# Table of Contents

What are Architecture Principles? .................................................................................................................. 3
Further Information ........................................................................................................................................... 3
References ........................................................................................................................................................ 3
Summary of Principles ....................................................................................................................................... 4
Principles ............................................................................................................................................................ 6
  Business Principles .......................................................................................................................................... 6
  Principle 1: Requirements-Based Change .......................................................................................................... 6
  Principle 2: Re-Engineer Processes First ........................................................................................................... 7
  Principle 3: Use A Total Cost Of Ownership Model .......................................................................................... 8
  Principle 4: ICT Responsibility ........................................................................................................................ 9
  Technology Principles ...................................................................................................................................... 10
  Principle 5: Reuse Before Buy, Buy Before Build ............................................................................................ 10
  Principle 6: Common Use Applications And Solutions .................................................................................... 11
  Principle 7: Control Technical Diversity ........................................................................................................ 12
  Principle 8: Ensure Interoperability And Reduce Integration Complexity ....................................................... 13
  Principle 9: Use Mainstream Technologies, Industry Standards And Open architecture .................................. 14
  Principle 10: Ensure Security, Confidentiality And Privacy ............................................................................. 15
  Data Principles .................................................................................................................................................. 16
  Principle 11: Data Is An Enterprise Asset ......................................................................................................... 16
  Principle 12: Common Vocabulary And Data Definitions ................................................................................ 17
What are Architecture Principles?
Architectures define the underlying general rules and guidelines for the use and deployment of all ICT resources and assets across the department. They reflect a level of consensus among the business units of the department, have been endorsed by the ICT Strategy Committee, and form the basis for making future ICT decisions.

Further Information
Contact: Manager Enterprise Architecture or Manager ICT Strategy & Governance.

References
- The Open Group Architecture Framework (Togaf) v9
- Australian Government Architecture Reference Models Version 1.0
- Australian Government Information and Communications Technology Security Manual (ISM)
Summary of Principles

Business Principles

Principle 1: Requirements-Based Change
Statement: Changes to applications and technology are only made in response to an approved business case.

Principle 2: Re-Engineer Processes First
Statement: Applications and solutions will only be built or redeveloped after business processes have been analysed, simplified or otherwise redesigned as appropriate.

Principle 3: Use a Total Cost of Ownership Model
Statement: A total cost of ownership model applies to applications and technologies which balance the costs of development, support, security, risk mitigation, disaster recovery and retirement against the costs of flexibility, scalability, ease of use and reduction of integration complexity.

Principle 4: ICT Responsibility
Statement: eBusiness is responsible for owning and implementing ICT processes and infrastructure. eBusiness is responsible for implementing applications in partnership with the business owners that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

Technology Principles

Principle 5: Reuse before Buy, Buy before Build
Statement: We will re-use and integrate existing applications and solutions defined as target architecture before investing in new solutions. We will use Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) before building software.

Principle 6: Common Use Applications and Solutions
Statement: Development of applications and solutions used across the department is preferred over the development of similar or duplicative applications which are only provided to a particular business unit.

Principle 7: Control Technical Diversity
Statement: Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Principle 8: Ensure Interoperability and Reduce Integration Complexity
Statement: Applications must be designed, acquired, developed and enhanced such that data and processes can be shared and integrated across the department and with our partners, recognising that some information is confidential and access to it is controlled by the business owner.

Principle 9: Use Mainstream Technologies, Industry Standards and Open Architecture
Statement: ICT solutions must use industry-proven, mainstream technologies except in those areas where advanced higher-risk solutions provide a substantial benefit. Mainstream is defined to exclude unproven technologies and older technologies and systems that are identified as not part of our target architecture.

Statement: Applications and systems must be implemented in adherence with all applicable security, accessibility, confidentiality, and privacy policies, architectures and legislation.
Data Principles

Principle 11: Data is an Enterprise Asset
Statement: Data is an asset that has value to the enterprise and is managed accordingly, recognising that some information is sensitive and access to it is controlled by the business owner.

Principle 12: Common Vocabulary and Data Definitions
Statement: Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users.
Principles

Business Principles

Principle 1: Requirements-Based Change

Statement: Changes to applications and technology are only made in response to an approved business case.

Rationale: This principle will foster an atmosphere where the information environment changes in response to the needs of the business. It will allow business needs to be considered and prioritisation of projects based on which business cases bring the greater benefit to the department.

Implications:
- Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.
- We do not fund a technical improvement or system development unless an agreed documented business case exists.
- Client engagement will be part of normal project management processes.
- ICT Governance needs to be clear with stated policies around roles and responsibilities, controls, processes.
Principle 2: Re-Engineer Processes First

Statement: Applications and solutions will only be built or redeveloped after business processes have been analysed, simplified or otherwise redesigned as appropriate.

Rationale:
- Business processes will be streamlined, efficient and cost effective.
- Business processes, business rules will be well understood and documented.
- Reduce total cost of system ownership.

Implications:
- Time and resources will have to be invested for business process modelling activity.
- Organisational change may be required to implement reengineered business processes.
- Business process modelling is a skill that needs to be developed with supportive training.
- Business areas need to document their processes. The amount and quality of documentation is commensurate with the risk involved.
- Analysis and documentation of business processes enables the discovery of common processes.
Principle 3: Use a Total Cost of Ownership Model

Statement: A total cost of ownership model applies to applications and technologies which balance the costs of development, support, security, risk mitigation, disaster recovery and retirement against the costs of flexibility, scalability, ease of use and reduction of integration complexity.

Rationale:
- Leads to higher quality solutions.
- Enables improved planning and budget decision-making.
- Reduces the ICT skills required for support of obsolete applications or old standards.
- Simplifies the ICT environment and should reduce lifecycle costs.
- Longer term stability, affordability, productivity, performance and a better understanding of the real cost of ICT.

Implications:
- Need to consider technical and user training costs when making major platform or software upgrades.
- Need to consider appropriate funding for application and system maintenance and support over a lifecycle.
- Need to develop better costing and monitoring tools.
- Need to develop decision criteria for new ICT investments that also considered whole-of-government obligations.
- Factors contributing to ongoing support costs such as disaster recovery and service levels must be defined and considered up front as part of the consideration for the solution.
Principle 4: ICT Responsibility

**Statement:** eBusiness is responsible for owning and implementing ICT processes and infrastructure. eBusiness is responsible for implementing applications in partnership with the business owners that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

**Rationale:**
- Effectively align business unit expectations with ICT capabilities, timelines and costs to achieve improved outcomes, focus eBusiness capability and improve customer satisfaction.
- A centralisation of ICT skills and responsibilities allows for a reduction in cost to the department by reducing duplication of responsibilities, skills, infrastructure and processes.
- Some business applications, such as Corporate systems, require specialist subject matter expertise. Those skills reside in the application owner's business units.*
- Allows for a strategic and holistic focus.

**Implications:**
- ICT responsibilities must be clarified within the department.
- ICT processes to meet user-defined requirements.
Technology Principles

Principle 5: Reuse before Buy, Buy before Build

Statement: We will re-use and integrate existing applications and solutions defined as target architecture before investing in new solutions. We will use Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) before building new software.

Rationale:

- Use of effective packaged solutions is increasing.
- Using tested solutions reduces risks and reduces delivery times.
- Reduces total cost of ownership.
- Most business units share a considerable amount of common functionality. This must be understood and leveraged in future-state architectural design.
- This functionality is often duplicated unnecessarily in different enterprise solutions, increasing costs and reducing effectiveness.
- Meets our obligations under whole-of-government policies.

Implications:

- Commonality among business functions/programs must be identified and enterprise solutions provided in a reusable manner. The department's standard program typologies are an example.
- Existing solutions, available functional components and business services must be catalogued in such a fashion that makes it easier to determine their reusability.
- A target architecture for the department must be defined.
- Longer lead time in analysis phase but shorter overall delivery times.
- Newly purchased software should be compatible with the department’s technical architecture.
- Define and adhere to a formal technical review process for evaluating new solutions.
- Develop and publish a portfolio of current applications and solutions.
- Software licensing agreements and system development contracts should be written to allow for re-use.
- Whole of Government solutions must be considered as part of this process.
- The Enterprise Architecture process must be optimised to ensure that reuse occurs where possible, and that building for reuse occurs where necessary.
Principle 6: Common Use Applications and Solutions

Statement: Development of applications and solutions used across the department is preferred over the development of similar or duplicative applications which are only provided to a particular business unit.

Rationale:

- Duplication of solutions leads to increased costs in management and maintenance.
- Within DIISR, there will always be conflicting and competing projects and subsidiary initiatives for the limited resources available. Keeping an enterprise wide perspective is the most fair and equitable mechanism for resolving such conflicts.
- Managing from the enterprise wide perspective provides the best opportunity to identify duplication of effort, as well as to rationalise and reuse solutions.
- Adopting a holistic view within DIISR will maximise the potential synergies across business unit boundaries and increase the reuse potential of solutions developed.

Implications:

- DIISR must identify commonality of functionality and build ICT solutions in a reusable fashion.
- Whole of Government and existing solutions are considered in the initial stages of every project.
- Business units which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability.
- Business units will be directed to use established ICT capabilities that meet their needs rather than seek to develop bespoke solutions. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Some business units may have to concede their own preferences for the greater benefit of the entire department.
- Application development priorities must be established for the entire enterprise with business owner involvement and acceptance.
- DIISR's governance processes must ensure that tailored solutions that address unique agreed requirements are strictly managed to avoid incremental divergence from the Enterprise Architecture over time.
Principle 7: Control Technical Diversity

Statement: Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale:
- Every technology supported increases cost to the organisation, such as maintaining skill sets, licensing and infrastructure.
- Limiting the number of supported components will simplify maintainability and reduce costs and risks.
- The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements.
- Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications:
- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
- Technology choices will be constrained by the choices defined as target architecture within the department.
- Target architecture will take account of technology advances when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated and agreed.
- Evaluating technologies and implementing them into the environment are different steps.
- New technologies will only be introduced if they provide value to the Department.
**Principle 8: Ensure Interoperability and Reduce Integration Complexity**

**Statement:** Applications must be designed, acquired, developed and enhanced such that data and processes can be shared and integrated across the department and with our partners, recognising that some information is confidential and access to it is controlled by the business owner.

**Rationale:**
- Interoperability enhances the ability to share data and other resources.
- Increases the ability of the department to adapt and change.
- Increases efficiency while better serving our clients.
- Reduces product and support costs.
- Reduces technical and financial risk and improves delivery times.
- Standards for interoperability additionally help ensure product support from multiple vendors, and they facilitate supply chain integration.
- Ease of access to information and services is essential to DIISR’s internal productivity.
- Some information is confidential and access to it is controlled by the business owner.

**Implications:**
- Define and adhere to a formal set of integration criteria when evaluating vendor products.
- Use industry standards to expose application functions.
- Commitment from the department to support shared standards is essential.
- A process for setting interoperability standards, reviewing and revising them periodically, and granting exceptions must be established.
- DIISR interoperability standards and industry standards will be followed except where there is and agreed and compelling business reason to implement a nonstandard solution.
Principle 9: Use Mainstream Technologies, Industry Standards and Open Architecture

Statement: ICT solutions must use industry-proven, mainstream technologies except in those areas where advanced higher-risk solutions provide a substantial benefit. Mainstream is defined to exclude unproven technologies and older technologies and systems that are identified as not part of our target architecture.

Rationale:
- Reduce risks through comprehensive risk analysis process.
- Ensures robust product support.
- Enables great use of commercial and government off-the-shelf components (COTS/GOTS) and to take advantage of industry trends and future technology.
- Allow flexibility and adaptability in product replacement.
- Industry standards help ensure consistency improving the ability to manage systems and improve user satisfaction. They also protect existing business and ICT investments maximising return on investment and reducing costs.

Implications:
- Determine a life for existing technology so that moving to newer technologies is managed with more certainty
- Manage resistance to change.
- Balance desire for the most modern with the risks and costs associated with being a first mover.
- Tie policies, standards and procedures that govern acquisition of technology to this principle.
- Existing ICT products and platforms must be identified and documented.
- Develop strategies to move away from solutions that are not part of our target architecture in the ICT portfolio.

Statement: Applications and systems must be implemented in adherence with all applicable security, accessibility, confidentiality, and privacy policies, architectures and legislation.

Rationale:
- Safeguard sensitive and proprietary information.
- Ensure the integrity of the information.
- Enhances public trust.

Implications:
- Security must be incorporated as an essential part of all information systems.
- Relevant documentation needs to be produced as part of application and system development.
- Identify, publish and keep the applicable policies current.
- Educate staff on issues of security, privacy and confidentiality.
- Require assignment of security levels from business areas.
- Develop common security components for use by all applications.
Data Principles

Principle 11: Data is an Enterprise Asset

Statement: Data is an asset that has value to the enterprise and is managed accordingly, recognising that some information is sensitive and access to it is controlled by the business owner.

Rationale:
- Data is a valuable departmental resource and has real, measurable value.
- The purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions.
- DIISR must carefully manage data to ensure that it is secure, we know where it is, can rely upon its accuracy, and can access it when and where it is needed.
- Departmental assets are carefully managed, and data is no exception.

Implications:
- There is an education task to ensure that all business units within the department understand the relationship between value of data, sharing of data, and accessibility to data.
- The department must make the cultural transition from “data ownership” thinking to “data stewardship” thinking.
- The role of data stewardship is critical because obsolete, incorrect, or inconsistent data could be passed to departmental personnel and adversely affect decisions across the department.
- Part of the role of data stewardship is to ensure data quality. Procedures must be developed and used to prevent and correct errors in information holdings and to improve the processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality.
- Policies and procedures will need to be developed on data stewardship and on information sharing.
- Authoritative sources must be identified.
- Data warehouses need to be developed to facilitate information availability for decision making.
- Data needs to be restructured for easy access and management.
- Sufficient metadata must be stored with the information to enable its easy management and retrieval.
Principle 12: Common Vocabulary and Data Definitions

Statement: Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users.

Rationale:
- The data used in the development of applications must have common definitions throughout the department to enable sharing.
- A common vocabulary will facilitate communications, enable dialog to be effective and assist in interfacing systems and exchanging data.

Implications:
- The department must establish the initial common vocabulary.
- Whenever a new data definition is required, the definition effort will be co-ordinated and reconciled with the corporate "glossary" of data descriptions.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted enterprise-wide definitions and understanding.
- Multiple data standardisation initiatives need to be co-ordinated.
- Where available, an Australian or Australian Government standard should be followed as a basis for data definitions.