

# **Functional Principles**

## **Enterprise Architecture: Governing Principles**

## Contents

|   |   |
|---|---|
| Common Functionality .....  | 3 |
| Modular Solutions .....   | 4 |
| Scalability and Performance .....                                     | 4 |
| Legal and Regulatory Requirements.....                                | 5 |
| Confidentiality, Integrity and Availability of Data and Systems ..... | 6 |
| Security Policy.....  | 7 |
| Information Quality .....   | 8 |
| Business Continuity.....  | 8 |

### Common Functionality

|                     |  |
|---------------------|--|
| <b>Principle</b>    | System design must re-use existing functionality to support products and services.   |
| <b>Rationale</b>    | <p>Most business units share a considerable amount of common functionality. This must be understood and leveraged in future-state architectural design.</p> <p>This functionality is often duplicated in different enterprise solutions, increasing costs and time-to-market, creating inconsistent customer experience and reducing quality and effectiveness.</p>  |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. The business must standardise business process</li> <li>2. Business processes must be documented and published across the BC organisation</li> <li>3. Existing solutions, available functional components and business services must be catalogued in such a fashion that makes it easier to determine their reusability, initially focussing on services which are likely to be reused frequently</li> <li>4. A case may be made to build up the catalogue of reusable components and services to justify an internal build or Service Based Architecture implementation.</li> <li>5. Governance processes, supported by appropriate tools must be put in place to ensure that common services and components are created, used and re-used.</li> </ol> |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Not all processes are owned and under the control of BC, e.g. other stakeholders or partners</li> <li>2. Currently Silo'd organisation makes it difficult to identify how much common ground there is for business processes</li> <li>3. FABs has already failed to get senior management commitment to significant business process change, the current appetite is for delivery</li> <li>4. There is a risk of change fatigue, it becomes too hard</li> </ol>  |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Document and publish business processes</li> <li>2. Address the silo mentality</li> <li>3. Identify existing services and components (focus on components which are most likely to be re-used)</li> <li>4. Create and publish service catalogue</li> <li>5. Specify existing catalogue capabilities in FABS/SAP and OTP</li> <li>6. Establish and activate service governance processes and tools</li> </ol>   |

### Modular Solutions

|                     |   |
|---------------------|---|
| <b>Title</b>        | F2 – Modular Solutions  |
| <b>Principle</b>    | System designs are organised into re-usable functional components, separating business functionality from presentation.   |
| <b>Rationale</b>    | <p>There is a fundamental business requirement for agile, re-usable solutions.</p> <p>Separating presentation from business functionality will enable BC to modify or create channels, with minimum impact on existing services and functionality.</p>          |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. Solution designs should be modularised</li> <li>2. Solutions must separate business functionality from presentation</li> <li>3. Solution components must communicate via standard interfaces</li> </ol>               |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Capacity (resources) to do this may be limited</li> </ol>   |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Define and publish BC interface standards</li> <li>2. Review existing projects to ensure they are compliant</li> <li>3. Ensure architecture governance processes are in place to ensure ongoing compliance</li> </ol> |

### Scalability and Performance

|                     |  |
|---------------------|--|
| <b>Principle</b>    | Any system implementation, or modification, must be able to scale based on current understanding of business strategy and project requirements.  |
| <b>Rationale</b>    | Any breakpoints in a systems capability to handle transaction volumes, bandwidth, data capacity or messaging capacity should be identified and options for exceeding those breakpoints identified to ensure customer service levels are maintained.  |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. A formal capacity planning process need to be embedded within the development lifecycle of all applications and services</li> <li>2. We need to use technical solution to provide flexibility</li> <li>3. We should implement and manage IT solutions as services</li> </ol> |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Existing systems may not be able to scale appropriately</li> </ol>   |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. We need to implement ITIL capacity management process</li> <li>2. Ensure all solutions are reviewed to ensure they meet scalability and performance requirements</li> </ol>  |

## Legal and Regulatory Requirements

|                     |  |
|---------------------|--|
| <b>Principle</b>    | Solutions must conform to legal, regulatory requirements.  |
| <b>Rationale</b>    | Non-conformance of the above may result in legal action being taken against the British Council which will both damage the reputation of the organization and potentially result in compensation payments to regulatory bodies or disaffected personnel.   |
| <b>Implications</b> | <ol style="list-style-type: none"><li>1. The architecture group need to be aware and regularly updated about new regulations which may impact the design of IT systems</li><li>2. The relevant requirements must be analysed to determine what impact they have on architecture standards</li><li>3. Standards need to be defined and published</li><li>4. Enterprise Architecture governance needs to be put in place</li></ol> |
| <b>Obstacles</b>    | <ol style="list-style-type: none"><li>1. The global nature of the organisation may result in conflicts for compliance</li></ol>  |
| <b>Actions</b>      | <ol style="list-style-type: none"><li>1. Should become part of scope of the security domain group</li><li>2. Define and publish standards</li><li>3. Ensure that all solutions are reviewed to ensure compliance with standards</li></ol>  |

## Confidentiality, Integrity and Availability of Data and Systems

|                     |  |
|---------------------|--|
| <b>Principle</b>    | <p>All systems (including business and IT systems) must cooperate to protect the confidentiality, integrity and availability of data while being handled by the British Council systems, to a level commensurate with the assessed and accepted risks.</p>   |
| <b>Rationale</b>    | <p>Confidentiality, integrity and availability of systems and information are the foundations of information security.</p>   |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. Solutions must maintain the confidentiality of information at rest and in transit, at a level commensurate with the recognised risks. Examples include, but are not limited to:             <ol style="list-style-type: none"> <li>a. the use of one-way encryption for storing user passwords and credit card information</li> <li>b. encrypting interactive network-based administrative access to systems</li> </ol> </li> <li>2. Solutions must maintain the integrity of information at rest and in transit, at a level commensurate with the recognised risks - this includes, but is not limited to, methods of data validation being incorporated into any solution that is capable of creating, modifying or deleting data</li> <li>3. Solutions must maximise the availability of information and systems, at a level commensurate with the recognised risks - this includes, but is not limited to, the elimination of single points of failure for key business systems, such as billing systems and customer web portals</li> <li>4. All solutions must be risk assessed</li> </ol> |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Existing systems and/or components might present security risks</li> <li>2. Existing systems and/or components might not have been risk assessed</li> <li>3. Unrealistic business expectations</li> </ol>  |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Ensure that all systems (business and IT), components and information have been risk assessed</li> <li>2. Ensure that the governance process includes regular reviews of risk assessments</li> <li>3. Review architecture and designs to ensure that there is no single point of failure for key business systems. Include business and components within this assessment</li> <li>4. Ensure that weak physical security does not undermine technological measures</li> <li>5. Raise awareness that this extends to externally sourced contracts and systems and ensure that 'off-the-shelf' clauses are readily accessible for inclusion in contracts and service specification documents.</li> </ol>   |

### Security Policy

|                     |  |
|---------------------|--|
| <b>Principle</b>    | Security policies covering all explicit and implicit business activities must exist.   |
| <b>Rationale</b>    | <p>Security policies, aligned to the higher-level security strategy, must exist to ensure that the British Council can comply with all business and regulatory requirements.</p> <p>Examples of common policies include, but are not limited to:</p> <ul style="list-style-type: none"> <li>o the monitoring of email and web traffic to detect inappropriate content</li> <li>o recording of administrative users' actions</li> <li>o restricting physical and/or logical access to removable media at the desktop</li> </ul> |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. Security policies must be available and publicised</li> <li>2. The architecture must comply with security policies at the functional, technical and implementation levels</li> <li>3. Governance processes must be in place to ensure that security policies are maintained and complied with</li> </ol>   |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Existing systems or services may be non-compliant</li> <li>2. It may be difficult to find out which systems are non-compliant</li> </ol>   |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Ensure that existing security policies are current</li> <li>2. Ensure that existing security policies are being applied</li> <li>3. Ensure that the governance policy allows for the time limited and risk assessed dispensation of non-compliance to security policies.</li> <li>4. Ensure that awareness is raised that security policies apply to all systems and services we commission whether internal or external</li> </ol>  |

### Information Quality

|                     |  |
|---------------------|--|
| <b>Principle</b>    | Information must be maintained to an appropriate level of quality.   |
| <b>Rationale</b>    | Information is an asset. Inaccurate information is worse than no information at all as it is misleading.   |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. Information quality standards need to be defined and published</li> <li>2. Need to define and publish exactly what constitutes personal data</li> </ol>  |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Lack of clarity as to what exactly constitutes personal data</li> <li>2. There may be a reluctance to share data (and hence standards) across the organisation</li> </ol>  |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Should become part of scope of the data domain group</li> <li>2. Define and publish standards</li> <li>3. Classify personal data</li> <li>4. Ensure that all solutions are reviewed to ensure compliance with standards</li> </ol> |

### Business Continuity

|                     |  |
|---------------------|--|
| <b>Principle</b>    | Business systems must continue to operate at an appropriate level of service in the event of disaster or other unforeseen situation.   |
| <b>Rationale</b>    | If we cannot provide an effective level of service to our customers, we will lose their custom.  |
| <b>Implications</b> | <ol style="list-style-type: none"> <li>1. Business continuity requirements need to be defined and agreed with the business and then published</li> <li>2. Business architecture must support business continuity requirements</li> <li>3. IT architecture must support business continuity requirements</li> </ol> |
| <b>Obstacles</b>    | <ol style="list-style-type: none"> <li>1. Cost may outweigh the business benefits</li> <li>2. Unrealistic business expectations</li> </ol>   |
| <b>Actions</b>      | <ol style="list-style-type: none"> <li>1. Establish business case for continuity</li> <li>2. Define and publish business continuity requirements</li> <li>3. Review business architecture to ensure that is compliant</li> <li>4. Review IT architecture to ensure it supports business requirements</li> </ol>    |