Architecture Principles

Designs Goals & Constraints

AWG Workshop 1

Session 4

5th December 2019

ELEXON

Health & Safety

In case of an emergency

An alarm will sound to alert you. The alarm is tested for fifteen seconds every Wednesday at 9.20am

Evacuating 350 Euston Road

- If you discover a fire, operate one of the fire alarms next to the four emergency exits.
- Please do not tackle a fire yourself.
- If you hear the alarm, please leave the building immediately.
- Evacuate by the nearest signposted fire exit and walk to the assembly point.
- Please remain with a member of ELEXON staff and await further instructions from a Fire Warden.
- For visitors unable to use stairs, a Fire Warden will guide you to a refuge point and let the fire brigade know where you are.

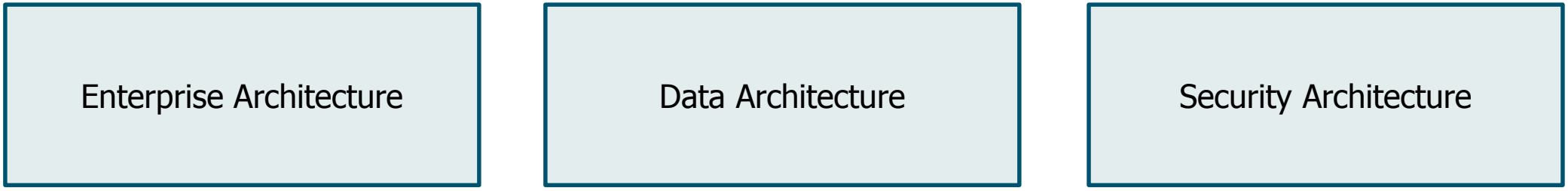
When evacuating please remember

- Do not use the lifts.
- Do not re-enter the building until the all clear has been given by the Fire Warden or ground floor security.

Our team on reception is here to help you, if you have any questions, please do ask them.

ELEXON

Architecture Principles, Design Goals & Constraints



Business Continuity

Adopt Best Practices

Component Reusability

Adaptable & Flexible

Technology Interoperability

Data Governance

Data Management

Information Security

NCSC Guidelines

SPaR Impact Guidance

Enterprise Architecture:

Business Continuity	There must be no interruption to business activities. The business must continue their core operations regardless of unexpected, internal or external technical issues.
Adopt Best Practices	Projects must deliver progressively better services, to a higher quality and within effective cost controls.
Component Reusability	The architecture is constructed with functionally modular components that implement reusable or extensible business services.
Adaptable & Flexible	This will reduce complexity and promote integration to achieve improved efficiency of technology and business services. Avoid expensive projects and overruns whilst increasing system durability and life-span.
Technology Interoperability	Infrastructure and software should follow established standards or patterns that promote data, application and technology component interoperability.

Data Architecture:

Data Governance

Accountability – roles for data and transparency of data ownership.

- Data Stewards
- Data Architects

Consistency – standards (organise) and policies (rules) for data.

- Standards
    - ETL / Storage / Analytics / Technology types
- Policies
    - Data Quality / Data Retention / Legal Accountability

Adaptability – enable governance to be modified for changing conditions.

Data Management

How to capture, store, retain and manage data so it can be used appropriately.

- Data Storage Types / Data Acquisition patterns / Tools and Processes
- Data Access Methods / User Roles and Security

How can data quality be validated and how can business be confident it is accurate.

Security Architecture:

Information Security (CIA)

Information must be protected against unauthorised usage or modification.

- Confidentiality – data cannot be accessed by those whom are not authorised.
- Integrity – data cannot be inadvertently or maliciously modified or corrupted.
- Availability – authorisation and access to data is appropriate.

NCSC Guidelines

National Cyber Security Centre (UK) has the:

- Cyber Assessment Framework 3.0
- NCSC Cloud Security Guidance

SPaR Impact Guidance

As recommended by Ofgem, the Security, Privacy and Risk Impact Guidance is used to gauge the level of impact against different types of harm caused by risks.

Example risk impact concerning a loss of security and privacy to data for:

Government Reputation

- Level 1 = minimal negative impact
- Level 4 = prolonged parliamentary scrutiny
- Level 6 = widespread condemnation

NCSC Cyber Assessment Framework 3.0:

Objective	Category
A.1 Governance	Process & People
A.2 Risk Management	Process
A.3 Asset Management	Technology & Process
A.4 Supply Chain	Process & People
B.1 Service Protection Policies & Processes	Technology
B.2 Identity & Access Control	Technology
B.3 Data Security	Technology
B.4 System Security	Technology
B.5 Resilient Networks & Systems	Technology
B.6 Staff Awareness & Training	People
C.1 Security Monitoring	Technology
C.2 Proactive Security Event Discovery	Technology
D.1 Response & Recovery Planning	Technology, Process, People
D.2 Lessons Learned	Process & People

NCSC Cloud Security Principles:

1. Data in Transit Protection
2. Asset Protection & Resilience
3. Separation between Users
4. Governance Framework
5. Operational Security
6. Personnel Security
7. Secure Development
8. Supply Chain Security
9. Secure User Management
10. Identity & Authentication
11. External Interface Protection
12. Secure Service Administration
13. Audit Information for Users
14. Secure Use of Service