CREATING A CULTURE OF COMPLIANCE

COMPLIANCE LOGISTICS

DISCOVER WHY IT'S SO IMPORTANT TO MEASURE INFORMATION COMPLIANCE, WHAT THE MOST SUCCESSFUL SELF-ASSESSMENT PROGRAMMES HAVE IN COMMON – AND HOW YOU CAN USE THEM TO UNDERSTAND YOUR COMPLIANCE RISK.

THINK COMPLIANCE, THINK METRICS

Why measure information compliance? The answer seems obvious, but research suggests only 15% of organisations actually bother to do so. You might have comprehensive, up-to-date records and information management (RIM) policies, but if you don't adhere to them they may as well not exist. You could follow the highest standards of information compliance, but without documentation and assessment then you can't hope to satisfy regulators.

THE LOGISTICS OF MEASUREMENT

There are many ways to measure information compliance – there's no 'one size fits all'. However, all methods have the same goal: to gather evidence that employees understand their obligation to protect and maintain information.

Self-assessment delegates measurement to business units to ascertain how closely they follow policies, standards and controls, with each team scoring its performance against a Risk and Control Self-Assessment (RCSA). Together, these RCSAs document, assess and quantify risks across the entire organisation.

3 MINUTE READ

The most successful self-assessment programmes do these three things well:

1. **Make the process consistent**
   Once you have agreed RCSAs with each business unit and stakeholder, the focus is consistency. This can be achieved by clearly communicating the purpose of RCSAs, the steps for completing self-assessments and guidance on how to score them.

2. **Test before rollout**
   Use 'guinea pig' business units to iron out process issues before rolling out self-assessments across your organisation.

3. **Stagger the effort**
   Spread self-assessment activities across the year. Peak times will vary for different business units, so stagger self-assessment to ensure that they can devote the appropriate time and resources.

Our RIM Risk Guide white paper gives you a thorough grounding in using self-assessment to understand your compliance risk.

STAFFING

People are the first line of defence where compliance is concerned. Do you have the staff to maintain your RIM programme's aims? Do you have departmental champions in senior management helping to instil a culture of self-assessment?

Use a sliding scale to determine whether your human resources are sufficient to uphold compliance. Rate your organisation from one to four, where one is *we have sufficient, fully-trained staff and are supported by senior leadership* and two is *we have no RIM support staff*.

TRAINING

All the staff in the world can't ensure compliance if they aren't properly trained. Your people should be trained regularly, and training monitored to ensure everyone is well-positioned to maintain compliance.

You can use a staggered approach to measure the effectiveness (or otherwise) of your training processes. A score of one would mean all employees have successfully completed training courses, and we have evidence to support the fact. A score of four would mean no training occurs.

NEARLY 10% DON'T HAVE – OR DON'T KNOW IF THEY HAVE – TRAINING ON DATA PROTECTION AND COMPLIANCE REGULATIONS.*

WHAT NEXT?

Download our RIM Risk Guide white paper and read the Practical Guide to Information Governance to learn more about the role of logistics in maintaining compliance.

* 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.