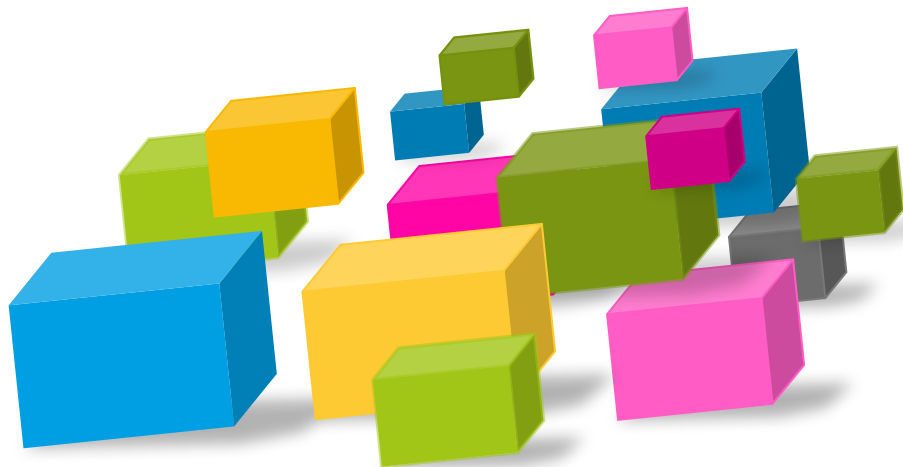


Architecture Principles Examples

Kim Horn

Version 1.0

1 August 2016





Background

- In managing a complex technical environment, decision making is informed and supported by strategies, plans, principles, policies and standards. This document details our Architecture Principles.
- These Architecture Principles set the broad direction in the areas of Enterprise, Data, Applications, Infrastructure and Security architecture. They should be able to be understood by anyone within the organisation.
- More specific principles will be developed within the particular areas i.e. Data, Applications, etc.. These will be more technical and are designed to provide guidance to architects and designers.

Intended Audience

- These Architecture Principles should be communicated to relevant business and technology stakeholder groups to ensure common understanding and usage. Stakeholder groups include senior business and technology managers, architects, designers, delivery managers and project managers.

Usage

- These Architecture Principles will be used by all architects in support of their recommendations and high-level decision making (see Appendix for examples). They represent a set of high-level requirements that will be used “by default” to guide the planning, design, development, deployment and operations of the organisation’s applications and infrastructure.
- Whenever proposed solutions do not align with any of the principles, the reasons behind the requested exception need to be documented and reviewed by the Architecture Team.



Architecture Principles are intended to guide the organisation in delivering business imperatives in the most efficient and effective manner through Information Technology

- A principle is a statement of intent for use of IT
- It describes preferred practices to be followed when implementing new or upgraded systems
- It is a “soft policy” or a “fat standard”
- It is a foundation to build the enterprise architecture
- It supports:
 - Business capabilities and strategies
 - IT strategies
 - Vision of the IT environment
 - Architecture drivers

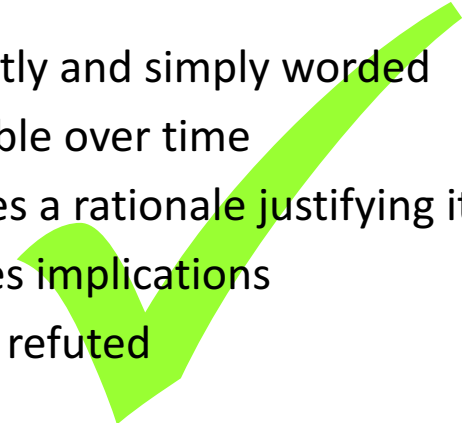
Principles should be:

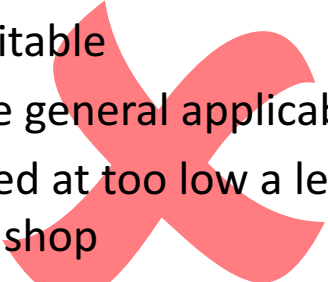
- Abstract - should be a general rule not a specific practice.
- Falsifiable – a reasonable person can disagree with it. It should have examples that refute it, other wise its not worth stating. If it is universally true then it is uninteresting. They are not platitudes.
- Prescriptive not descriptive – rather than state a fact it directs action.



- Each Principle has:
 - Title, short description or catch-phrase
 - Principle, statement of the principle
 - Rationale, the reason for being included
 - Implications, the effect it will have on future IT related decisions (people, processes, architecture, technology)
- Principles are defined at multiple levels in line with the Enterprise Architecture Framework
 - Business Principles
 - Guiding IT Principles
 - Architecture Principles
 - Business Architecture Principles
 - Application Architecture Principles
 - Information Architecture Principles
 - Integration Architecture Principles
 - Technology Architecture Principles
 - Security Architecture Principles



- Recommends a preferred course of action
 - Is directly and simply worded
 - Is durable over time
 - Provides a rationale justifying its use
 - Outlines implications
 - Can be refuted
- 

- A “motherhood” e.g. easy to use
 - A general business statement e.g. profitable
 - Little general applicability
 - Stated at too low a level e.g. we’re a .net shop
 - Not durable
 - More than an opinion e.g. because “I say so”
- 

Definition of Principles – The Format



Statement	The statement succinctly and unambiguously describes the principle.
Rationale	The Rationale highlights the business benefits of adhering to the principle. It describes the relationships to other principles, and the intentions regarding a balanced interpretation. It describes situations where one principle would be given precedence or carry more weight than another for making a decision.
Implications	The Implications highlight the requirements, both for the business and IT, in carrying out the principle in terms of resources, costs and activities.



- Teams should be able to autonomously manage their architecture, need to remove top down hierarchical management as this introduces delays and compromises, and is driven by lack of trust;
 - Reduce decisions going through a centralised Architecture Review Board (ARB);
 - Instead Architecture is driven by well formulated, documented and rationalised Principles;
 - Move Architecture Governance to the teams.
-
- Only significant architecture change that violates our principles needs to go through ARB;
 - All new solutions should check list the principles.
-
- Principles are what ARB should deal with, not solutions;
 - Principles are evolved, changed and agreed by ARB;

Architecture Principles – Architecture Check List



ID	Name	Architecture Domain					
		Enterprise	Applications	Information	Integration	Technology	Security
A01	Maximise the overall benefit to the organisation	✓					
A02	Ensure that change is based on requirements	✓	✓	✓	✓	✓	✓
A03	Reuse before buy before build	✓	✓	✓	✓	✓	✓
A04	Control technical diversity	✓	✓	✓	✓	✓	✓
A05	Remain technically current	✓	✓	✓	✓	✓	✓
A06	Manage data as an asset			✓			
A07	Ensure interoperability			✓	✓		
A08	Ensure reliability, scalability, availability and manageability			✓		✓	
A09	Ensure security and privacy		✓	✓	✓	✓	✓

A01 – Maximise the overall benefit to the Organisation



Statement	Technology decisions are made to provide maximum benefit to the organisation as a whole.
Rationale	<ul style="list-style-type: none">• By re-using existing technology within the organisation we maximise our existing investment. Therefore applications and technology already deployed and maintained should be considered when deploying new systems and proposing solutions.• Decisions made from an organisation-wide perspective have greater long-term value than decisions made from the isolated perspective of individual business units.• Minimise fragmentation of information and maximise investment by deploying common services that serve organisation-wide purposes.• Minimise the deployment of multiple (and overlapping) solutions that serve individual business units purposes.• Duplicated capability is expensive to develop and maintain and often results in duplicated and conflicting data i.e. it undermines the establishment of a common system of record.
Implications	<ul style="list-style-type: none">• Priorities must be established for the entire organisation.• As needs arise, priorities must be adjusted. A forum with comprehensive stakeholder representation should make these decisions.• Use of common services should be a ongoing goal.

A02 – Ensure that change is based on requirements



Statement	Ensure that change is based on requirements.
Rationale	<ul style="list-style-type: none">• This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes.• This is to ensure that the purpose of the information support - the transaction of business - is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.
Implications	<ul style="list-style-type: none">• Requirements include functional and non-functional requirements (NFR). The architecture is largely driven by the non-functional requirements. The NFR's need to be captured and realistic e.g. availability of 99.9% vs 99.999% as they are major drivers of cost of implementation and operations.• Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.• We don't fund a technical improvement or system development unless a documented business need exists.• Change management processes conforming to this principle will be developed and implemented.• The purpose of this principle is to keep us focused on business, not technology needs - responsive change is also a business need.



Statement	<ul style="list-style-type: none">• Consider the re-use of existing applications and technologies before investing in new solutions. Only invest in new solutions that will provide clear business advantages and demonstrable cost savings.• Use “commercial off the shelf” (COTS) solutions and technologies (including SaaS) to increase capability, leverage industry economies of scale and lower the total cost of ownership.• Select integrated suite solutions where the business value of integration exceeds the value of interfacing the “best of breed” solutions.
Rationale	<ul style="list-style-type: none">• The use and availability of effective packaged solutions is increasing.• Using tested and supported solutions reduces risks.• This Reduces the total cost of ownership.• If a new solution is deemed to be necessary, COTS application packages from strategic vendors will be utilised for the enterprise applications before we look to other vendors or initiate internal development efforts.
Implications	<ul style="list-style-type: none">• Software license agreements and system development contracts should be written to allow for re-use.• If a new solution is required, we will look to purchase packages first. If we can get 80% of the value required from a package, we will purchase it.• If two or more packages have similar functionality, we will purchase the one from our strategic vendor.• If a critical business driver exists to modify the package, we will leverage the package vendor to make the change.



Statement	Technological diversity is controlled based on a defined set of policies and standards to ensure that technology services are efficient, sustainable, robust and secure. We will promote coherence across technologies by dealing with a smaller set of major vendors generally preferring “good enough” components over “best of breed”.
Rationale	<ul style="list-style-type: none">• Limiting the number of supported components will simplify maintainability and reduce costs.• Technological diversity is controlled to minimise the cost of maintaining multiple and often duplicate technologies and the connectivity between them.• Fewer technologies to maintain will improve the response time to support issues.
Implications	<ul style="list-style-type: none">• We are not freezing our technology baseline. Technology advances are welcomed and will be analysed for business benefits and compatibility with the current infrastructure and staff capabilities.• Guidelines for acquisition of technology must be linked to this principle.



Statement	The technical environment will be technically current with both software and hardware kept at vendor supported levels.
Rationale	This principle will ensure that all elements of the technical environment are maintained at supported versions of hardware and software to avoid obsolescence, unnecessary downtime due to unsupported environments, lack of knowledge of systems that have not been updated in a considerable time and increase in general availability and manageability characteristics of the systems under our control.
Implications	<ul style="list-style-type: none">• Funds need to be allocated in operating budgets to ensure that there is a periodic refresh of both hardware and software technologies.• Lifecycle management plans for key technologies needs to be developed and maintained.• We need to ensure that proactive maintenance and planning is undertaken.



Statement	Data is an asset that has value to the organisation and is managed accordingly. Data is an enterprise asset that should be leveraged across the organisation.
Rationale	<ul style="list-style-type: none">• Data is a valuable corporate resource; it has real, measurable value.• Accurate, timely data is the foundation of our decision making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.• Information lifecycle management is used to manage the retention of the data and is appropriately disposed off based on its classification.• Protecting the data is paramount to ensure that company information is kept safe.
Implications	<ul style="list-style-type: none">• Each data set must have a Information Owner accountable for its quality, validation, auditing and security in order for it to be regarded as a trusted source.• Obsolete, incorrect, or inconsistent data could adversely affect decisions across the organisation.



Statement	Software and hardware should conform to defined standards that promote interoperability for data, applications and technology.
Rationale	<ul style="list-style-type: none">• Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing technology investments.• Standards for interoperability additionally help ensure support from multiple vendors for their products.• Using open standards and industry standards help better support business process integration and data accessibility.• Open and standards based integration enables and supports data principles.
Implications	<ul style="list-style-type: none">• Interoperability and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.• A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.• The existing technology platforms must be identified and documented.



Statement	All solutions must conform with the non-functional requirements as agreed with the system stakeholders and ensure that it meets fundamental criteria for reliability, scalability, availability and manageability.
Rationale	There is a need to meet increasingly higher levels of service demanded by customers. Flexibility is needed in the IT environment to enable migration toward a highly available environment, with the capability to be expanded to meet additional capacity demands. This implies a rigorous service based environment that is readily measured and managed.
Implications	<ul style="list-style-type: none">• Increased costs may be incurred in developing robust solutions that need to be balanced against business benefits.• Design for available and scalable services is a significant challenge requiring the development of additional design skills. In particular, solutions must be designed to recover from failure.• Choice of ready-built solutions will be constrained by their ability to support continuous availability, be scalable, and be readily manageable.• Systems management software is still maturing and the full benefits may not be immediately realisable.• Processes are required for the agreement, monitoring, and review of service levels.



Statement	Secure all information and resources to comply with corporate policies, local laws and regulations, international and local data privacy standards. At the same time, make information more accessible to users, with controls and restrictions to those having appropriate authority to view and modify the information.
Rationale	<ul style="list-style-type: none">• Providing information significantly increases the abilities of the users and promotes self help / service• Information Assets must have a classification level because the classification drives the access and security requirements for protecting them.
Implications	<ul style="list-style-type: none">• Enterprise security infrastructure in place for use by all enterprise applications.• Security policies published, actively maintained, and enforced through audits and reviews.• Chief security architect/officer in place.• Data classification guidelines established and enforced to comply with privacy laws and to protect sensitive or proprietary data.