KPMG Cyber

The challenge of governing your information

A new, coordinated, and practical approach to introducing information governance

September 2016

kpmg.com/us/cyber

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

Contents

It's about people 2

The need for a common agenda 3

KPMG's DC² approach 4

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

It's about people

The Chief Information Security Officer (CISO) is the protector and guardian of your organization's information assets. This responsibility is becoming more and more difficult, given the explosive growth of information, the rapid pace of transformation impacting information technology (IT) and business, and the proliferation of information across contractors and trusted third parties.

Given recent, well-publicized cybersecurity incidents affecting companies and their private and confidential information, CISOs across all industries are now receiving scrutiny from their management teams regarding how best to manage and protect information. **This is both a blessing and a curse**. A blessing because budgets are now being made available and organizations are quickly embracing change. A curse because cybersecurity is proving to be bad business where CISOs struggle to demonstrate a return on their investment. **Although organizations spend more and more money on cybersecurity initiatives, greater volumes of information continue to be compromised or lost**.

The Chief Legal Officer (CLO) or General Counsel also plays an important role related to the protection of an organization's information assets. CLOs and General Counsel must address an ever-increasing and demanding set of regulatory requirements impacting information across its life cycle (i.e., creation to destruction). Many CLOs own records and information management processes and controls, which may cause people to think of old filing cabinets and boxes at off-site facilities. **This could not be further from the truth, given the importance and value of records and unstructured information today**.

Both the CISO and the CLO have responsibility over various information-related processes and controls, which may include managing and sustaining confidentiality, integrity, availability, and privacy of information. Typically, the CLO has primary responsibility for policies that govern the management, retention, and privacy of an organization's information. **Organizations often neglect these retention and privacy responsibilities as they redirect their focus to more pressing legal matters**. Typically, the CISO has primary responsibility for introducing and managing processes and controls related to the confidentiality, integrity, and availability of an organization's information. **At other times, organizations relegate these responsibilities across various roles and, instead, focus on firefighting and escalation**.

Organizations must address how best to allocate scarce resources to protect and govern information. This question encapsulates the evolving dilemma of information governance. How should an organization protect and govern its information assets when the rate of data growth is estimated to be nearly 50 percent year over year? These growth rates present tremendous cost pressures. While the cost of information storage has proven to decrease over time, the cost of incident, fraud, and escalation management continues to increase at exponential rates, with no end in sight.

KPMG

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

The need for a common agenda

Information governance is about improving information economics. This means successful organizations help their employees, trusted third parties, and customers extract and realize value from the proper use of information. This requires that organizations identify and protect at-risk information while reducing the total cost of information ownership.

In general, the CISO and the CLO are not acting in concert to protect and govern their organization's information assets. Their respective agendas, budgets, and reporting standards are separate and, quite often, unaligned. It is now an imperative that these two functions work together to devise, implement, and sustain a strong information governance capability in their organization.

The information governance capability includes many different functions and activities that organizations perform every day, including data classification, records management, data privacy, IT security, legal, compliance, risk management, electronic discovery, defensible disposition, data quality, and information life cycle management. What organizations tend to neglect is coordinating and managing these many different functions and activities under one point of view and control, i.e., information governance.

There is no way to govern every information asset. Organizations need to make tough decisions about how best to allocate scarce resources and introduce effective governance of their information assets. **KPMG member firms' approach outlines a practical and effective means to introduce information governance**.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

KPMG's DC² approach

One critical point for all parties to agree on before introducing information governance is:

Controls ≠ Governance

The first mistake that many organizations make when trying to establish an information governance program is to equate controls with governance. This point of view results in repetitive control assessments and exhaustive controls portfolio updates.

While controls are important, organizations should start from the position that:

Culture = Governance

You must work across your environment and your stakeholder community to understand your business, IT, risk, legal, and compliance cultures before you can introduce information governance. There are two ways to think about culture as it relates to information governance.

I. **Evaluate whether or not your organization has the right foundational elements in place that define expected behaviors, processes, and controls to help govern all information assets belonging to all business processes.** These foundational elements help govern information assets via the use of harmonized policies, procedures, training, and communications.

The following list summarizes typical foundational elements employed by organizations:

- Policy and Procedure Framework
- Controls Portfolio
- Enterprise Risk Management
- IT Architecture
- IT Operations
- Governance, Risk, and Compliance
- Records Management
- Records Retention Schedules
- Data Classification
- Information Life Cycle Management
- eDiscovery
- Investigation and Incident Response
- Third-Party Risk Management
- Change Management
- Corporate Communications
- Corporate Affairs
- Legal
- Data Quality
- Master Data Management
- Intellectual Property
- Data Privacy
- Business Intelligence

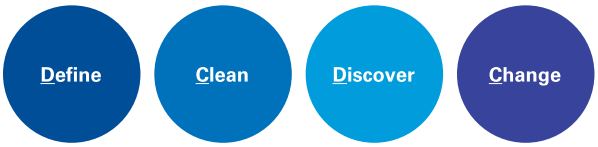
Many organizations are content with allowing these foundational elements to (loosely) work together, with the hopes that information will be governed (fingers crossed!). **This is not an effective approach to information governance**. Organizations must operationalize and embed information governance into their culture by identifying which information assets deliver the most value and present the most risk to the organization. This starts with prioritizing the process portfolio.

II. **Prioritize business processes** that deliver the most value and present the most risk to the organization. The related information—structured, unstructured, and physical—are the exact assets that need to be governed.

KPMG

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

A simple way to introduce the two considerations summarized in points I and II is to follow KPMG's DC² approach. This approach includes the following key actions:



Each of these actions requires the following activities and outcomes:

Define: What does good look like?

— Educate business and IT partners, secure buy-in, and agree on how to value and risk/rank business processes (think of the 95/5 rule when prioritizing business processes)

— Review existing policies, procedures, standards, minimum security baselines, tools, schedules, and function level responsibilities related to information governance (i.e., foundational elements)

— Identify legal, regulatory, compliance, contractual, and commercial requirements (i.e., external factors)

— Identify third parties involved with business processes, IT, information, storage, and records management

— Identify ongoing and planned changes that may impact information governance; this should include an evaluation of external factors (e.g., regulatory changes)

Clean: Eliminate immediate risk exposures.

— Perform a gap assessment of processes and controls governing prioritized business processes and related information assets, with a focus on:

  – Behavior-based items, including policy, training, schedules, incident management, etc.

  – Access control items, including privileged access, identity management, etc.

  – Management responsibilities, including information oversight, identification, retention, protection, disposition, and destruction

— Remediate critical process and control issues impacting information assets

— Develop and document a remediation plan for impacted or nonexistent foundational elements

— Develop and document a remediation plan for information assets that aligns to your business and IT target state

Discover: You cannot govern what you do not know.

— Leverage automated tools and manual inspection efforts to identify information assets belonging to prioritized business processes

— Conduct information use surveys to better understand end-user and trusted third-party behaviors impacting information assets

— Work with trusted third parties to identify information assets used, accessed, processed, managed, archived, etc., on behalf of your organization

— Update the gap assessment (see the Clean stage) based on newly identified information assets and results of use surveys

— Update remediation plans, as needed

Change: Embed governance into the culture.

— Implement mid- and long-term change and remediation plans related to foundational element gaps and deficiencies

— Implement mid- and long-term change and remediation plans related to business and IT process and control gaps and deficiencies

— Manage information-related changes that impact or are required of third parties

— Introduce automated capabilities to better manage and govern information assets

— Update business and IT management reporting to track and sustain the information governance program

Organizations can benefit from information governance. **Improved information economics directly and positively impacts your customers, employees, and trusted third parties.**

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459

Contact us

David Remick
Partner, Cyber
T: 404-769-1096
E: jremick@kpmg.com

Steve Stein
Principal, Forensic Technology
T: 312-952-3110
E: ssstein@kpmg.com

Call our 24/7 Cyber hotline at **855-444-0087**.

kpmg.com/us/cyber

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the specific circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 562459