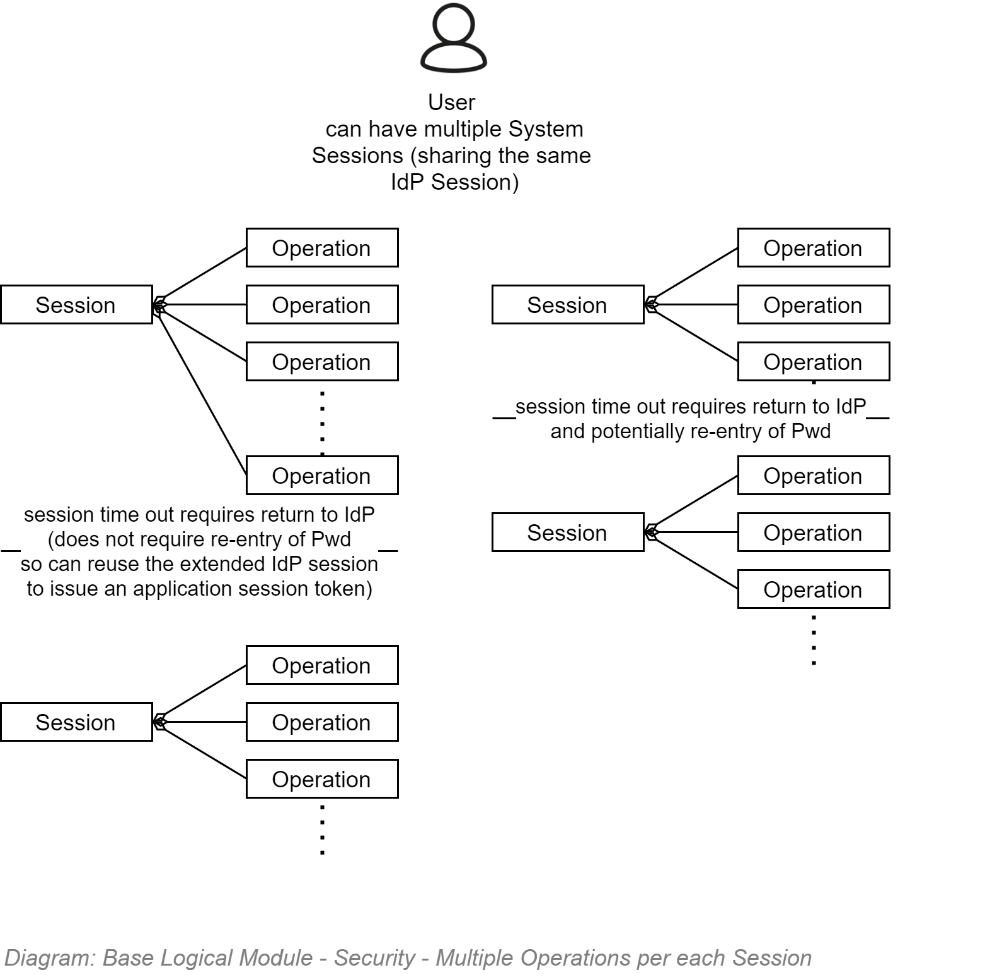
All Operations – including List & View Operations that do not actually change system data – undertaken by users -- irrespective of whether the user is Unauthenticated or Authenticated (both user categories get a Session) -- are permanently and immutably logged.

The SessionOperation record created for each HTTP request captures the UTC Date and Time, users current IP (IPs issued to all devices – especially mobile ones can change over the duration of a Session), the geo location of the WAN IP address if known, etc. and associates it to the Session record.

If an Unidentified user signs in, all operations attributed to that Session before and after the sign in event are attributable to the identified User associated to the Session record.

Note:  
Auditing of operations like List & View, which do not modify data, is still required to better understand the impact of poor security controls (i.e., who has seen a specific record or resource).

If a System Session token times out it will redirect the user back towards the remote IdP, which will challenge the User for their credentials if the IdP Session (an IdP Session is different than a System Session…) has timed out, or reuse a still-open IdP Session to issue a new System Session token.



### Availability

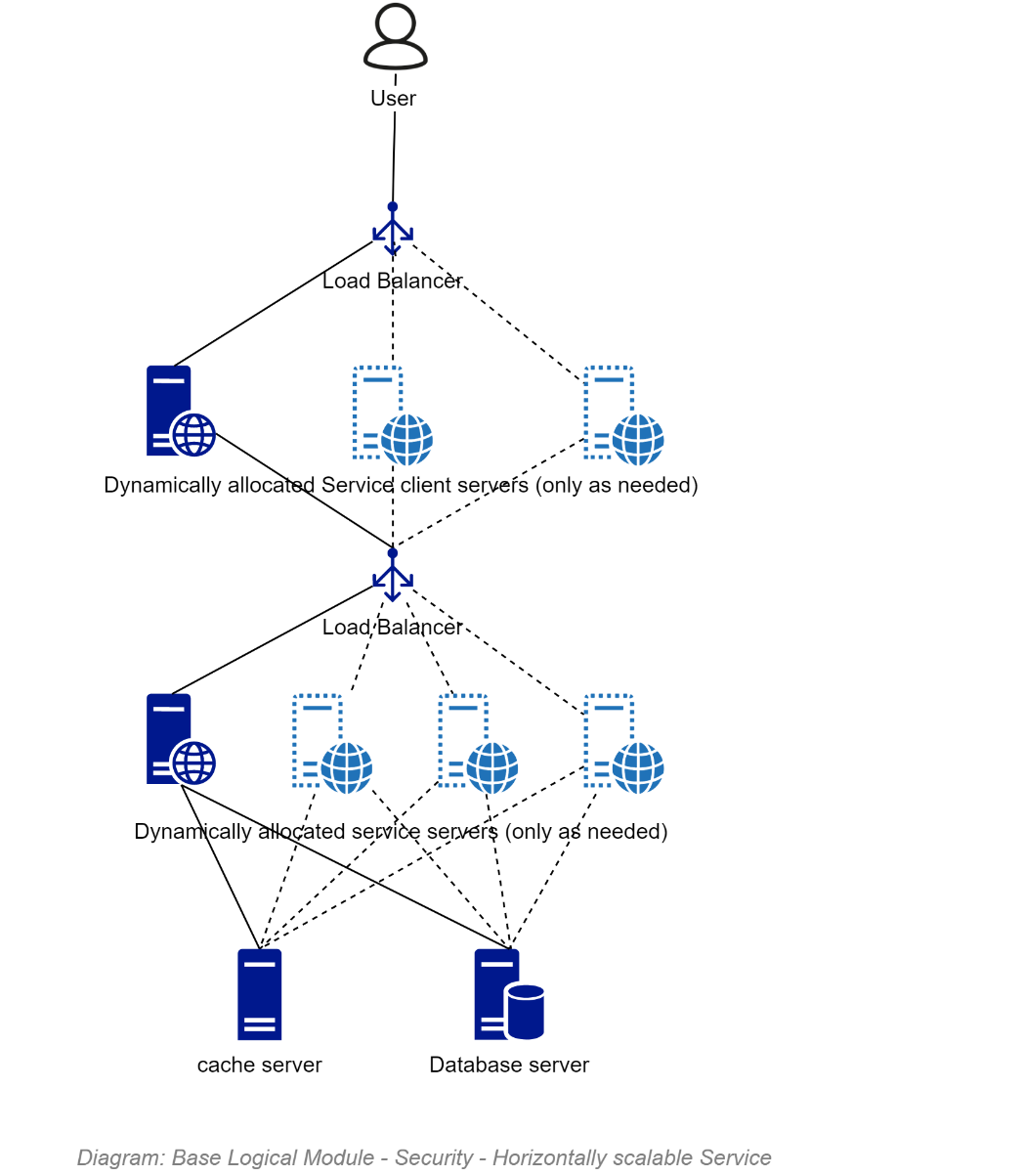
#### DDOS

TODO: BASE

#### High Availability

The infrastructure as code (IaC) instructions executed by the continuous delivery service ensure that the cloud infrastructure is instructed to horizontally scale up to handle peak surge demands.

The trigger used to decide when to instantiate another host is when the CPU has been above a Quality Requirements specified amount for a Qualities Requirement specified duration (eg: 50% for 3 minutes).



**Note:**  
The icons used above show virtual servers – but it’s only for lack of a more suitable image to use for a non-proprietary Container/PaaS based architecture. This point is made to ensure there is no confusion over our position that the use of VMs – and IaaS – are a legacy approach which have little to no remaining value in current system design.

#### Redundancy

If the cloud service goes offline, we are reliant on our contracted SLAs for the service to rebecome available.

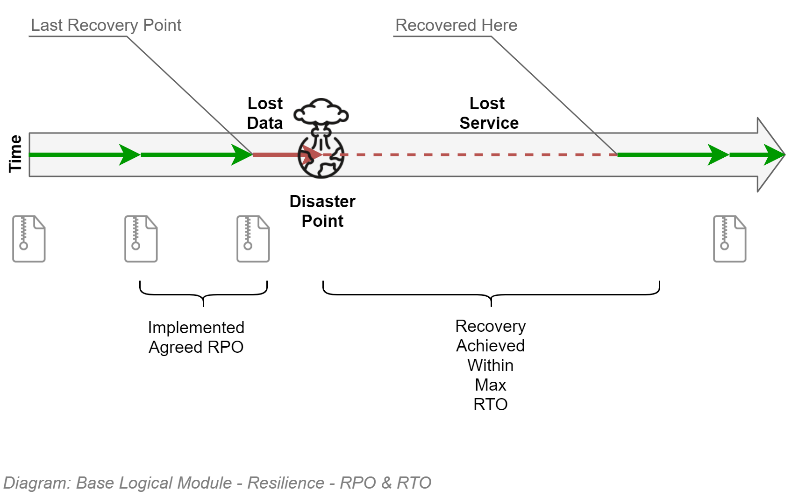
#### GeoReplication

We are not committing to geo-replication at this point based on the cost versus vanishingly small risk.

#### Disaster Recovery

##### Automated Backup and Restoration

The Infrastructure as Code instructions which the Continuous Deployment Pipeline execute include instructions to configure full and incremental backups to meet RPO and RPT obligations as specified in the Quality Requirements.



##### Recovery Point Objective (RPO)

Disaster recovery is implemented by using the cloud provider’s database backup service taking full backups every day, and incremental backups at intervals satisfying the RPO objectives specified in the quality requirements (between 1 and 15 minutes apart).

##### Recovery Time Objective (RTO)

The automation available by the cloud provider allows the initiation of a full redeployment of the environment and full restoration of the backups within an interval satisfying the RTO value specified in the Quality Requirements (less than an hour after the automated task is initialised).

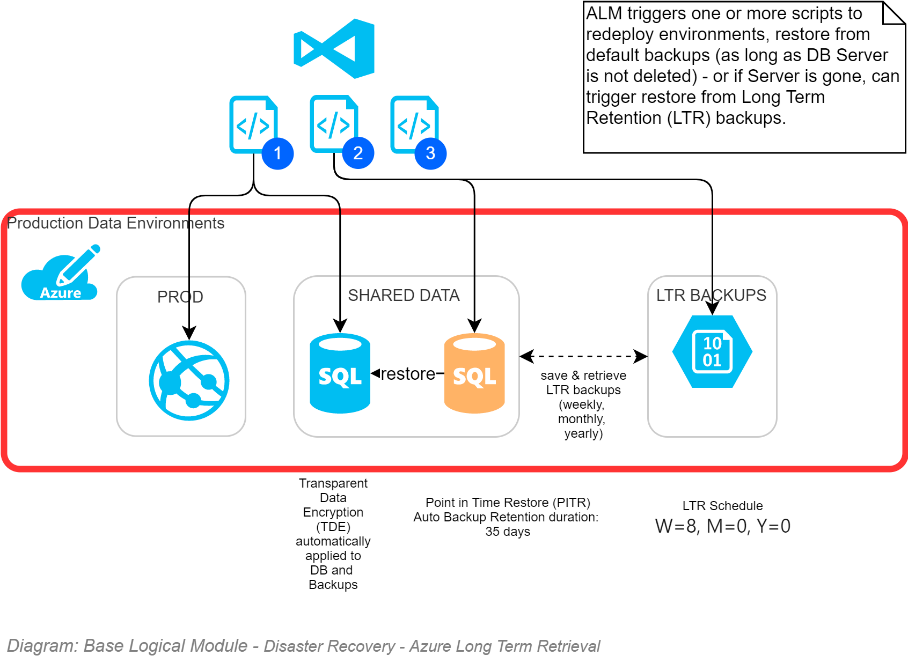
#### Business Continuity

The Infrastructure as Code instructions which the Continuous Deployment Pipeline execute include instructions to setup long term storage of the database in the event everything else is deleted.

Whereas GeoReplication is not required to run the service, it is wise to persist the Long-Term Storage in a geographically different location – within a country with an acceptable legal system.

The exact implementation depends on the Cloud platform.

###### Azure



###### Amazon

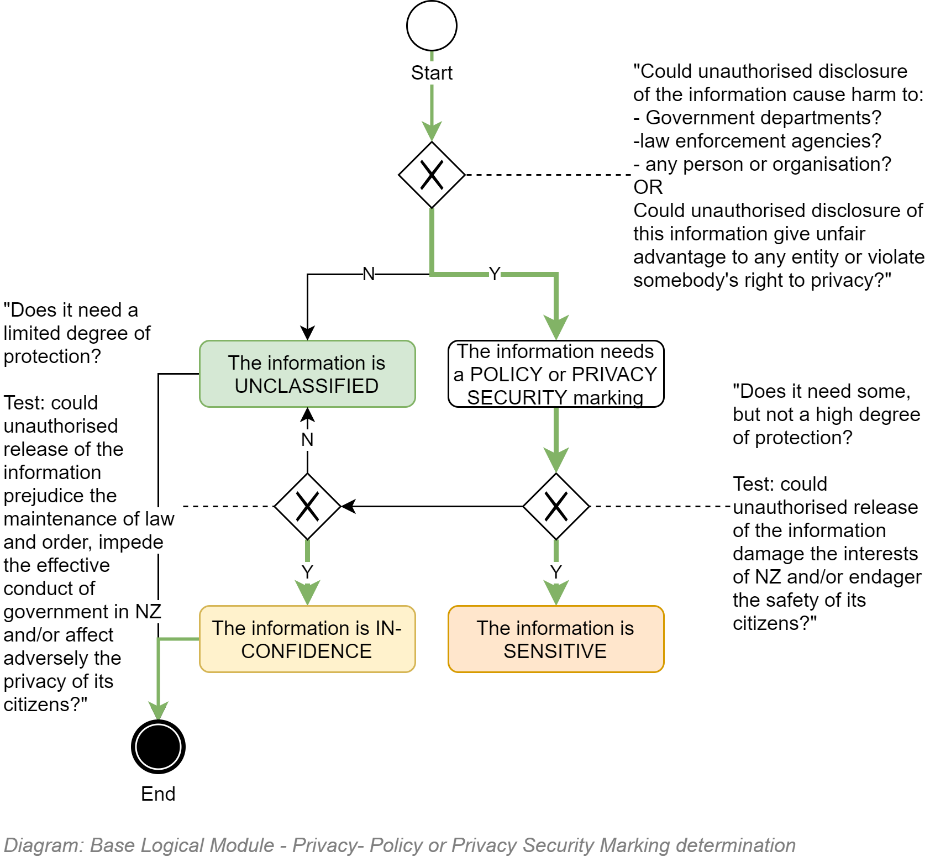
TODO

### Data Classification

The data’s classification is determined according to the following workflow.

 **Warning:**  
even if an information system manages UNCLASSIFIED data, the system manages some form of private identifying information (PII) of users, the disclosure of which would harm a person or organisation, making even if an information system manages UNCLASSIFIED data, the system manages some form of private identifying information (PII) of users, the disclosure of which would harm a person or organisation, making even if an information system manages UNCLASSIFIED data, the system manages some form of private identifying information (PII) of users, the disclosure of which would harm a person or organisation, making some of the data managed by the system IN-CONFIDENCE.

 **Note:**  
even if some of the information managed by a system is IN-CONFIDENCE, the system MUST meet its other Open & Transparent Data obligations to NZ and the UN. even if some of the information managed by a system is IN-CONFIDENCE, the system MUST meet its other Open & Transparent Data obligations to NZ and the UN. Therefore, a system must and can expose most of its data – excluding its IN-CONFIDENCE data.even if some of the information managed by a system is IN-CONFIDENCE, the system MUST meet its other Open & Transparent Data obligations to NZ and the UN. even if some of the information managed by a system is IN-CONFIDENCE, the system MUST meet its other Open & Transparent Data obligations to NZ and the UN. Therefore, a system must and can expose most of its data – excluding its IN-CONFIDENCE data.



## Roles to Permissions Schedule

TODO: Include Image

Availability

Disaster Recovery

Appendices

Appendix A - Document Information

### Versions

* 1. Initial Draft

### Images

[Figure 1: TODO Image 2](#_Toc144995112)

### Tables

[Table 1: TODO Table 3](#_Toc145048484)

[Table 2: TODO Table 2 3](#_Toc145048485)

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
|  |  |
|  |  |
|  |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Standards

ISO-25010

: …

ISO-25012

: …

ISO-25022

: …

### Acronyms

Refer to the project’s Glossary.

IT

: acronym for Information, using Technology to automate and facilitate its management.

##### ICT

: acronym for Information & Communication Technology, the domain of defining Information elements and using technology to automate their communication between entities. IT is a subset of ICT.

### Terms

1. Even Social Media (e.g.: Facebook) data is UNCLASSIFIED – but users expect their private photos are shared only with specific users -- *not* testers, not DBAs, not operations specialists, not developers. [↑](#footnote-ref-2)
2. ISO-27001 Level 1 – i.e. self-assessment -- is not enough [↑](#footnote-ref-3)
3. Avoid relying on communication channels that rely on certs, in order to not rely on long-life certs that end up being a security risk in themselves. [↑](#footnote-ref-4)