



Implementation guide

Information and records management standard

May 2017



New Zealand Government

Document details

Document Identifier: 16/G8

Version	Date	Description	Revision due
0.1	Mar 2016	Development Draft	
0.2	May 2016	Final draft. Updated with consultation feedback	
1.0	Jul 2016	Published	
2.0	Oct 2016	Updated with new guidance	
3.0	Dec 2016	Updated with new guidance	
4.0	May 2017	Updated with new guidance	

Contact for enquiries

Government Recordkeeping Directorate

Archives New Zealand

Phone: +64 4 499 5595

Email: rkadvice@dia.govt.nz

Licence



Crown copyright ©. This copyright work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to Archives New Zealand, Department of Internal Affairs and abide by the other licence terms. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/nz/>.

Implementing the *Information and records management standard*

We have written this guide to help your organisation understand and apply the requirements of the *Information and records management standard*. The *Information and records management standard* was issued by the Chief Archivist on 22 July 2016.

The standard's purpose

The standard covers information and records in any format. It has been designed to support digital recordkeeping as the public sector continues its transition to digital business processes. The purpose of the standard is to ensure that business is supported by sound, integrated information and records management in complex business and information environments. This approach better reflects the way that most organisations now manage their information assets.

The earlier standards

This standard is the result of consolidating and streamlining the requirements from these Archives New Zealand standards:

- *Records Management Standard for the New Zealand Public Sector 2014*
- *S4 Access Standard 2006*
- *S5 Digital Recordkeeping Standard 2010*
- *AS/NZS ISO 13028: 2012, Information and documentation – Implementation Guidelines for digitization of records*

The Archives New Zealand standards above have been revoked and incorporated into this standard.

Further requirements for local authorities and approved repositories

Local authorities and approved repositories must follow:

- the *Protection and preservation of protected records: Instruction to local authorities*
- the *Maintenance of public archives: Instruction to approved repositories*.

How to implement the standard

The table in this document sets out three principles:

Principle 1: Organisations are responsible for managing their information and records

Principle 2: Information and records management supports business

Principle 3: Information and records are well managed

Under each principle are listed the minimum compliance requirements, an explanation for each requirement, and key guidance for implementing the requirements. This guidance will be regularly added to.

Principle 1: Organisations are responsible for managing information and records

To ensure information and records are able to support all business functions and operations, organisations must establish a governance framework. This framework will help an organisation to:

- develop strategies and policies to direct how information and records will be managed
- assign responsibilities and allocate resources
- establish provisions for information and records management in outsourcing and service delivery arrangements
- monitor information and records management activities, systems and processes.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
1.1 Information and records management must be directed by strategy and policy, and reviewed and monitored regularly.	<p>Governance frameworks are critical to the achievement of effective information and records management.</p> <p>Your organisation must set high-level strategy and policy for managing its information and records. The administrative head of the organisation must adopt it.</p>	<p>16/F4 Effective information and records management</p> <p>16/F6 Key obligations - Public Records Act 2005</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>Strategy and policy include:</p> <ul style="list-style-type: none"> • appointment of an Executive Sponsor to oversee information and records management – requirement 1.2 • clear requirements for the creation, capture and management of information and records – requirement 3.1 • setting an information security policy – requirement 3.4 • identifying and assigning responsibilities of senior management for information and records management – requirement 1.2 • identifying the need for information and records management staff or skills (do this through performance plans and/or service agreements) – requirement 1.4 • identifying business owners responsible for including information and records management in all systems and processes – requirement 1.5 • setting information and records management responsibilities for staff and contractors – requirement 1.6 • addressing information and records management in all service arrangements – requirement 1.7 • implementing an information security policy and appropriate security mechanisms – requirement 3.4 • implementing policies (and business rules and procedures) to ensure that information and records are kept for as long as they are required and to identify how their disposal is managed – requirement 3.6 • implementing policies to identify how to manage the disposal of information and records – requirement 3.7. 	<p>16/F9 Information and records management strategy</p> <p>16/F10 Information and records management policy</p> <p>Association of Local Government Information Management - Information Management Toolkit</p>
<p>1.2 Information and records management must be the responsibility of senior</p>	<p>Ultimate responsibility for information and records management lies with the administrative head and senior management. They must provide direction and support and ensure information and records</p>	<p>16/F6 Key obligations - Public Records Act 2005</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>management. Senior management must provide direction and support to meet business requirements as well as relevant laws and regulations.</p>	<p>management meets business requirements, the law and regulations. Responsibility for information and records management is cascaded down throughout the organisation, through various levels of management.</p> <p>Responsibilities are identified and assigned in strategy and policy.</p> <p>This requirement mirrors legislative obligations for example in the <i>State Sector Act 1988</i> (s.32(1)) and the <i>Local Government Act 2002</i> (s.42(2)) and reinforces the need for the Administrative head and senior management to provide high-level direction and support, including ensuring adequate resourcing for information and records management.</p>	<p>Association of Local Government Information Management - Information Management Toolkit</p> <p>AS/NZS ISO 30301:2012 Information and documentation – Management systems for recordkeeping – Requirements</p>
<p>1.3 Responsibility for the oversight of information and records management must be allocated to a designated role (the Executive Sponsor).</p>	<p>This new requirement clarifies what was implicit in the previous standard.</p> <p>The Executive Sponsor oversees information and records management.</p> <p>They must be a senior manager with organisation-wide influence and appropriate strategic and managerial skills. Their role is to:</p> <ul style="list-style-type: none"> • provide oversight of information and records management within the organisation, including monitoring of information and records management to ensure that this meets the needs of the organisation • ensure responses to monitoring/reporting requests from Archives New Zealand. 	<p>16/F7 Monitoring</p> <p>16/F11 Role and responsibilities of an Executive Sponsor</p> <p>16/F21 Information and records management capability</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>AS/NZS ISO 30301:2012 Information and documentation – Management systems for recordkeeping – Requirements</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>Include establishing this role in your policies and strategies for information and records management.</p> <p>The Executive Sponsor's role should be incorporated into their performance plan.</p> <p>Your organisation must advise us of your Executive Sponsor, when they are appointed and when the role changes hands.</p>	
<p>1.4 Organisations must have information and records management staff, or access to appropriate skills.</p>	<p>Your organisation must have staff with information and records management skills or be able to access this expertise.</p> <p>Each organisation's strategy will likely need a range of different levels of responsibility and skills. Reflect this in job descriptions.</p> <p>An organisation must be able to access information and records management skills through recruitment, service providers, and by networking with other organisations.</p> <p>An organisation must identify and assign responsibilities through strategy and policy, performance plans and/or service agreements.</p>	<p>16/G5 Providers of education and training in information and records management</p> <p>AS/NZS ISO 30301:2012 Information and documentation – Management systems for recordkeeping – Requirements</p>
<p>1.5 Business owners and business units must be responsible for ensuring that information and records management is integrated into business processes, systems and services.</p>	<p>This new requirement clarifies what was implicit in the previous standard.</p> <p>An organisation must identify business owners and system owners who are responsible for ensuring information and records management is included in all systems and processes used.</p> <p>Those owners must be aware that information and records</p>	<p>16/F9 Information and records management strategy</p> <p>ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles</p> <p>AS/NZS ISO 30301:2012 Information and</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>management requirements are needed when they move to a new service environment, develop new business processes, systems or services, or improve on existing business processes, systems or services.</p> <p>Responsibilities for business owners must be identified and assigned in policies and within performance plans.</p> <p>Business owners must demonstrate that they have considered information and records management requirements and assessed risks as part of the development process.</p> <p>This requirement places responsibilities more broadly within an organisation. It reflects a business manager’s detailed understanding of the information and records produced by and necessary to perform their work, and their responsibility for ensuring its management.</p> <p>Cascading responsibility to different business areas of the organisation lets business unit staff and information and records staff work together to ensure that information and records management is integrated into business processes, systems and services.</p>	<p>documentation – Management systems for recordkeeping – Requirements</p> <p>Information Asset Catalogue Template</p>
<p>1.6 Staff and contractors must understand the information and records management responsibilities of their role. They must understand relevant policies and procedures.</p>	<p>All staff of the organisation, including contractors, must understand their information and records management responsibilities.</p> <p>Policies, business rules and procedures must include clear requirements for all staff for creating and managing information and records.</p> <p>Contractors come into organisations to perform specified tasks.</p>	<p>16/F6 Key obligations - Public Records Act 2005</p> <p>16/F9 Information and records management strategy</p> <p>16/G3 Outsourcing business</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>Information and records that are produced and managed in their performance of the contract need to be covered. And contractors must know their information and records management responsibilities and the relevant policies and procedures.</p> <p>Responsibilities must be identified and assigned in policies. Skills, capabilities and responsibilities must be assigned in role descriptions and performance plans.</p>	
<p>1.7 Information and records management responsibilities must be identified and addressed in all outsourced and service contracts, instruments and arrangements.</p>	<p>This new requirement clarifies what was implicit in the previous standard.</p> <p>An organisation must ensure that information and records management is addressed in all service contracts, instruments and arrangements.</p> <p>An organisation’s strategy and policy must include responsibilities to ensure that information and records requirements are identified and addressed. An organisation must undertake risk assessments and address information and records management risks in contracts, instruments and arrangements that it agrees to.</p> <p>Service contracts, instruments and arrangements include:</p> <ul style="list-style-type: none"> • functions, activities or services of the organisation being outsourced to an external provider • functions, activities or services being moved to cloud services or other service providers (internal or external to the New Zealand public sector). <p>An organisation must ensure that the portability of information and records and associated metadata is assessed and appropriately</p>	<p>16/G3 Outsourcing business</p> <p>16/F9 Information and records management strategy</p> <p>.govt.nz New Zealand Data and Information Management Principles</p> <p>Information Security</p> <p>Guidance on Privacy Management</p> <p>Requirements for cloud computing</p> <p>NZ Government Procurement</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	addressed in outsourced and service contracts, instruments and arrangements.	
<p>1.8 Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business needs.</p>	<p>An organisation must regularly monitor information and records management activities, systems and processes to ensure they are meeting the needs of the organisation and conforming to requirements. Any issues identified through a monitoring process must be addressed in a corrective action plan.</p> <p>An organisation must monitor activities such as process and system audits of systems that are high-risk, high-value, or both. Any system of assurance for information and records management should be integrated into the wider organisational assurance processes.</p> <p>The Executive Sponsor has responsibility for overseeing this monitoring.</p>	<p>16/F7 Monitoring</p> <p>16/F11 Role and responsibilities of an Executive Sponsor</p> <p>16/F21 Information and records management capability</p> <p>AS/NZS ISO 19011:2014 Guidelines for auditing management systems</p> <p>AS/NZS ISO 9001:2008 Quality management systems – Requirements</p> <p>AS/NZS ISO 30301:2012 Information and documentation – Management systems for recordkeeping – Requirements</p>

Principle 2: Information and records management supports business

Information and records management ensures the creation, usability, maintenance, and sustainability of the information and records needed for business operations. It also ensures business operations meet government and community expectations.

By appraising business activities, organisations define their key information requirements. Appraisal is used to design and embed information and records management into business processes and systems.

Taking a planned approach to information and records management means:

- considering all operating environments
- ensuring that all service and systems arrangements consider the creation and management of information and records needed to support business.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>2.1 Information and records required to support and meet business needs must be identified.</p>	<p>This requirement provides the foundation for managing information and records in all environments.</p> <p>By appraising its functions and activities, an organisation can identify what information and records it needs to support business. It can also identify other requirements, including Treaty of Waitangi / Te Tiriti o Waitangi obligations, and government and community expectations.</p> <p>This work provides the foundation for understanding what information and records to keep. It identifies what systems and business processes are high-risk, high-value, or both for the organisation, and the information and records required to support these.</p> <p>An organisation must incorporate this work into comprehensive and authorised disposal authorities for its information and records</p>	<p>16/F2 High-value and high-risk information and records</p> <p>16/F10 Information and records management policy</p> <p>16/F14 Appraisal</p> <p>16/G9 Disposal - Authorisation</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles, section 7</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>An organisation must document in its business rules, policies and procedures decisions about what information and records are required. The decisions must also be reflected in specifications for systems and metadata schema.</p>	<p>Association of Local Government Information Management - Information Management Toolkit</p> <p>Information Asset Catalogue Template</p>
<p>2.2 High-risk/high-value areas of business, and the information and records needed to support them, must be identified and regularly reviewed.</p>	<p>An organisation must identify the areas of high risk, high value, or both of its business. An organisation can better prioritise how it manages, treats and protects these critical systems and the information and records they contain.</p> <p>An organisation must identify the likely or potential risks to information and records management and manage or mitigate them. This includes protecting the systems that manage information and records that are high-risk, high-value, or both, from loss and damage.</p> <p>An organisation should set up appropriate security measures and business continuity strategies and plans.</p> <p>By identifying high-value information and records at creation, an organisation can better manage and use this core asset.</p>	<p>16/F2 High-value and high-risk information and records</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles</p> <p>SA/SNZ TR 18128:2015 Information and documentation – Risk assessment for records processes and systems</p> <p>AS/NZS 5050:2010 Business continuity: managing disruption-related risk</p> <p>SA/SNZ HB 436:2013 Risk management guidelines – Companion to AS/NZS ISO 31000:2009</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>.govt.nz</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Information Security New Zealand Data and Information Management Principles Guidance on Privacy Management Information Asset Catalogue Template
<p>2.3 Information and records management must be design components of all systems and service environments where high-risk/high-value business is undertaken.</p>	<p>This new requirement clarifies what was implicit in the previous standard.</p> <p>In complex business and systems environments, it is important to design information and records management at the start. This is particularly important where the business involved is high-risk, high-value, or both.</p> <p>Include information and records management when you specify systems and service environments which manage high-risk and/or high-value information and records. You will be better able to manage and use the information and records.</p> <p>An organisation must consider at the start how to make system maintenance, migrations and decommissioning easier. In taking this “by design approach”, an organisation must ensure:</p> <ul style="list-style-type: none"> • systems specifications for information and records that are high-risk, high-value, or both, include requirements for managing them • systems specifications include requirements for minimum metadata needed to support information and records identification, usability, accessibility and context • it keeps documents about systems design, configuration and any changes 	<p>16/F8 Metadata for information and records</p> <p>16/G2 Integrated information and records systems, processes and practices</p> <p>16/G7 Minimum requirements for metadata</p> <p>17/Sp7 Authority to retain public records in electronic form only</p> <p>17/G13 Destruction of source information after digitisation</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	<p>made over time.</p> <p>Migrating and decommissioning systems can be expensive and time-consuming. An organisation may hold insufficient documentation about:</p> <ul style="list-style-type: none"> • the information and records held in the system • the configuration of the system • the disposal requirements for information and records held in the system. 	<p>AS/NZS 5478:2015 Recordkeeping metadata property reference set</p> <p>AS/NZS ISO 13028: 2012 Information and documentation – Implementation guidelines for digitization of records, section 6.2</p>
<p>2.4 Information and records must be managed across all operating environments.</p>	<p>This is partly a new requirement. Physical information and records are only part of an organisation’s “operating environment” and this requirement widens the standard to better cover digital information and records.</p> <p>If an organisation knows what information and records assets it has and where they are located and managed, then it can better control them. By maintaining visibility of information and records, no matter what system is used or where the information and records are stored, the organisation can better protect these assets.</p> <p>Information and records assets can be held in diverse systems environments, in third-party systems in the cloud, by service providers, and in a range of physical locations.</p> <p>By identifying where information and records are held, an organisation can better manage them in diverse system environments, storage environments and physical locations, and give appropriate access.</p>	<p>16/F3 Text messages</p> <p>16/F13 Storage of physical records</p> <p>17/Sp7 Authority to retain public records in electronic form only</p> <p>17/G13 Destruction of source information after digitisation</p> <p>Association of Local Government Information management - Information Management Toolkit</p> <p>.govt.nz New Zealand Data and Information Management Principles</p> <p>Information Security</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Guidance on Privacy Management AS/NZS ISO 13028: 2012 Information and documentation – Implementation guidelines for digitization of records, section 6.2 and 6.4
<p>2.5 Information and records management must be designed to safeguard information and records with long-term value.</p>	<p>This requirement ensures that an organisation identifies which systems and service environments hold information and records with identified long-term value. This requirement builds on <i>Minimum Compliance Requirements 2.1 and 2.2</i>.</p> <p>Once the organisation knows what information and records are needed long-term and where they are kept, it can safeguard and manage them. Information and records required for the long term will outlive both the systems in which they are managed and any outsourcing arrangements and contracts with service providers.</p> <p>An organisation must ensure it plans and manages the protection of long-term information and records during transitions of systems and changes to service arrangements. Two such transitions are system migrations and decommissioning systems processes. Two such changes to service arrangements are termination of services and new outsourcing arrangements.</p> <p>An organisation must protect its long-term information and records during changes in administration and through changes in the machinery of government. This includes where information and records must be transferred between organisations.</p> <p>To help with identifying long-term information and records, an organisation can refer to their authorised disposal authorities.</p>	<p>16/F14 Appraisal</p> <p>16/G2 Integrated information and records systems, processes and practices</p> <p>16/G9 Disposal - Authorisation</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>.govt.nz Information Security</p> <p>Guidance on Privacy Management</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>2.6 Information and records must be maintained through systems and service transitions by strategies and processes specifically designed to support business continuity and accountability.</p>	<p>This new requirement makes the standard’s focus more explicit to include both physical and digital information and records.</p> <p>This requirement ensures that information and records are managed appropriately through system migrations and service transitions. Two examples are upgrades of systems and services offered in cloud environments.</p> <p>An organisation must have documented migration strategies, and appropriate planning and testing processes. These must ensure that information and records are not “left behind” or disposed of unlawfully.</p> <p>An organisation must use a managed process to migrate information and records and associated metadata from one system to another. The process must be managed to deliver records that are accessible, reliable and trustworthy. Maintaining appropriate system documentation will help to make migration strategies successful.</p> <p>An organisation must use migration and decommissioning processes that ensure that information and records are kept for as long as needed for business, legal requirements (including in line with authorised disposal authorities), and government, and community expectations.</p> <p>This requirement builds on <i>Minimum Compliance Requirement 2.2</i> and <i>Minimum Compliance Requirement 2.5</i>. They require that information and records that are high-risk, high-value, or both, are supported and migrated appropriately.</p> <p>The portability of information and records and associated metadata must be assessed in outsourced or service arrangements. Information and records</p>	<p>16/F15 Disposal</p> <p>16/G2 Integrated information and records systems, processes and practices</p> <p>16/G3 Outsourcing business</p> <p>17/Sp7 Authority to retain public records in electronic form only</p> <p>17/G13 Destruction of source information after digitisation</p> <p>AS/NZS ISO 13028:2012 Information and documentation – Implementation guidelines for digitization of records</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	must not be “left behind” in outsourced arrangements. Such arrangements must include provisions for transferring the information and records back to the organisation.	

Principle 3: Information and records are well managed

Effective management underpins trustworthy and reliable information and records that are accessible, usable, shareable and maintained. This management extends to information and records in all:

- formats (and associated metadata)
- business environments
- types of systems
- locations.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>3.1 Information and records must be routinely created and managed as part of normal business practice.</p>	<p>Policies, business rules and procedures must tell an organisation’s staff the requirements and responsibilities for creating, capturing and managing information and records.</p> <p>An organisation must regularly assess or audit its practices to demonstrate that its business rules, procedures and systems are operating routinely.</p> <p>An organisation must identify, resolve and document any exceptions that affect the creation, integrity, accessibility and usability of its information and records.</p> <p>An organisation’s staff and contractors must conform to policies, business rules and procedures, to ensure information and records are routinely created and managed.</p> <p>The Executive Sponsor is responsible for overseeing this monitoring. This requirement builds on the earlier principles in the standard.</p>	<p>16/F7 Monitoring</p> <p>16/F10 Information and records management policy</p> <p>16/G2 Integrated information and records systems, processes and practices</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>3.2 Information and records must be reliable and trustworthy.</p>	<p>An organisation’s information and records must have enough metadata to ensure they are reliable and trustworthy.</p> <p>Information and records must be accurate, authentic, and reliable as evidence of transactions, decisions and actions. This requirement ensures that information and records have appropriate minimum metadata to provide meaning and context (including te reo Māori), and that this metadata remains associated or linked.</p> <p>Do regular assessments or audits to demonstrate that management controls of business rules, procedures and systems are operating correctly. This provides assurance of the integrity of the information and records stored in the system.</p> <p>This requirement builds on the earlier principles in the standard.</p>	<p>16/F7 Monitoring</p> <p>16/F8 Metadata for information and records</p> <p>16/G7 Minimum requirements for metadata</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and Principles</p> <p>AS/NZS 5478:2015 Recordkeeping metadata property reference set</p> <p>AS ISO 23081-1:2006 Metadata for records – Principles</p> <p>AS/NZS ISO 23081-2:2007 Metadata for records – Conceptual and implementation issues</p> <p>AS/NZS ISO 23081-3:2012 Managing metadata for records – Self assessment method</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>3.3 Information and records must be identifiable, retrievable, accessible and usable for as long as they are required.</p>	<p>Information and records must be identifiable, retrievable from storage (physical or digital), and accessible, usable and reusable for as long as required.</p> <p>To maintain the accessibility and usability of physical information and records, an organisation must store them in appropriate storage areas and conditions.</p> <p>To maintain the accessibility and usability of digital information and records, an organisation must ensure it regularly migrates or moves them from one system or platform to another.</p> <p>An organisation must associate or link appropriate minimum metadata (including te reo Māori terms) to information or records to ensure the information and records can be identified, retrieved and shared.</p> <p>An organisation must regularly test systems and perform assessments or audits to demonstrate that the systems can locate and produce information and records that people can read and understand.</p> <p>This requirement builds on the earlier principles in the standard.</p>	<p>16/F8 Metadata for information and records</p> <p>16/F12 Public access to information and records</p> <p>16/F13 Storage of physical records</p> <p>16/G7 Minimum requirements for metadata</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles</p> <p>.govt.nz Information Security</p> <p>Open data Toolkit for Agencies</p> <p>Open data Toolkit for Local Government</p> <p>Guidance on Privacy Management</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>3.4 Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.</p>	<p>An organisation must protect information and records.</p> <p>An organisation must implement an information security policy and appropriate security mechanisms. The policy must cover information and records held physically or digitally, or both.</p> <p>Security measures must include:</p> <ul style="list-style-type: none"> • access and use permissions in systems • processes to protect information and records no matter where they are located, including in transit and outside the workplace • secure physical storage facilities. <p>Undertaking regular assessments or audits will help an organisation verify that access controls have been implemented appropriately and are working.</p>	<p>16/F12 Public access to information and records</p> <p>16/G13 Access16/F13 Storage of physical records</p> <p>16/Fm2 Disposal schedule and access status template (with examples)</p> <p>16/Sp2 Maintenance of public archives (Instruction to approved repositories)</p> <p>16/Sp3 Protection and preservation of protected records (Instruction to local authorities)</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles</p> <p>Official information Guides</p> <p>.govt.nz</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Information Security Guidance on Privacy Management
<p>3.5 Access to, use of and sharing of information and records must be managed appropriately in line with legal and business requirements.</p>	<p>This requirement builds on the requirements in Part 3 of the Public Records Act 2005.</p> <p>An organisation must ensure that access to, use and sharing of information and records are in line with legal requirements including:</p> <ul style="list-style-type: none"> • the <i>Official Information Act 1982</i> • the <i>Local Government Official Information and Meetings Act 1987</i> • the <i>Privacy Act 1993</i> • the <i>Health Information Privacy Code 1994</i> • organisational policies, business rules and procedures. <p>Undertaking regular assessments or audits of systems will help an organisation verify that access to, use and sharing of information and records is managed in line with business requirements, legal obligations and the Government ICT Strategy or Action Plan (where appropriate).</p>	<p>16/F7 Monitoring</p> <p>16/F12 Public access to information and records</p> <p>16/G13 Access</p> <p>16/Fm1 Access Authority Form</p> <p>16/Fm2 Disposal schedule and access status template (with examples)</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>Official information Guides</p> <p>.govt.nz Information Security</p> <p>Guidance on Privacy Management</p>
<p>3.6 Information and records must be kept for as long as needed</p>	<p>An organisation must implement policies, business rules and procedures to ensure that information and records are kept for as long as required, and to identify how their disposal is managed.</p>	<p>16/F15 Disposal</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
<p>for business, legal and accountability requirements.</p>	<p>The policies, business rules and procedures must be in line with the requirements of the <i>Public Records Act 2005</i> and authorised disposal authorities.</p> <p>Information and records must be sentenced and disposed of in line with the practices of authorised disposal authorities. This includes information and records located in business systems, in outsourced or service arrangements, or in physical storage. Disposing of digital information and records may be part of a planned migration process or the decommissioning of systems.</p> <p>Information and records of permanent value that are identified as public or local authority archives must be transferred to Archives New Zealand, an approved repository or a local authority archive, when authorised and no longer needed for business purposes.</p>	<p>16/F10 Information and records management policy</p> <p>16/F16 General disposal authorities</p> <p>16/Sp4 List of protected records for local authorities</p> <p>16/G4 Explanatory notes for the List of protected records for local authorities</p> <p>16/Sp5 GDA6: Common corporate service public records</p> <p>16/Sp6 GDA7: Facilitative, transitory and short-term value records</p> <p>16/Fm2 Disposal Schedule and Access Status template (with examples)</p> <p>16/G10 Disposal - Sentencing</p> <p>16/Fm4 Disposal - Precedent Register example</p> <p>16/F1 Methods of destruction</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		<p>16/G11 Disposal - Transfer</p> <p>16/F20 Transport of your transfer to Archives New Zealand</p> <p>16/F18 Digital transfer readiness characteristics</p> <p>16/F19 Digital transfers – interim operating model</p> <p>16/Fm5 Transfer Agreement Form</p> <p>16/Fm6 Deferral of Transfer Agreement Form</p> <p>16/Fm7 Deferred Transfer and Access Schedule template (with examples)</p> <p>16/Fm3 Disposal register example</p> <p>17/Sp7 Authority to retain public records in electronic form only</p> <p>17/G13 Destruction of source information after digitisation</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Association of Local Government Information Management - Information Management Toolkit
<p>3.7 Information and records must be systematically disposed of when authorised and legally appropriate to do so.</p>	<p>This requirement builds on the earlier principles in the standard.</p> <p>An organisation must implement policies, business rules and procedures that identify how the disposal of information and records is managed. This includes:</p> <ul style="list-style-type: none"> • assigning responsibility for sentencing and disposal of information and records (sentencing is using a disposal authority to decide whether to keep, destroy or transfer a record) • using disposal authorisation processes • implementing disposal actions • deleting metadata • decommissioning systems • documenting the disposal of information and records. <p>An organisation must be able to account for their disposal of information and records in business systems, outsourced arrangements, and physical storage. This includes providing evidence that the disposal of information and records is permitted and authorised under disposal authorities' and legal obligations, including the <i>Public Records Act 2005</i>.</p>	<p>16/F10 Information and records management policy</p> <p>16/F15 Disposal</p> <p>16/G9 Disposal - Authorisation</p> <p>16/Fm2 Disposal schedule and access status template (with examples)</p> <p>16/G10 Disposal - Sentencing</p> <p>16/Fm4 Disposal - Precedent Register example</p> <p>16/F1 Methods of Destruction</p> <p>16/G11 Disposal - Transfer</p> <p>16/Fm5 Transfer Agreement Form</p> <p>16/Fm6 Deferral of Transfer Agreement Form</p> <p>16/Fm7 Deferred Transfer and Access Schedule template (with</p>

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		<p>examples)</p> <p>16/Fm3 Disposal register example</p> <p>17/Sp7 Authority to retain public records in electronic form only</p> <p>17/G13 Destruction of source information after digitisation</p> <p>Association of Local Government Information Management - Information Management Toolkit</p> <p>.govt.nz Information Security</p> <p>Guidance on Privacy Management</p>