EA Principles - complete list

Approved by Technical Architecture Design Council 9th April 2014

	#	Name	Description	Rationale	Implication	Applicable to Solution Y/N	Application
Overarching Architecture Principals	1	Principles apply to all	Architecture principles apply to all IR business units, programmes and projects.	A single set of architectural principles will ensure the provision of consistent, measurable, quality information across IR. This will enable balanced, consistent decision-making on architectural or design choices and trade-offs.	Enterprise Architecture principles must take priority over other design principles at business unit, programme or project level, with any departure approved at Board level or through formal delegation e.g. to the Design Authority.		
	2	One coherent architecture	There is a single joined-up architectural view of IR current and desired future states.	All Enterprise Architecture components must fit a single, coherent framework. This is to ensure IR maintains knowledge and control of the end-to-end tax system, and is not reliant for this knowledge on external parties if future changes are required.	IR must retain the knowledge and ownership of the architectural framework including methods, standards, models and content, regardless of where, how, or by whom these are developed, or methodologies used. Architectural content must be delivered to IR in line with this framework, and knowledge transfer achieved as part of delivery.		
	3	Business driven architecture	All investment in changes to business, information applications, and technology is in response and directly traceable to IR strategic objectives and business drivers.	Investments are only made where there are clear business drivers for change. Solutions exist to support business outcomes and change should not occur without a business driver.	IR will move towards a complete and consistent Enterprise Architecture model encompassing business functions, processes, organisational structures and business roles, and supporting information, applications and technology to achieve strategic objectives and outcomes. Solutions must demonstrate strong links to IR's Enterprise Architecture model.		
	4	Safeguard the tax system	The tax system's integrity is paramount.	The integrity of the end-to-end tax system is critical to Crown revenue collection and social policy administration. Public trust in the tax system is essential to maintaining compliance with tax obligations. Regardless of which parties, agencies and systems are involved in its development and operation, IR must retain knowledge of, and operational control over, the working of the end-to-end tax system.	All systems and processes must be designed to maintain integrity, preserve information confidentiality, and ensure consistent, fair and accurate application of relevant IR legislation.		
	5	Comply with legislation	Our systems and processes comply with all relevant laws, policies, and regulations.	Failure to comply with all legislation would compromise IR ability to collect and disburse revenue as required, and erode the tax system's integrity.	Architecture ensures legislative needs are highlighted and compliant solutions defined.		
	6	Decisions based on the right information at the right time	All decisions are principle-based, informed and enforced.	Architecture provides confidence to decision makers that we are doing the right things, at the right time, for the right reasons, and do not deviate from IR strategic goals and business objectives.	Architecture must provide guidance so decision makers have the confidence to make and enforce decisions, and deliver on IR commitments.		
	7	Optimise the long-term value of investments	Enterprise Architecture optimises the long-term value of investments in tax and social policy systems.	A well-defined architecture optimises the economic value of our systems to ensure they are cheaper to run, maintain and change, and minimise investments that do not support IR strategic goals.	Initiatives and solutions must be the building blocks of a coherent Enterprise Architecture.		
	8	Mandated government services	Mandated Government Services become part of our common business services.	IR recognises the value of participating in AOG activities including sharing information and services with other agencies to minimise costs.	IR must adopt Government Services at the time appropriate to support its needs. To ensure Government Services are suitable for adoption, IR must be actively involved in their specification and as appropriate, influence their development.		
	9	Promote flexibility and agility	Enterprise Architecture must promote flexible policy, processes, and systems.	The organisation is required to change at an increasing rate to satisfy business demand.	During all stages of the change lifecycle, IR must specify and deploy capabilities and services that can be re-used, re-assembled and used for different purposes. Systems must offer a high level of configurability to minimise future development needs.		
	10	Common services and processes	Common services and processes ensure consistent results, and re-use across business units.	Re-using the same processes and services across the organisation reduces costs while providing a consistent customer experience.	Processes and services must be defined within a coherent framework which ensures they will be re-useable across the business. Duplicate processes and services must be rationalized and services and processes managed under a governance framework.		

Step 1:
Review all 41 EA Principles, and define whether they are (Y) or are not (N) applicable to the solution that is being assessed.

Step 2:
Specify how the EA Principle will be applied in relation to the solution being assessed.

Business Architecture Principles	11	Enable third parties to contribute	Third parties are able to deliver business functions in partnership with IR.	Allowing IR to focus on its core business will simplify core IR administration and provide opportunities to take advantage of capabilities within other agencies and partnerships.	IRs business services will need to be built within a coherent framework, including well-defined roles and responsibilities. Services identified as non-core will become candidates for sourcing via partnerships, All-of-Government (AOG) collaboration or intermediaries.		
	12	Business continuity	IRs business services will continue to operate despite the failure of individual components, or complete outage at locations.	The ability to operate is critical to IR ability to collect Crown revenue and the tax system's integrity.	Each change initiative must assess the impact of downtime on affected business services, develop a recovery plan, budget for additional infrastructure and added system costs, and more expensive service-level agreements.		
	13	Speed and quality	Applying architecture increases "speed-to-market" while maintaining outcome quality.	Quality cannot be compromised while IR improves its ability to respond to increased demand.	Business solutions must build on enterprise-wide capabilities to take advantage of economies-of-scale without impeding quality.		
	14	Integrated solutions	Integrated and unified business solutions will be provided to staff and customers.	Integrated solutions reduce the need for IR support by improving staff efficiency while providing customers with a simpler experience.	IR will need to develop an integrated view of business capabilities to ensure all initiatives improve integration at an enterprise level. Examples include channel strategy implementation, and a single Service-Oriented Architecture.		
	15	Fit for purpose, fit for use	Solutions must be fit for the purpose they are defined for, and fit to be used within IR.	IR must have processes and systems that allow services to be efficiently and effectively delivered. This will improve user experience and provide a reliable platform on which IR can do business.	IR needs to continue refining its common business services to ensure business capabilities remain fit for purpose. In addition, IR needs to align business capabilities to processes and systems to ensure they remain fit for use.		
Information Architecture Principles	16	Common data definitions	Data is consistently defined throughout the extended enterprise, are understandable, and available to all users.	A single set of understood and available data definitions will minimise system integration efforts, simplify data exchanges between systems, and facilitate communication and information exchange internally and between agencies.	As part of its enterprise information architecture, IR must establish a common data vocabulary for standardisation and change initiatives. These definitions will need to be properly used, documented and managed, and progressively migrated to existing systems and interfaces.		
	17	Data is trusted and owned	Each information object has a steward who provides and requires good practices for managing information over its life-cycle.	Stewardship provides a cohesive, trusted, timely, and secure set of data assets that enables consistent and credible business processes within IR and with external parties.	IR must identify and allocate data stewards at business and system levels. The allocation rationale, role definition, responsibilities and processes, such as dispute resolution, must be reflected in a Data Ownership Policy. Stewards must be accountable and responsible for the integrity, accuracy, classification, privacy, and usage of their designated data elements.		
	18	Information is an asset	As an asset of value to all of New Zealand, IR manages its information accordingly.	Quality information is critical to IR ability to function as an organisation. Furthermore, IR is the custodian of information increasingly sought after by third parties for use in decision making. Accurate, complete, reliable and timely information is essential to well-informed decision making. The execution of IR's responsibilities takes place in an increasingly open Public Sector.	Management of the lifecycle of core information must be formally delegated to an IR information steward who has appropriate authority and accountability for its quality and integrity, regardless of where it is located. The information steward must exercise responsibility for technological obsolescence, long-term preservation, and access.		
	19	Information is shared and available	Users require appropriate access to data necessary to perform their duties.	A single reliable and accessible view of information is essential to building customer trust and confidence, and promoting voluntary compliance. In line with government Information Management Principles, IR's data and information should be open, readily available, well managed, reasonably priced, and re-usable unless there are reasons for its protection. IR's data and information should also be trusted and authoritative.	IR must understand what data is to be used by whom. Data must be accessible to appropriate parties through IR's systems, search and collaboration tools. IR must evaluate its data in terms of being an authoritative source and develop policies and frameworks to support this.		
	20	Single system of record	A single system records the truth of any given information object.	Establishing a single system as the “owner”, or authoritative source, of data records ensures better data integrity, simpler systems, and better alignment with a common information model. This in turn improves or quality of services and ability to change them.	IR will need to develop a common information model as part of its Enterprise Information architecture, and to map data entities to their single system of truth. A framework will need to be developed to manage policies, processes, and the relationships between data in “master” and other repositories. New initiatives will be required to use or establish capabilities that implement these single record sources.		

Information System Architecture Principles	21	Buy before build	Buy suitable Commercial-Off-The-Shelf (COTS) or Free and Open Source Software (FOSS) products in preference to bespoke development, assuming the component in question is sufficiently flexible and fit for purpose. If appropriate, buying the required capability as a service should be considered.	Commercial software, open source software, and Software as a Service provides IR with an opportunity to obtain functionality faster and cheaper than building bespoke software. This approach will allow IR to focus on its core business and reduce specialist technology.	Selection processes must evaluate and select software that is fit for purpose. In some cases affected business processes will be tailored to align with functionality available from the selected product. Where this is not possible, software must be built in a way that does not lock IR into maintaining bespoke software. Over time the amount of bespoke development will be significantly reduced.		
	22	Configure, don't customise	COTS and FOSS products and AOG solutions will be configured with minimal customisation.	Once customised, COTS and FOSS applications are hard to upgrade and support increasing cost, complexity and maintenance risks.	To avoid customisation, IR may need to tailor some business processes to match processes supported by COTS, FOSS, or AoG products. Any customisation must be implemented in a way that does not impact a product's ability to be upgraded.		
	23	Capabilities have a clear purpose and scope	Solutions must be built on a set of capabilities and services, each of which has a clear business function and boundary.	Delivering solutions as integrated capabilities and services provides clarity to business, and results in a smaller set of applications over time. This simplifies integration, prevents capability duplication, and eliminates conflicting data and processes.	IR will need to increase standardisation of business processes across the organization to avoid the cost and complexity of each capability becoming unsustainable. Reference models will need to be enhanced to identify the scope and behaviour of capabilities, so processes and systems can be developed which optimise commonality and reuse.		
	24	Re-usable, modular, open and service-oriented	Solution architectures must be based on re-usable and modular components, using open standards and assembled using a services-oriented approach.	Composing services in this way allows IR to reuse investments to satisfy new business scenarios, and to operate with and consume services from other vendors or partner agencies.	Solution architectures must be designed for re-use so each provides a well-defined function that can be assembled with others as part of a bigger system. All modules must follow open standards to ensure they operate with each other in a services-oriented approach.		
	25	Version currency (n-1)	IR will aim to maintain software products within one version of the most current.	IR current software must be maintained to ensure software vendor support, the latest security patches, and current release new feature benefits.	A robust upgrade and patching programme must be implemented. System capability roadmaps must be developed to plan for appropriate upgrades, and factored into application lifetime planning, service provider selection, and support and warranty agreements.		
	26	Quality aspects are defined and assured	All requirements for new applications will include a set of non-functional requirements including Quality Characteristics.	Quality aspects contributing to a large part of the total cost of system ownership must be defined up-front and managed throughout to reduce delivery risks. Failure to identify quality aspects will lead to unexpected consequences and systems unable to satisfy IR needs.	Quality definitions and assurance measures must be included in every aspect of a change lifecycle and recorded as requirements. Architecture must directly address quality requirements to ensure solutions correctly address IRs on-going needs.		
	27	Applications run on various platforms or as a Service	Applications are independent of specific technology choices or service providers and can operate on a variety of technology platforms.	Platform independence offers more technology infrastructure choices which reduces obsolescence risks and vendor lock-in, and allows AoG Infrastructure Service adoption.	Infrastructure and information system architectures must define portability standards, application runtime environment preferences, and application and platform consolidation strategies.		
	28	Applications accessible via most channels with Digital first	Applications and services are designed and built to be independent of, and support, multiple delivery channels. Digital channels must be the first and preferred channels.	To allow users to choose the best channel and ensure the same results are obtained regardless of the channel chosen, business system functions can be offered over new channels with minimal additional investment.	Channels must not contain business functions, and applications providing business functionality must be independent of channels presenting it. Functionality must be exposed using a well-defined service framework to insulate the application from the consuming channel and allow the simple addition of new channels.		
	29	Ease of use	Solutions are designed for ease-of-use by staff and customers.	Easy-to-use solutions increase adoption levels and reduce errors improving staff efficiency and customer satisfaction.	Simplicity and ease-of-use must become primary considerations in IR process and system design; ease-of-use in one group should not be traded off at the expense of another.		
	30	Isolation of business rules	Definition and execution of policy and business rules are implemented separately from application code and data.	A policy of agility and speed-to-market for legislative changes should be applied consistently and correctly across products.	New solutions and systems are used to consume rules from external sources, such as rules engines. Any rules capability must be capable of defining rules efficiently and independent of the consuming systems.		
ructure	31	Rent before buy / build / operate	Rent technology infrastructure as a Service before Buy/Build/Operate (aka "Invisible Infrastructure").	This approach will allow IR to focus on its core business and simplify administration by delegating technology infrastructure to specialist service providers.	IR will need to develop detailed service level agreements and increase governance to effectively utilize service providers. The security architecture will need to address specific security concerns associated with managed services.		
	32	Consolidate infrastructures into common capabilities	Technology infrastructure should be consolidated into common capabilities to allow hosting on common platforms, including AOG platforms.	Consolidation simplifies the technology landscape and assists improved IR staff efficiency.	The IR technology infrastructure must be designed for a reduced footprint that takes advantage of technology supporting multiple services on a common operating platform. Application consolidation may be required as a first step to fully realize common technology capabilities.		
	33	Minimise environmental impact	Applications and Infrastructure should use resources efficiently to minimise environmental impact.	IR is required to comply with government policies for the efficient energy use of ICT resources.	IR will need to identify and apply environmental and energy rating standards during infrastructure and service procurement.		

Technology Infrast	34	Meet availability and performance requirements	Infrastructure should be designed and implemented to meet business availability and performance requirements.	The availability and performance of IR business systems are critical for our ability to administer Crown revenue and to the tax system's integrity.	Availability and performance requirements will need to be clearly understood and communicated through Business Impact Analysis of services to ensure selection of the right levels of resiliency, availability and performance.		
	35	Separate production environments	Production runtime environments are separated from their equivalent non-production environments to reduce production interference and security risks.	Separation reduces risks associated with production environment changes which can lead to system unavailability and data corruption. Separation also makes it harder for internal hackers to access production systems.	Separate environments require a larger investment in infrastructure, version control, access control, and de-identified data sets.		
	36	Common authentication and access control	Parties will need a single set of credential and access rights across all enterprise resources.	One set of credentials and common access control saves the business time and improves audit efficiency.	IR will need to expand its common authentication and access control capabilities to interact with AOG initiatives and provide common security for all IR business services.		
	37	Adapt to business requirements	Technology infrastructure should be adaptable to the business' changing requirements.	To satisfy business demand in a timely and cost effective way, IR is required to provide new services and to institute change at an increasing rate.	The technology infrastructure must be architected and designed to be able to provide throughput, volumes, and functions required by changes in a timely and cost effective way.		
Information Security Architecture Principles	38	Risk-based security, privacy and audit controls	Adopt a risk management approach covering all protective security areas. Apply the right level of Security control to match the risk tolerance level of each situation.	Control and enablement objectives are derived from analysing risks in terms of likelihood vs. consequences. Deliver the maximum level of security for the smallest investment of time and money, while having assurance risk has been properly evaluated and either appropriate controls applied, or risks explicitly accepted by the appropriate authority.	IRD must proactively and routinely manage security risks based on breach events probability and the impact breaches may have on IR's business continuity and reputation. IRD must: • identify and classify business information assets that need protecting • identify controls to mitigate the risks • do a cost / benefit analysis controls where not mandated by government guidelines • apply the right level of controls to match the risk tolerance level for each situation • ensure executives accountable for decisions are made aware of all applicable risks via an enterprise risk management framework • ensure that security risk assessments are completed as part of the IR change lifecycle		
	39	Multiple layers of security	Defend the enterprise with a variety of security controls, including managerial, operational, and technical controls (also called "defence in depth").	Layered security mechanisms increase the security of systems as a whole. If an attack caused a security mechanism to fail, other mechanisms should provide the necessary security to protect the enterprise.	Enterprise Information Security Architecture must be adopted to direct security control implementation which should have traceability to the safe enablement of business operations. Staff education is a critical piece of security architecture.		
	40	Separation of security concerns	Identify and group different security concerns in systems and business functions under the same set of security controls. Design security functions to be logically separate from the enterprise capabilities they protect.	Grouping systems and functions with similar security concerns under the same security controls simplifies security management, and ensures the right level of security is applied at the right place.	Security Architecture must define various security zones as required and controls applied in each. These should be designed as re-usable within the zone.		
	41	Security as an enabler of business objectives	Security enables IR to perform its business functions while ensuring information assets remain secure and available.	Security ensures IR has access to the information it needs to do its job and meet confidentiality, accessibility and integrity obligations, while allowing new technologies to be adopted.	Security requirements should be identified from a viewpoint of: • how can we do this safely? • how can we make it easy for people to do the right thing regarding security.		

EA Principles - for KDD

NOTE: do not alter any content, or change formatting on this page. All content edits should be done on sheet "All EA Principles"

Copy/Paste Area

Principle	Application	Filter Applicable to Solution Y/N
1. Principles apply to all - Architecture principles apply to all IR business units, programmes and projects.	0	0
2. One coherent architecture - There is a single joined-up architectural view of IR current and desired future states.	0	0
3. Business driven architecture - All investment in changes to business, information applications, and technology is in response and directly traceable to IR strategic objectives and business drivers.	0	0
4. Safeguard the tax system - The tax system's integrity is paramount.	0	0
5. Comply with legislation - Our systems and processes comply with all relevant laws, policies, and regulations.	0	0
6. Decisions based on the right information at the right time - All decisions are principle-based, informed and enforced.	0	0
7. Optimise the long-term value of investments - Enterprise Architecture optimises the long-term value of investments in tax and social policy systems.	0	0
8. Mandated government services - Mandated Government Services become part of our common business services.	0	0
9. Promote flexibility and agility - Enterprise Architecture must promote flexible policy, processes, and systems.	0	0
10. Common services and processes - Common services and processes ensure consistent results, and re-use across business units.	0	0
11. Enable third parties to contribute - Third parties are able to deliver business functions in partnership with IR.	0	0
12. Business continuity - IRs business services will continue to operate despite the failure of individual components, or complete outage at locations.	0	0
13. Speed and quality - Applying architecture increases "speed-to-market" while maintaining outcome quality.	0	0
14. Integrated solutions - Integrated and unified business solutions will be provided to staff and customers.	0	0
15. Fit for purpose, fit for use - Solutions must be fit for the purpose they are defined for, and fit to be used within IR.	0	0
16. Common data definitions - Data is consistently defined throughout the extended enterprise, are understandable, and available to all users.	0	0
17. Data is trusted and owned - Each information object has a steward who provides and requires good practices for managing information over its life-cycle.	0	0
18. Information is an asset - As an asset of value to all of New Zealand, IR manages its information accordingly.	0	0
19. Information is shared and available - Users require appropriate access to data necessary to perform their duties.	0	0
20. Single system of record - A single system records the truth of any given information object.	0	0
21. Buy before build - Buy suitable Commercial-Off-The-Shelf (COTS) or Free and Open Source Software (FOSS) products in preference to bespoke development, assuming the component in question is sufficiently flexible and fit for purpose. If appropriate, buying the required capability as a service should be considered.	0	0
22. Configure, don't customise - COTS and FOSS products and AOG solutions will be configured with minimal customisation.	0	0
23. Capabilities have a clear purpose and scope - Solutions must be built on a set of capabilities and services, each of which has a clear business function and boundary.	0	0
24. Re-usable, modular, open and service-oriented - Solution architectures must be based on re-usable and modular components, using open standards and assembled using a services-oriented approach.	0	0

Step 3:
Set filter to applicable principles (Y), and paste list into KDD.

25. Version currency (n-1) - IR will aim to maintain software products within one version of the most current.	0	0
26. Quality aspects are defined and assured - All requirements for new applications will include a set of non-functional requirements including Quality Characteristics.	0	0
27. Applications run on various platforms or as a Service - Applications are independent of specific technology choices or service providers and can operate on a variety of technology platforms.	0	0
28. Applications accessible via most channels with Digital first - Applications and services are designed and built to be independent of, and support, multiple delivery channels. Digital channels must be the first and preferred channels.	0	0
29. Ease of use - Solutions are designed for ease-of-use by staff and customers.	0	0
30. Isolation of business rules - Definition and execution of policy and business rules are implemented separately from application code and data.	0	0
31. Rent before buy / build / operate - Rent technology infrastructure as a Service before Buy/Build/Operate (aka "Invisible Infrastructure").	0	0
32. Consolidate infrastructures into common capabilities - Technology infrastructure should be consolidated into common capabilities to allow hosting on common platforms, including AOG platforms.	0	0
33. Minimise environmental impact - Applications and Infrastructure should use resources efficiently to minimise environmental impact.	0	0
34. Meet availability and performance requirements - Infrastructure should be designed and implemented to meet business availability and performance requirements.	0	0
35. Separate production environments - Production runtime environments are separated from their equivalent non-production environments to reduce production interference and security risks.	0	0
36. Common authentication and access control - Parties will need a single set of credential and access rights across all enterprise resources.	0	0
37. Adapt to business requirements - Technology infrastructure should be adaptable to the business' changing requirements.	0	0
38. Risk-based security, privacy and audit controls - Adopt a risk management approach covering all protective security areas. Apply the right level of Security control to match the risk tolerance level of each situation.	0	0
39. Multiple layers of security - Defend the enterprise with a variety of security controls, including managerial, operational, and technical controls (also called "defence in depth").	0	0
40. Separation of security concerns - Identify and group different security concerns in systems and business functions under the same set of security controls. Design security functions to be logically separate from the enterprise capabilities they protect.	0	0
41. Security as an enabler of business objectives - Security enables IR to perform its business functions while ensuring information assets remain secure and available.	0	0