NO. 1 IN A SERIES OF 6

CREATING A CULTURE OF COMPLIANCE

TAKE ACTION TO UNITE INTERNAL AND EXTERNAL COMPLIANCE

FIND OUT WHY INTERNAL AND EXTERNAL COMPLIANCE MATTER, AND WHAT YOU CAN DO TO PROTECT YOUR BUSINESS FROM FINES AND REPUTATIONAL DAMAGE.

How we consume, share and protect information has changed forever. As a result, information risks are at an all-time high. Today, some businesses are struggling to manage, store and dispose of information and data without compromising on compliance.

Get compliance wrong and costs can quickly run into thousands through fines, sanctions and negative headlines. Goodwill and reputation vanish overnight. Problems escalate into job losses.

But you can prevent this by helping your business understand and follow clear policies, processes and protocols to reduce risks when handling sensitive, private or business-critical information.

TWO SIDES OF COMPLIANCE

Thinking about compliance as two sides of the same coin – external and internal – can help you focus on priorities. Internally, your goals are to monitor and enforce policies on information management, privacy and security. Externally, it's about meeting the growing expectations of regulatory bodies, other authorities, shareholders, citizens and customers.

External compliance relies heavily on robust internal processes. These include information governance, inventory, retention, disposition, privacy and security, vendor management and training. See our records and information management (RIM) self-assessment framework – a useful tool to score and benchmark your all-around compliance performance.

3 MINUTE READ

3 min

COUNTER YOUR COMPLIANCE CHALLENGES

As regulations change, it's a constant challenge to strengthen compliance and safeguard information. Key opportunities and areas for improvement are listed below.

1. **Train your people**
   This is your first line of defence. Investment here can pay for itself many times over. If your teams and senior leaders understand the basics of information security, you'll reduce your overall risk profile. Measure the effectiveness of your training.

   53% say they have left business-sensitive information on their desks.*

2. **Know what you've got**
   Controlling your information inventory (what you have, where it's stored and in which media) can save resources, time and money.

   21% indicate they have no centrally managed filing system. Departments decide for themselves how and where to store information.*

3. **Only store what you need**
   Dispose of records and information – as well as data and IT assets, such as old computers and hard drives – in the right way at the right time. Compliance is responsible and cost effective.

   30% admit they know how long their companies are legally entitled to retain contracts and legal forms, but have kept them in their files or computers beyond the retention date.*

4. **Build teamwork**
   Compliance is everyone's responsibility and the effort needs to be shared, so find knowledge gaps and weak links and give teams the clarity they need.

5. **Know what success looks like**
   Set goals across your business and measure progress against your key performance and risk indicators.

WHAT NEXT?

Find out more about the challenges and benefits of managing information risk by reading the PwC report. Then learn how to help make information compliance a shared responsibility with Iron Mountain's RIM self-assessment framework.

*Research was undertaken for Iron Mountain by Opinion Matters. It questioned a total of 4,006 workers in mid-market companies (250-3,000 employees - 250-5,000 in North America) across the UK, France, Germany, The Netherlands, Belgium, Spain and North America.

www.ironmountain.co.uk

IRON MOUNTAIN®