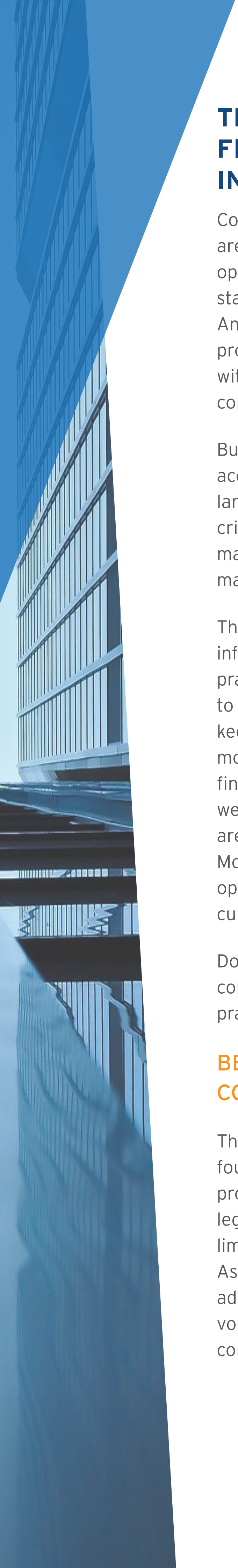
UNCOVERING OPPORTUNITIES TO IMPROVE COMPLIANCE ACROSS FIVE BEST PRACTICE AREAS

A MANUAL FOR COMPLIANCE PROFESSIONALS

IRON MOUNTAIN®



THINK OUTSIDE THE BOX: FIND THE KEY TO BETTER COMPLIANCE IN YOUR COMPANY'S INFORMATION

Companies of every size and specialisation are looking for ways to ensure that their operations align with the regulations and standards governing their specific industry. And with breach notification regulations proliferating at a break-neck pace, coping with change is the name of the game when it comes to compliance.

But as they work hard to understand and accommodate a rapidly changing regulatory landscape, many companies overlook a critical consideration that is essential to maintaining compliance: the five information management best practice areas.

This manual will help you understand the influence information management best practices have on compliance, and how to leverage these concepts as a means of keeping your operations up to date with the most pertinent regulations. Inside, you'll find worksheets that help you assess how well you stack up across each best practice area – and examples from actual Iron Mountain customers – so you can identify opportunities to promote a business-wide culture of compliance.

Doing so is the first step toward more compliant information management practices. Let's get started.

BEST PRACTICES ARE THE KEY TO COMPLIANCE

The five best practice areas form the foundation of an information management program that reduces risk by minimising legal exposure, improving governance and limiting the potential for fines and penalties. As such, assessing your organisation's adherence to these best practices will speak volumes to the overall strength of your compliance posture.

POLICIES AND PROCEDURES

Formal, company-wide policies set the standards for your overarching information management program and provide evidence of your commitment to maintaining compliant operations. These guidelines should address such important information management concepts as privacy, active records, vital records and destruction holds, to name a few.

It's essential that your policies and procedures are comprehensive – covering all forms of information, across all business units and locations – and fully documented and communicated organisation-wide. In addition, you should educate all employees about your policies and procedures and establish well-defined and formalised accountability – via an employee acknowledgement form – throughout the business.

RETENTION

A records retention schedule supports your organisation's efforts to protect its intellectual property, locate and retrieve documents for legal discovery, address compliance considerations and dispose of records at the end of their business lives. Think of your retention schedule as a universal set of rules that addresses all of the information you create or receive in the conduct of business.

Retention guidelines are best implemented in stages, starting with critical records from the most high-risk areas of your organisation and working out from there, following a systematic, staged approach. And to help you further reduce risk, you should regularly and consistently review changing regulations, industry standards and business mandates and update your retention schedule every 12 to 18 months.

INDEX AND ACCESS

Your organisation's ability to successfully locate and retrieve records using defined criteria, such as subject matter, record creator and system of creation, may be essential to satisfying legal and regulatory requirements – and avoiding the penalties associated with failing to do so.

Index and access go hand-in-hand because records must be properly organised to enable timely, accurate and controlled access that is authorised by the proper security controls. As such, it's important to perform a systematic indexing of all records by subject matter, regardless of the storage medium or location. This information should then be protected by clear ownership profiles and authorisation rights designed to control access to confidential information.

PRIVACY AND DISPOSAL

When conducted in accordance with a well-defined retention schedule, privacy and disposal practices that span all active and inactive records facilitate retrieval and help you decrease the corporate and brand risk related to the security of confidential information. To this end, you should build policies that promote company-wide implementation, education, ongoing assessment and accountability for the confidentiality of information as it is destroyed.

These efforts will help you ensure that records are disposed of in a consistent, secure manner – following formalised policies – so you can minimise undue risk and limit the potential for inadvertent data leakage.

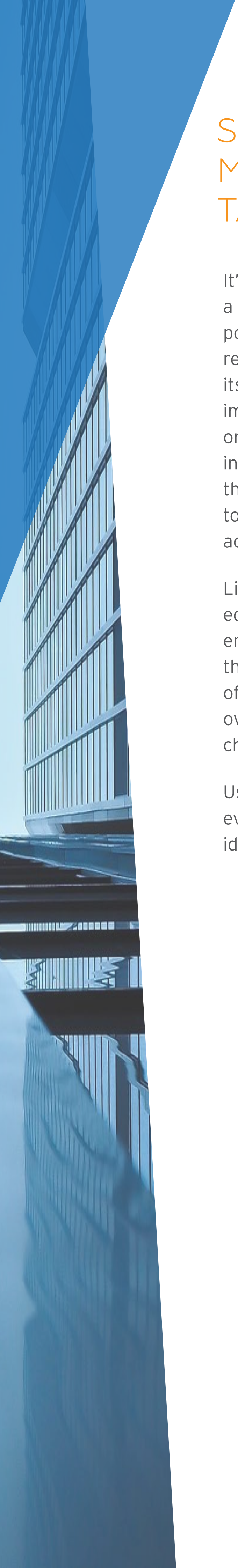
AUDIT AND ACCOUNTABILITY

The concept of audit and accountability refers to the business-wide ownership of your information management program. Audit requirements should be defined, communicated, measured, reported and resolved company-wide. This will ease the burden of responding to other external audits or regulatory assessments and allow for remediation actions before things get too far off track.

The best way to do this is to have defined roles and responsibilities for executive, management and coordinator levels of the program. Put oversight responsibilities in the hands of a steering committee that includes a Compliance Officer and risk-management stakeholders from Legal, IT, Finance and other important departments. A Records Manager should be designated to administer the program and create liaisons between the organisational program and end users.

NOW WHERE DO YOU STAND?

Now that you understand the five key information management best practice areas, it's time to see how you stack up. Follow these five steps to assess your information management program against each best practice, and learn what you can do to make it more compliant.



STEP 1:
MAKE YOUR POLICIES AND PROCEDURES TAKE HOLD

It's likely that your company has developed a basic set of information management policies and procedures, and is currently relying on these guidelines to support its compliance efforts. But if they are implemented in specific pockets of the organisation, address only some types of information or lack senior-level support, then you will find it particularly challenging to ensure they are followed and enforced across the business.

Likewise, understaffed training and educational resources mean that your employees will struggle to understand how the actions they take with a specific piece of information will affect the organisation's overall risk profile, which only increases the chances for fines and penalties.

Use this self-assessment checklist to evaluate your policies and procedures, and identify key areas for improvement.

SELF-ASSESSMENT CHECKLIST	
Policies and procedures for information management compliance are well documented.	
Policies and procedures address hardcopy and electronic formats and include vital records.	
Policies and procedures include information that is "born digital," including electronic documents, spreadsheets, emails and social media content.	
Compliance policies and procedures are part of senior management's strategic planning.	
Specific individuals, or a group of people, are accountable for consistent compliance with policies and procedures – and regularly review compliance.	
Training on compliance policies and procedures is required and ongoing for both new and existing employees.	
Policies and procedures are easily accessible by employees via the company Intranet.	
Destruction hold policies are documented and include automatic notification and verification.	

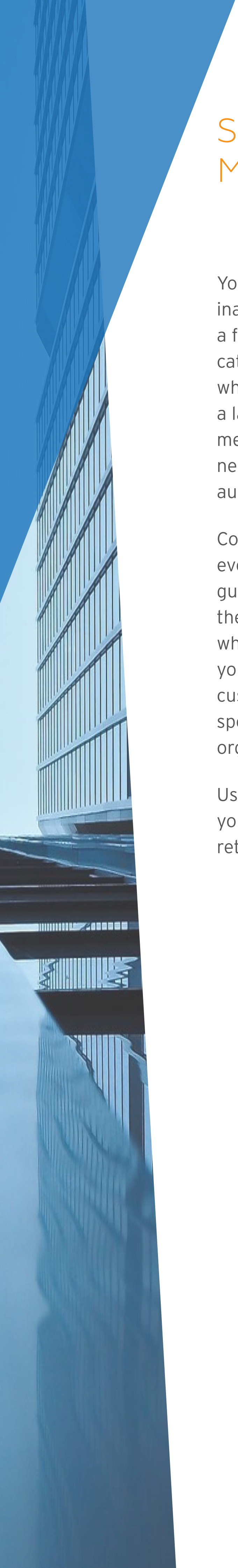
STEP 2:
KNOW WHAT STAYS AND WHAT GOES

Even if you have a retention schedule in place, making sure it's followed by all personnel, in all departments and locations is no easy task – especially when there is no single authority enforcing these rules across the organisation. When this happens, you may find yourself subjected to the penalties associated with being unable to produce the records needed during audits.

If your retention guidelines aren't applied to all types of electronic records – including collaboration technologies and social media content, both of which are the subject of emerging regulations – you'll be increasing the chances that sensitive information could fall into the wrong hands.

Fill in this checklist to understand the strengths and weaknesses of your retention guidelines.

SELF-ASSESSMENT CHECKLIST	
Our retention schedule cites the specific laws and regulations to which it's tied.	
The retention schedule undergoes regular legal review, providing risk-related guidance.	
We update it every 12 to 18 months.	
Retention policies and practices are implemented and acted upon the same everywhere we do business.	
The retention policy covers both hardcopy and electronic information.	
IT works closely with records managers to ensure all information formats are covered.	
The retention schedule makes it clear which rules apply to which classes of information – in a way that is easy to understand and apply.	
The retention schedule is available on the company Intranet or collaborative site, in an easy to browse, searchable format.	
Our retention policy outlines a clear process for examining inactive information for disposition or storage.	



STEP 3:
MAKE SURE YOU CAN FIND WHAT YOU NEED

You have a growing volume of active and inactive records, however, most likely, only a few people capable of properly filing, cataloguing and locating them for retrieval when needed. And even if this isn't the case, a lack of a systematic indexing methodology means you'll struggle to locate what's needed to prove compliance or answer an audit within the required timeframe.

Complicating matters is the fact that almost every regulatory mandate or discovery guideline includes clear instructions about the integrity of information – who handled it when, and what, if anything was done to it. If you're unable to maintain a strong chain-of-custody as you locate, access and transport specific records, you'll be opening up your organisation to various compliance risks.

Use this checklist to evaluate how well you're currently able to index, classify, retrieve and protect your information.

SELF-ASSESSMENT CHECKLIST	
We have a common index and metadata approach for both paper and electronic information, whether active or inactive.	
We use the same classification scheme (and keep it updated) in all of our locations.	
We can find information using technology rather than manual methods.	
We can locate hardcopy information and backup tapes stored offsite using an online portal.	
We have a repeatable process for imaging paper documents to make them litigation ready.	
We can easily send our indexed, imaged documents into our ECM system.	
We have a process for easily and successfully retrieving data residing on tape.	
No matter what the format, we have strong security and chain-of-custody control for accessing and delivering our information.	

STEP 4:
KEEP IT SAFE AND DESTROY IT WHEN YOU'RE DONE

It's clear that protecting sensitive information is essential to the well-being of your company and its employees and customers. But these efforts can easily be undone – with disastrous consequences – when your disposal policies are poorly defined and improperly communicated and enforced across the business.

And as the industry, government regulations governing disposal rapidly evolve to reflect new requirements and incorporate additional types of information, any deficiencies in your current processes will be amplified as you work to adopt the latest rules.

This self-assessment checklist will help you examine your existing information disposal practices, and identify key gaps and exposure points.

SELF-ASSESSMENT CHECKLIST	
We have a policy and program, set at the corporate level, which covers the secure destruction of sensitive information.	
We ensure that our employees acknowledge these policies and the associated consequences.	
We monitor and measure our consistency in following the policy company-wide.	
Our policies clearly reflect the requirements of both industry and national privacy and disposal regulations.	
We have implemented policies that address mandated requirements for the handling of private information.	
We monitor and audit our destruction program.	
When a hardcopy record reaches the end of its life, per our retention policy, it is shredded with authorised approval.	
We are not storing information past the end of its life.	

STEP 5:
ESTABLISH CLEAR OVERSIGHT RESPONSIBILITY

Recognising the importance of maintaining compliance is easy. But the same can't be said for identifying the individuals responsible for program oversight, and carving out the time to routinely audit your information management practices.

And without clear accountability at all levels of your program, it can be tough to enforce your policies and procedures, ensure records are retained for the proper amount of time, monitor security protocols and align destruction efforts with retention guidelines. Plus, you'll also struggle to demonstrate your commitment to protecting sensitive information during audits and compliance reviews, opening your organisation up to steep fines and penalties.

Fill in this checklist to get a handle on the overall strength of your auditing processes.

SELF-ASSESSMENT CHECKLIST

We have a team staffed with members from key functional areas and business units that regularly addresses compliance concerns.	
This group develops the policies and procedures of our compliance program, and is accountable for all review and oversight.	
We can demonstrate our strong chain-of-custody over the movement of information both within and outside of the company.	
We can prove that processes are in place to protect access to sensitive information in both hardcopy and electronic formats.	
We use centralised, system-based reporting that allows us to assess information management behaviour and perform cost analyses.	
We conduct regular, company-wide audits of all policies and procedures and review the results with senior management.	
We have a process for remediating the vulnerabilities detected by audits.	

READY TO IMPROVE YOUR COMPLIANCE STANDING?

Using this manual to understand and assess how well your organisation is performing across the five best practice areas is a strong first step toward maximising the compliance of your information management program.

Now it's time to take the necessary steps to strengthen and improve upon any areas you identified while filling in each section's self-assessment checklist.

Before you invest your valuable time and resources in determining the best way to do this in-house, consider a more cost-effective, efficient and reliable alternative: outsourcing these tasks to a qualified solution provider like Iron Mountain.

1300 476 668 | IRONMTN.COM.AU
0800 732 255 | IRONMOUNTAIN.CO.NZ