How to implement a compliant information management policy

IM Policy Checklist

The importance of a compliant record management process

Information and records are key strategic assets at the core of any business. Effective information management helps organisations to have meaningful, reliable and usable information available when their business needs it to enable effective and efficient business operations.

It is important that all organisations take accountability for the information and data they collect (whether it be generated from customers or through internal processes) and should establish processes that manage information and records securely, efficiently and systematically. A records management policy should set down the minimum level of compliance for information management best practice.

With information formats and storage options constantly changing and regulatory legislation and standards specific to various industry segments continuing to expand, it is becoming increasingly more important for businesses to implement structured information management processes and procedures.

Most importantly an information governance program formalises intentions for information and records management and therefore decreases the level of risk.

IM Policy Checklist

Step 1:
Develop an information management strategy

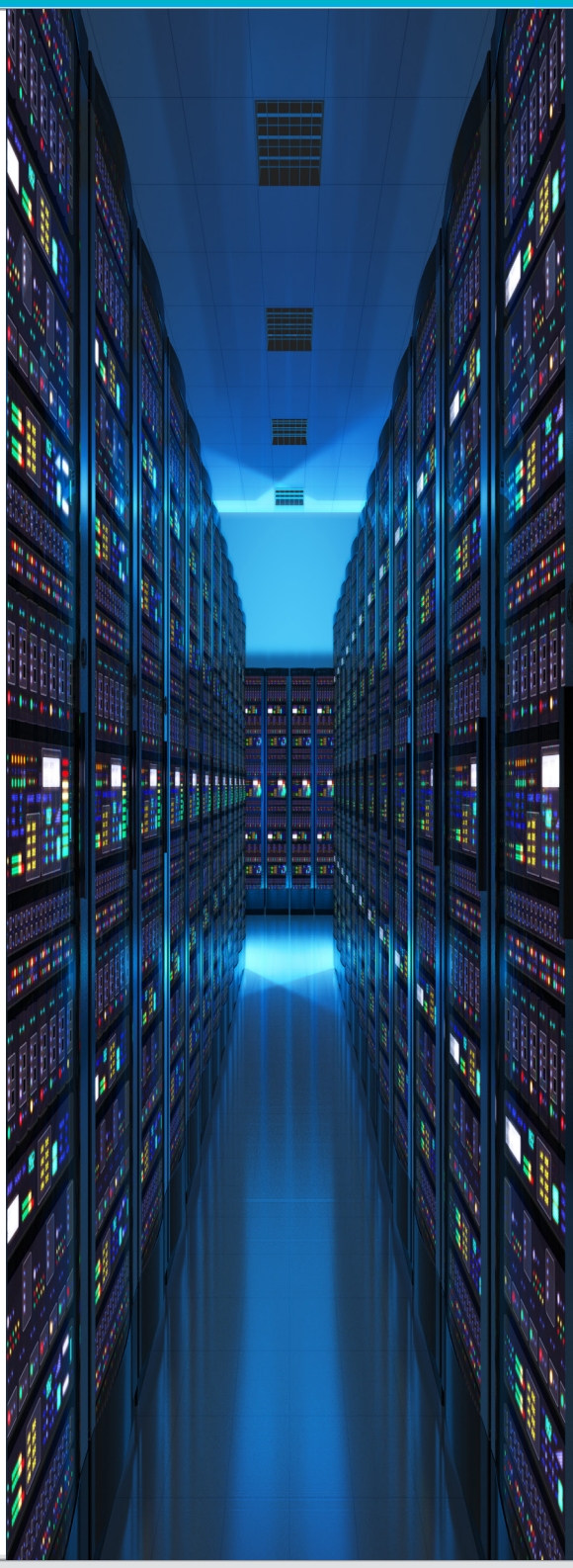
	Ensure senior executives adopt an organisation wide strategy on information management
	This strategy should align with other business objectives and strategies
	The strategy should overview the current situation and clearly outline a vision for a future state. It should also identify objectives and goals, an implementation plan and success metrics
	Appoint ownership, responsibility and accountability of the information management program. The person in this role typically sits in the legal, IT, compliance or risk business units
	The construction of an information management steering committee should also be considered, consisting of representatives from the above functional areas (this could also be expanded to tax and HR business units)
	Set information management responsibilities for employees and ensure you have staff with the right skill set to manage these responsibilities or that they have the opportunity to access this expertise from an outsourced agency
	Information should be identified and managed across all systems and processes used for example in the cloud, by external service providers, and in a range of physical locations
	Regularly communicate your information management strategy to the organisation so that every employee understands the information policies and procedures
	Provide ongoing training on information management policies and procedures for relevant staff, including testing and certification wherever possible

"Ensure senior executives adopt an organisation wide strategy on information management"

IM Policy Checklist

Step 2:
Manage your information intelligently

	Ensure there are clear requirements in place for the creation, capture and management of information to ensure that it is accessible, usable, shareable, maintained correctly and is sustainable. The focus should be on ensuring that information can be utilised to enhance business operations
	Information management policies should apply to all formats (and associated metadata), business environments, systems and locations
	Metadata is information that helps people to find, understand, authenticate, trust, use and manage information. If information and records have metadata, we know what it is, what it has been used for, and how to use it. Metadata also makes information and records easier to find. Information should have enough metadata to ensure it is reliable and trustworthy and provides meaning and context and that it remains associated or linked
	Information must be identifiable, retrievable from physical or digital storage and accessible, usable and reusable for as long as required
	Take a "by design" approach to information management. This ensures that considerations are made before, at the start of, and throughout the development and improvement of both new and existing business systems, processes and practices
	Use technology to intelligently manage your information and improve your information management program, for example: automated workflows, imaging/document capture and e-Discovery



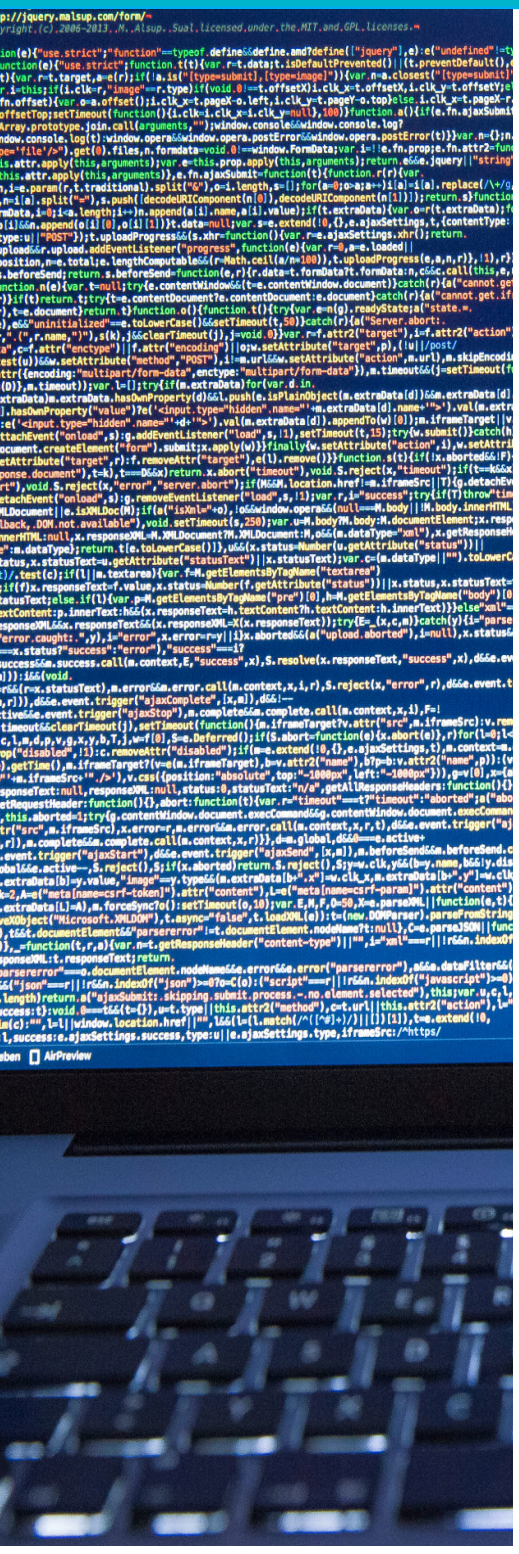
IM Policy Checklist

Step 3:
Securely protect your information

	Set in place an information security policy to maintain the confidentiality, integrity and availability of business information
	Identify high risk or high value business systems and processes and what information is required to support these
	Particular attention should be paid to systems that manage personal information as, if these are not managed correctly the business will be exposed to significant risk in regard to reputation, financial or material loss or breach of regulatory obligations. There are strict rules governing how an organisation may retain and use personal data and report on this is also required both to the individual concerned and to regulatory bodies. Organisations should be aware of these requirements and ensure that systems managing personal information and records are especially secure
	Potential mechanisms to ensure security of information include restricting access and use permissions in systems, implementing processes to protect information no matter where they are located including transport outside the workplace and ensuring secure physical storage facilities
	Protect critical systems and the information they contain with business continuity strategies and plans

"Set in place an information security policy to maintain the confidentiality, integrity and availability of business information. Identify high risk or high value business systems and processes and what information is required to support these"

IM Policy Checklist



Step 4:
Understand retention requirements

	Implement policies to ensure that information is systematically kept for as long as required for business and legal purposes and identify how disposal of this information is managed
	Policies must include a commitment by the organisation to adhere to any relevant legislation and governing standards
	Undertake legal investigation into the retention period for information within your specific industry segment and overlay this with the operational retention requirements of your business
	Ensure retention policies take into account information in systems, outsourced arrangements or physical storage
	Archiving services may be required for information of permanent or long term value
	Implement disposal authorisation policies and procedures
	Document the disposal of information as required (from internal systems, outsourced arrangements and physical storage). The disposal of information may need to be evidenced for legal purposes
	An organisation that keeps information and records for longer than required is exposed to three risks: cost, efficiency, and reputation. The costs of maintaining, accessing and preserving information is significant and systems work less efficiently if they contain too much information, making it harder and more time-consuming to find the information needed to carry out day to day business activities. Finally, not disposing of information responsibly and in a timely fashion puts organisations at risk of non-compliance and increases the risk of inappropriate access

IM Policy Checklist

Step 5:
Monitoring and audit processes

	Information audit policies should explain how the organisation will carry out reporting, internal audits and self-monitoring
	Regularly monitoring information management activities will ensure they are meeting the needs of the organisation and supporting business processes
	Organisations can monitor their compliance by assessing compliance against the requirements of standards issued by governing bodies such as Archives New Zealand or can benchmark against previous audit results to identify improvements or to identify issues of non-compliance
	Compliance audits can also be undertaken using internal auditors or an external party to provide an independent assessment of the organisation's information management program, practices and systems
	Identify, resolve and document any exceptions that affect creation, integrity or accessibility and usability of information
	Audits will assist in verifying that security protocols are being met
	Audits will also assist in verifying that access to, use or sharing of information is in line with business and legal requirements

The benefits of a structured information management policy include;

- *increasing efficiency by making retrieval faster and easier controlling how information and records are stored, maintained, accessed and managed for ease of use, reuse and sharing*
- *controlling the costs of managing information*
- *reducing the risk of breaches in both privacy and security*
- *supporting better decision making*
- *helping to identify and protect information and records that are high risk, high value, or both*
- *minimising the risk of unauthorised access or disposal*
- *facilitating legislative compliance*

Call our people now for a complimentary review of your current situation