Maritime &
Coastguard
Agency

Safer lives,
safer ships,
cleaner seas

Base Design Principles

Version 2.1

BUSINESS

1 **Business Capability** – Capability design must be customer centric.

2 **Service Design** - Design will prioritise customer information, useability, quality and availability.

3 **Customer Operation** - Systems must empower staff to serve customers.

4 **Consistent Experience** - The experience offline and online should be consistent.

5 **E2E Processes** - Processes should be connected end to end.

6 **Omnichannel -** Organisational structures will be aligned to omnichannel aspirations.

7 **Open Data Alignment** - Relevant information will be made available to a wide an audience as possible.

8 **Simplify Operations -** Decisions will seek to simplify the agency operations environment.

9 **Alignment -** All business change must be aligned with MCA goals and strategy.

10 **Requirements -** Business areas will provide robust functional and non-functional requirements.

IT SOURCING

1. **Manage Relationship** - IT will, where possible, manage and build on strategic vendor relationships.
2. **Ownership** - IT will retain accountability for strategy, architecture, and business relationships.
3. **Service Lifecycle** - Where possible the agency will bundle work across the lifecycle of the service until it becomes stable.
4. **Evaluation** - IT will choose qualified partners who align with the MCA values.
5. **Staff Impact -** IT will proactively manage staff impacts from sourcing initiatives.
6. **Contract Management** - All technical suppliers will have an appropriate contract management plan and associated KPI,CSF and SLA's including social value benefits.
7. **Cost Effective –** IT will leverage the UK governments buying power whenever possible.
8. **Outcome Based –** Every investment must show alignment with business goals, strategies and architecture.
9. **Scope –** Each contract Will have a defined scope and associated timeline.
10. **Time for Sourcing** – Appropriate time and effort will be allocated for the sourcing and contracting.

APPLICATIONS

1 **Application Investment - **Applications should be procured as a product or service, rather than developed (when developed this should be carried out using open source and reusable code).

2 **Customisation -** Third-party applications will be configured, not customised, to meet agency needs.

3 **Business Agility -** Solutions will be architected as a strong foundation for the future minimising costs for future changes.

4 **Extensibility –** Applications will provide hooks and integration that allow functionality to extended in the future.

5 **Modularity –** Applications must be easily altered, reconfigured, integrated and assembled to respond to changing business requirements.

6 **Reuse –** Where possible applications will reuse existing components.

7 **Integration –** Business logic should not be included within the integration layer.

8 **Modernisation–** Applications should have an agreed lifecycle (end of life and technical debt should be anticipated and planned for).

9 **Documentation -** Applications must have appropriate architecture, design and runbook documentation.

10 **Aligning Processes -** Unless relating to a strong strategic differentiator, business processes will be adapted to the technology choices.

DATA

1 **Data Stewardship -** Data assets will be subject to business ownership.

2 **Data Interpretation -** All data assets, should be accompanied by appropriate documented metadata which is linked with the data catalogue and data model.

3 **Master Data –** All data will have an identified golden copy.

4 **Data Validation –** Data will be validated at point of entry and users will never be asked twice for the same data.

5 **Data Retention -** Master data will be maintained in line with regulatory and business requirements.

6 **Channel independence –** Access to common information stores are designed to be available to all appropriate systems.

7 **Sharing Data -** Where possible data and analysis should be made available to third or external parties and this should be done in a done in a consistent, reliable, and ethical way, whilst safeguarding privacy.

8 **Data Quality –** Data quality should be documented and monitored.

9 **Data Currency –** Data must shown to be timely for purpose.

10 **Agency Wide Identifier -** Business critical data objects will have an agency wide unique identifier.

TECHNICAL

1 **Governed Evolution –** All elements of technology have a planned evolution and an agreed lifecycle ensuring supported version levels.

2 **Hosting -** Technologies should be cloud based and comply with data residency.

3 **Disaster Recovery –** Business activities must be appropriately maintained despite systems interruptions.

4 **Support model –** Support model will be simple with no manual interventions.

5 **Monitoring and Measurement –** Technologies will be designed to support monitoring and measuring.

6 **Alignment -** Technologies will be aligned to MCA patterns & standards unless there is a clear strategic business case for differentiation.

7 **Balancing Service Levels –** Technologies must balance total cost of ownership and service levels.

8 **Reliability, Availability and Scalability-** Projects will be implemented on reliable, scalable, and available technologies that are easily maintained.

9 **Repeatable Activities –** Any activates that are performed multiple times following a pre-set list of steps should be automated.

10 **Modifications –** Modifications to package implementation should balance the total cost of ownership over the lifetime of the service.

RADIO AND COMMUNICATIONS

1 **Business Agility -** Radio and Comms will create a strong foundation for the future minimising costs for changes in regulatory requirements.

2 **Governed Evolution –** All elements of radio and comms have a planned evolution and an agreed lifecycle ensuring supported version levels.

3 **Availability –** Solutions will be aligned to service level agreements and these should be measurable.

4 **Stakeholders Alignment -** Changes affecting key stakeholders (aircraft, police, ambulance, RNLI , Natural England, Planning Authorities, etc.…) will be agreed.

5 **Standards based compliance -** All services and solutions will comply with the appropriate current and emerging international and regional standards.

SECURITY

1 **Least Privilege -** A user or function will be given no more privilege than necessary to perform a task.

2 **Reuse –** Preference should be given to deploying existing or reusable security controls that enable a assured level of service.

3 **Minimize attack surfaces –** Minimization of exposure and therefor risk.

4 **Segregation of data -** Production information is separated from data used in development, test and training.

5 **Data location -** All data should be stored in a suitable secure location, and the method used recorded along with associated security controls.

6 **Security by Design -** Every element of information security must be designed to implement confidentiality, integrity and availability (both internal and external threats must be considered).

7 **Availability –** Systems must ensure delivery of required levels of service through a pervasive and resilient security framework that utilises known security frameworks (e.g. IAM).

8 **Fail security –** Failure of a component must not lead to a lower state of security.

9 **Need to know –** A user or function must establish a need to know information prior to that data being made available.

10 **Security ownership –** Security accountabilities and responsibilities will be made explicitly clear.

END USER COMPUTING

1. **Flexibility** - Staff should be able to perform their work anytime from anywhere.
2. **Segregation –** Corporate resources should not be intrinsically linked to the corporate network.
3. **Compliance –** All devices should meet a minimum compliance standard and automatically report on any compliance breaches.
4. **Remote Management –** The end user estate shall be able to be managed remotely for support & maintenance.
5. **Lifecycle –** Devices specifications should be able to support a 4 year device refresh cycle.
6. **Applications –** Applications should be web based where possible, and should not require any specific device alterations.
7. **Accessibility** – Device offerings should support accessibility needs through alternative screen size & touchscreen capabilities.
8. **Core Operating Environment** – All devices should be built with a consistent environment including O/S, standard set of applications, and remain compatible within an agreed number of previous versions.
9. **Management Tools –** Common tools and software should be used to manage the end user estate to avoid technical lock in and ensure skills are highly available.
10. **Procurement –** Devices should be procured in the most cost effective way and make use of warranties to reduce total cost of ownership.