1 Architecture Design Principles

1.1 Primacy of principles

1.1.1 Statement

These principles apply to Mott MacDonald Group.

1.1.2 Rational

Compliance with these principles enables consistent and efficient services supporting the business.

1.1.3 Implications

- Without this principle, decisions taken will be inconsistent and based on the priorities of individuals
- Initiatives introducing technological change will not begin until they are examined for compliance with the principles
- Principles will evolve based on Group risk tolerance and demand for innovation

1.1.4 Improvement Actions

- Define a governance framework for principle enforcement.
- Establish a regular review cadence to evolve principles.
- Introduce KPIs to measure adherence.

1.1.5 Control Linkage

This principle is supported by the Group policy - Information security and digital risk management .

This policy:

- Sets out the Group’s approach to information security and digital risk.
- Embeds risk management into all activities, aligned with business integrity and “Our Code”.
- Is implemented and monitored through the business management system (STEP), meeting ISO 27001 and Cyber Essentials Plus standards.
- Assigns clear responsibilities at executive, business, and project levels.
- Emphasises continuous improvement and staff training.

1.2 Maximise benefits to Mott MacDonald

1.2.1 Statement

Enterprise IT architecture decisions are made to provide maximum benefit to Mott MacDonald Group as a whole.

1.2.2 Rational

Decisions made from a Group perspective have greater long-term value than decisions made from any particular region, unit or division perspective. Maximum return on investment requires decisions to adhere to Group-wide drivers and priorities. No minority group will

detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.

1.2.3 Implications

- Achieving maximum enterprise-wide benefit requires governance and processes to manage information - we must not rely on technology alone
- Some groups may have to concede their own preferences for the greater benefit of the entire enterprise
- Service development priorities must be established by the entire enterprise for the entire enterprise
- Services should be made available across Mott MacDonald
- As business priorities change, service delivery priorities must be adjusted
- Track the usage rates and business value for all services to ensure they remain relevant to the end user

1.2.4 Improvement Actions

- Introduce a value realization framework (e.g., BRM).
- Allow controlled local innovation within global standards.
- Use metrics to track service adoption and ROI.

1.2.5 Control Linkage

This principle is supported by the Information Security Management System (ISMS). This requirement:

- Mandates group-wide, consistent management of information security and IT assets.
- Embeds risk assessment, system planning, and acceptance processes that ensure IT decisions benefit the Group as a whole.
- Requires service delivery and supplier management to align with Group priorities.
- Supports compliance, audit, and continuous improvement, ensuring ongoing value realisation and enterprise benefit.

1.3 Design for resilience

1.3.1 Statement

Mott MacDonald can continue to deliver to it's customers and people in the event of service failures

1.3.2 Rationale

We are a digital business and dependent on our services; therefore, we must consider the reliability of services throughout their design and use. Hardware failure, vendor failure, natural disasters, compromise, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of continuing to operate in the event of a service failure.

1.3.3 Implications

- The risks of business interruption must be established in advance and managed
- Management includes but is not limited to monitoring of service failures, periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities.

- Recoverability, redundancy, and maintainability should be addressed at the time of design
- Services must be assessed for criticality and impact on the enterprise in order to determine what level of continuity is required and what corresponding recovery plan is necessary
- Mott MacDonald must establish the capability and capacity to ensure services are managed to ensure resilience.

1.3.4 Improvement Actions

- Include cyber resilience and threat modelling.
- Adopt chaos engineering to test failure scenarios.
- Define RTO (Recovery Time Objective) and RPO (Recovery Point Objective) for critical services.

1.3.5 Control Linkage

This principle is supported by the ISMS Requirement – Business continuity management. This requirement mandates resilient systems, backup, and disaster recovery processes, with regular testing and continuous improvement to ensure service continuity.

1.4 Comply with regulations

1.4.1 Statement

Services must comply with all relevant laws, standards, policies, and regulations

1.4.2 Rationale

Our Code requires that we follow local legislation and regulation wherever we work. STEP lays out the internal requirements we must adhere to.

1.4.3 Implications

- Initiatives delivering technological change must understand and ensure compliance with laws, regulations, and both external and internal policies regarding the collection, retention, and management of data
- Services must comply with our ISMS and other requirements in STEP
- Staff must be aware of their responsibilities
- Operational processes must monitor and assess change in laws and regulations to ensure a secure and compliant service is maintained

1.4.4 Improvement Actions

- Automate compliance checks using tools like CSPM or GRC platforms.
- Include data residency and sovereignty in assessments.
- Maintain a regulatory change log and impact tracker.

1.4.5 Control Linkage

This principle is supported by the ISMS Requirement – Compliance. This document mandates compliance with data protection, privacy, copyright, and all relevant legal requirements, supported by regular audits and retention schedules.

1.5 Enterprise data will be managed as an asset

1.5.1 Statement

Data is an asset that has value to Mott MacDonald and is managed accordingly

1.5.2 Rationale

Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. To realise the value of our data we must ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

1.5.3 Implications

- All data must have an owner with accountability for data accuracy and integrity
- Where data is duplicated the master source must be documented. Copies must be synchronised with the master data source
- Data must be easy to find and retrieve
- Data must be secure. Data must only be accessible to the people and services entitled to process the data.

1.5.4 Improvement Actions

- Implement a formal data governance framework (e.g., DAMA-DMBOK).
- Assign data stewards and owners.
- Promote data literacy across the organization.

1.5.5 Control Linkage

This principle is partially supported by the Group policy - Information security and digital risk management . This policy sets out the Group’s approach to protecting and managing information as a key asset, embedding information security risk management into all activities, and supporting compliance with international standards.

Gap Identified

The current policy focuses primarily on security and risk management. It does not comprehensively address data governance, stewardship, data quality, or the broader concept of data as an enterprise asset.

1.6 Ease-of-use

1.6.1 Statement

Applications are easy to use so users can concentrate on tasks at hand

1.6.2 Rationale

The harder a user has to work to understand a service, the less productive that user is. A good user experience drives uptake and encourages users to work within the integrated information environment instead of developing isolated systems and processes. Intuitive and consistent user interfaces facilitate easy transition between systems, training is kept to a minimum, and the risk of using a service improperly is low.

1.6.3 Implications

- Services selection and design must consider user experience, not just functionality
- Accessibility legislation and best practice must be taken into account
- It should be possible to apply Mott MacDonald branding to provide a common look and feel
- Services should be accessible on all compliant devices
- Principle 2 may dictate that some minority groups accept a less than optimal user experience

1.6.4 Improvement Actions

- Apply user-centred design (UCD) principles to all new applications and major updates.
- Conduct usability testing and accessibility audits to ensure applications are intuitive and inclusive.
- Use design systems for consistency across platforms and to streamline the user experience.
- Develop or adopt a formal usability or user experience standard within STEP, referencing recognised frameworks (e.g., ISO 9241-210, WCAG).
- Establish clear usability metrics (e.g., user satisfaction, task completion rates) and incorporate user feedback into continuous improvement cycles.

1.6.5 Control Linkage

At present, there is no explicit STEP control or policy that directly addresses ease-of-use, usability, or user experience in application or system design.

Gap Identified

While related policies (such as ISMS and EDI) support secure and inclusive environments, they do not set requirements for usability or user-centred design

1.7 Requirements based change

1.7.1 Statement

Mott MacDonald led changes to our services will only be delivered in response to a business need

1.7.2 Rationale

Our services exist to support the business in delivering it's work. We will only change services in support of this goal. Maintaining our security and compliance is a business need. Modern suppliers will deliver frequent minor improvements.

1.7.3 Implications

- All change requires a documented business need
- An Enterprise IT Architecture check will be performed before technology change projects are approved
- We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs
- Modern evergreen services are preferred. Our change management processes must accommodate continuous vendor delivered improvements.

1.7.4 Improvement Actions

- Integrate agile and DevOps practices for responsiveness.
- Maintain a living backlog of business needs.
- Use lightweight documentation for rapid iteration.
- Formalise business case and requirements traceability for all service changes, ensuring that every change is explicitly linked to a validated business need and is reviewed as part of the change management and architectural assessment process.

1.7.5 Control Linkage

This principle is broadly supported by Information Security Management System (ISMS). This requires that all IT system changes are subject to change management, risk assessment, and authorisation, ensuring that changes are aligned with a documented business need and are properly evaluated for security and operational impact.

STEP Diagrams 10.1 Plan to deliver Group IT requirements Plan to deliver Group IT requirements and 13.6 Manage IT procurement and contract management provides an outline control as it lists activities such as defining the business need and undertake IT security and architecture assessments.

Gap Identified

While these controls provide important checkpoints, there is currently no explicit control that mandates end-to-end traceability of all changes to a validated business requirement throughout the change lifecycle. This gap means that, in practice, some changes could proceed without robust, ongoing linkage to business needs, especially in agile or iterative delivery contexts.

1.8 Control technical diversity

1.8.1 Statement

Technological diversity will be limited by using common platforms and shared services

1.8.2 Rationale

Every service we support carries a cost in addition to licensing/subscription. Services that are not properly supported introduce compliance and security risks. We can only ensure services are adequately supported at an acceptable cost by limiting the number of services offered and minimising complexity.

1.8.3 Implications

- Service duplication must be avoided. Service reuse should be the default. Business processes may need to adapt to allow reuse
- Commoditised processes should be adopted to maximise reuse
- Where duplication is introduced, consolidation of existing services must be considered
- Strategic suppliers will be used where they provide an acceptable solution
- Technology choices will be constrained to solutions already in use unless it is demonstrated that a new technology is required to meet business need

1.8.4 Improvement Actions

- Develop and implement a formal technology standardisation policy or platform governance framework.

- Establish criteria and processes for approving new platforms or technologies, prioritising the use of existing common platforms and shared applications and services.
- Regularly review the technology landscape to identify and rationalise redundant or overlapping technologies.
- Maintain a service catalogue and lifecycle roadmap.
- Encourage reuse through internal app stores or marketplaces.
- Allow innovation sandboxes for controlled experimentation.

1.8.5 Control Linkage

This principle is partially supported by STEP 13.6.8 – 1 Undertake IT security and architecture assessments. This control requires IT Architects to conduct security and architecture checks for new systems, significant upgrades, or contract changes, ensuring that suppliers meet these requirements before being considered for new services.

While this provides a checkpoint for reviewing technical decisions, STEP does not explicitly mandate the use of common platforms, shared services, or the limitation of technological diversity.

Gap Identified

There is currently no explicit control that requires technology standardisation, application or platform rationalisation, or the adoption of shared services to limit technical diversity. This gap means that, in practice, technical diversity may persist unless further controls or governance are established.

1.9 Design for interoperability

1.9.1 Statement

Services should be designed or chosen to allow sharing of data and capabilities

1.9.2 Rationale

Interoperability enables data synchronisation to ensure data is consistent; access to data for analytics and therefore better decision making; innovation through both data sharing and sharing of capabilities.

1.9.3 Implications

- Services must allow secure access through APIs to data held and capabilities delivered
- Open standards should be used to simplify integration
- Modular, loosely coupled solutions that support composability are preferred
- Ease of use, performance and scalability must be considered when designing or assessing the integration capability of a service

1.9.4 Improvement Actions

- Develop and implement a STEP control or policy that mandates interoperability as a requirement for all new or changed services.
- Require the use of open APIs, standard data formats, and shared vocabularies for all integrations.
- Establish interoperability checks as part of architecture and procurement assessments.

- Promote modular, loosely coupled architectures to support future integration and data sharing.
- Use open APIs and standard data formats (e.g., JSON, XML).
- Promote semantic interoperability through shared vocabularies.
- Adopt modular architecture (e.g., microservices, data mesh).

1.9.5 Control Linkage

There is currently no explicit control in STEP or the ISMS that mandates interoperability, open standards, or integration as a requirement for new or changed services. While the ISMS ensures security and operational control, it does not address the need for systems to share data and capabilities.

Gap Identified

Whilst designing for interoperability is an architectural principle, there are currently no explicit controls that require all services to be designed or selected for interoperability. This gap means that interoperability may not always be prioritised or enforced in practice.

1.10 Tier 1 Cloud SaaS first

1.10.1 Statement

New services will be delivered as a Cloud SaaS solution from a tier 1 provider unless there is a compelling business reason

1.10.2 Rationale

The scale of public cloud services enables the delivery of highly scalable, cost effective, secure solutions. Consumption based billing and rapid provisioning supports flexibility as required by our Group Strategy. Tier 1 vendors provide services appropriate to the size and complexity of Mott MacDonald and are able to invest heavily in product development.

1.10.3 Implications

- Choose Software as a Service (SaaS), before Platform as a Service (PaaS), before Infrastructure as a Service (IaaS), before on-premises solutions
- Consider the TCO. Cloud SaaS services from a tier 1 vendor may appear expensive, but the hidden costs increase significantly as you move down to PaaS, IaaS and on-premises, and management for a service from a tier 2 supplier
- Develop defensible charging models to help with this decision making
- Services should demonstrate a commitment to continuous product development

1.10.4 Improvement Actions

- Evaluate vendor lock-in and portability options.
- Include sustainability and carbon footprint in vendor assessments.
- Define exit strategies and data migration plans.

1.10.5 Control Linkage

This principle is partially supported by the Information Security Management System (ISMS) and STEP, specifically:

- STEP Diagram 10.1 – Plan to deliver Group IT requirements:
  Outlines the planning process for IT service delivery, including consideration of security, sustainability, and portability.
- STEP Diagram 13.6 – Manage IT procurement and contract management:

Provides a framework for procurement and contract management, including supplier assessment, risk management, and contractual controls.

- ISMS Requirements – Third Party Service Delivery Management & System Planning and Acceptance
  Require documented service agreements, risk assessments, and compliance checks for all IT services and suppliers, supporting evaluation of vendor lock-in, sustainability, and exit planning.

While these controls provide a foundation for reviewing technical decisions and supplier suitability, STEP does not explicitly mandate the use of Tier 1 suppliers or SaaS for all services. As a result, the architectural principle of “Tier 1 Cloud SaaS first” is not always prioritised or enforced in practice.

Gap Identified

Although “Tier 1 Cloud SaaS first” is established as an architectural principle, there are currently no explicit STEP or ISMS controls requiring all services to be designed or selected to use Tier 1 suppliers or SaaS. This gap means that the prioritisation and enforcement of Tier 1 suppliers and SaaS solutions may be inconsistent across the organisation.