

# Managing Information Risk in the Extended Enterprise



## Managing Information Risk in the Extended Enterprise: Why Corporate Compliance and IT Security Must Join Forces

### BUSINESS BOMBARDED BY RISK TO DOCUMENT SHARING AND COLLABORATION

The early stages of a paradigm shift can introduce a period of ignorance that quickly moves to fear, uncertainty, and doubt. Organizations find comfort in the old way of doing things, but must move forward and begin to leverage new approaches to stay competitive.

Seamless collaboration with electronic documents is one of those business practices that may completely revolutionize how technology creates value for companies. Thanks to a wealth of new tools, document collaboration has become much easier and more accessible to business users. This makes employees more productive and gives companies agility that helps them succeed in a complex, dynamic, and distributed business environment.

However, new methods of collaborating using online or other electronic means introduce serious risks. Documents shared outside the enterprise aren't protected by perimeter security, enterprise rights management and other infrastructure measures. These new approaches require organizations to extend security beyond the firewall.

How does business take advantage of the wealth of benefits that online document collaboration promises, while avoiding the compromise

of confidentiality, integrity, and availability of critical business information?

With an onslaught of regulations impacting security, this concern has continued to grow.



The good news: Organizations can provide employees with a secure online document collaboration environment. It's time to stop fighting collaborative processes that end-users have so avidly embraced, and objectively look at securing online document collaboration across extended business relationships, to take full advantage of its benefits.

### Legions of compliance obligations and risks to information

The information within electronic documents faces a bombardment of risk and compliance challenges from every direction. IT security has been in reactive mode, tightening down access using enterprise rights management, perimeter security, laptop encryption, but has not addressed the issue of how information is used outside the enterprise. Meanwhile, business users are sharing documents completely unprotected, often using online collaboration platforms, because it makes them more productive.



The onslaught of risk and compliance issues related to information sharing includes:

- **Intellectual property and trade secrets:** Technology licensing and collaboration can put intellectual property at risk through intentional or inadvertent exposure. Biopharmaceutical outlicensing, in which potential bidders review product dossiers, is a good example of this.
- **Sensitive customer information and data:** Communication with vendors, external auditors and customers need to be secured, not only to protect confidential customer information, but also to fulfill the company's contractual and service-level obligations to the customers.



- **Collaborations on strategy:** Work with management consultants, board members and investors requires sharing information on business strategy, execution, and partnerships. In fact, the more sensitive a document is, the more likely it will need to travel outside the enterprise, increasing the risk of exposure.

- **Personal information:** The onslaught of privacy laws mandating security, encryption, authentication and audit trails impacts documents shared with HR administrators, insurance and payroll providers, 401(k) administrators, and others. Additionally, privacy requirements continue to multiply, and require disclosure should this information be compromised.

- **Legal and compliance issues:** A variety of electronic discovery and litigation risks bear down on processes. These require organizations to have complete control and visibility into electronic document information, and to know who has accessed them. Legal, financial and contract-related documents all require documentation of accesses, non-repudiation, and control over document integrity.

- **Information getting in the wrong hands:** There is the general fear that encompasses all of these points of information getting into the wrong hands — this can be through inadvertent or accidental exposure or malicious behavior, all because the organization lacked the proper security

controls. Any employee with access to sensitive documents can put them at risk by sending email attachments, using unsecured online collaboration tools, or through offline communication such as shipping documents on CDs, USB drives or even as hard copies.

### **The distributed nature of documents compound risk**

Risk and compliance issues are compounded by the pervasive nature of electronic documents. Individuals and departments can quickly set up online collaboration portals and share documents inside and outside the organization, increasing the number of people who can misuse them and simultaneously decreasing the company's control over them.

End users have become accustomed to online applications through consumer tools such as social networks and file-sharing platforms. Based on their favorable experiences with consumer tools, employees are quite comfortable acquiring and using online applications in business settings. This consumerization of the enterprise has led end users to purchase collaboration applications at the departmental level, which creates silos of electronic documents, increases risk, and makes compliance unmanageable. Users can also easily purchase and share online collaboration spaces without the organization knowing, often without the document controls that security and compliance professionals require. The prolific propagation of multiple collaboration



platforms further compounds the problem — particularly when they are externally hosted, without much thought given to security or document discovery across the enterprise.

The danger is that well-meaning empowered users — through the likes of online collaboration tools — do not understand and monitor risk to document sharing. Security is an afterthought as users try to get their jobs done.

### Information risk moves across business relationships

Risk and exposure of online document collaboration grows with the dynamic and extended nature of business.

Business is dynamic — employees join or leave the organization or change roles, and documents grow and take on more and more information, increasing risk exposure. As technology changes, what was perhaps a secure portal for document collaboration is no longer secure because patches are not applied, the system is insecurely configured or it simply is no longer adequate for the company's needs.

This problem increases exponentially as document access is given across extended business relationships. The organization is not as static as the traditional brick-and-mortar companies of 30 years ago. Business is distributed, and extends across dozens to thousands of business relationships with partners, supply chains, service providers, contractors, consultants, outsourcers, and even temporary workers. All of

these relationships have collaboration needs within the organization. Access given to documents extends across networks and the Internet, increasing risk exposure.

The traditional infrastructure approach to security (firewalls, enterprise rights management, network access control, and endpoint security) can't protect collaboration in a dynamic and extended business environment. And if an organization closely restricts and monitors online collaboration without providing a secure alternative, users are forced to send documents as email attachments — completely unprotected.



### CRITICAL FACTORS IN MANAGING RISK TO DOCUMENT COLLABORATION

Fortunately, all is not doom and gloom. The demands of business to collaborate and share unstructured information will continue to grow. It is time for companies to stop resisting this change in business processes, face the fact that end users must share information in ways

that aren't protected by the current corporate infrastructure, and think outside the box to extend security to online collaboration. In most cases, this means using secure online workspaces that provide the collaboration features end-users demand, within a secure environment that transparently enforces security and compliance policies.

Critical factors to consider when managing risks to online document collaboration include:

- Balancing accessibility and security:** The job of information security is to provide the right access to the right individuals to the right information when they need it. Information must be both secure and accessible. This requires a balanced view of secure access that is an enabler and not a disabler.
- Classification of documents:** A cornerstone of providing appropriate security to a document is understanding what is in the document, and defining the proper controls in line with the risk the information warrants. This involves categorizing documents and information to define security controls and policies based on the level of risk exposure to the organization.
- Confidentiality of documents:** Critical to many documents shared across the extended enterprise is the need to protect documents and the information they contain from improper disclosure to unauthorized parties. This requires strong authentication and access controls to ensure that only the right people can see the information.



Some documents may require additional controls to prevent forwarding, saving or printing, even by users legitimately authorized to access them.

- **Integrity of information within documents:** Another level of security is concerned with the integrity of the information in the documents. While many may have legitimate access needs to see and review documents, not everyone needs the ability to change it. Security professionals must enforce and monitor access controls to ensure that only the right people can make changes to the information.

- **Auditability, to understand who did what to documents:** Providing accessibility while protecting confidentiality and integrity of electronic documents requires that there also be a robust audit trail to understand who did what to a document and when. Organizations need the ability to track what happened to a document as well as the information contained within it.

- **Understanding different roles:** End users with different roles must be empowered with appropriate levels of access. Individuals must be able to collaborate with others inside and outside the organization, while adhering to centrally-defined security policies to make sure they do not step out of bounds and expose the organization. This involves security and compliance establishing an ongoing ability to monitor risk exposure and mitigate risk to acceptable levels, while allowing

users to work with documents in online document collaboration portals.

#### PROVIDING SECURITY FOR ONLINE DOCUMENT COLLABORATION IN THE EXTENDED ENTERPRISE

Corporate compliance and IT security departments, working in tandem, have the responsibility to provide a clear strategy for secure online collaboration through document compliance management. This strategy is articulated within security policies enforced across the business, and protects the information stored and accessed electronically in a dynamic and extended business environment.

These policies:

- Provide information classification based on risk exposure to the organization.
- Define minimum security and access controls based on risk classification.
- Communicate responsibilities for implementation of secure online collaboration workspaces.
- Identify how risk to document collaboration will be managed and monitored on a continuous basis.

This requires changing the security culture in the organization from an end-point or network infrastructure-centric view to an information-centric view of security. This includes a new paradigm of managing security across the entire document lifecycle — even when they are outside the firewall.

The next step is for compliance and IT security to join forces to deliver a secure online collaboration platform. The goal is to empower end-users with a transparently secure online collaboration platform that integrates and supports the document and collaboration security policies.



The right secure online collaboration platform will provide:

- **Security certification:** The vendor should have a robust security architecture and infrastructure and make sure it is independently tested and evaluated.
- **Enterprise integration:** The vendor should easily integrate with the organization's own security infrastructure, enterprise applications and business



processes for authentication and access controls.

- **Choice of delivery model:** The vendor should be able to provide either a cloud or on-premise application according to the organization's requirements and offer a clear migration path between the new and old models.
- **Service level agreement:** If delivered in the cloud, the vendor should have clearly defined and committed service-level agreements for security as well as accessibility.
- **Flexibility for a variety of needs:** The online document collaboration platform should provide flexibility in an online workspace that allows for the right level of secure collaboration relevant to the risk exposure within the documents.

**The Bottom Line:** The CCO and CISO cannot be naysayers. They must analyze the company's business processes, and unleash the potential of collaboration across the business and its relationships, while minimizing information risk.

#### ABOUT CORPORATE INTEGRITY

Corporate Integrity, LLC is a GRC strategy advisory firm providing leadership in education, research, analysis, and advisory services by monitoring the challenges and trends of the business roles accountable for corporate governance, enterprise risk management, and compliance (GRC). These roles include executives responsible for risk, compliance, ethics, corporate social responsibility, sustainability, corporate governance, legal, IT, and audit.

Through ongoing research, interactions, and analytics Corporate Integrity is the authority in understanding how organizations can foster a culture that "walks the talk" - where integrity is central to governance, risk, and compliance (GRC) practices. Corporate Integrity educates organizations - and GRC professionals within those organizations - on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices so they maintain a position of integrity aligned with corporate values and business performance.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology vendors and professional service firms to align their

sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC. Corporate Integrity helps technology and professional service firms with go-to-market strategies that deliver results.



With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms that target the roles of GRC.

**|| THE CCO AND CISO CANNOT BE NAYSAYERS. THEY MUST ANALYZE THE COMPANY'S BUSINESS PROCESSES, AND UNLEASH THE POTENTIAL OF COLLABORATION ACROSS THE BUSINESS AND ITS RELATIONSHIPS, WHILE MINIMIZING INFORMATION RISK."**



### About Michael Rasmussen

J.D., CCEP, OCEG Fellow: Risk & Compliance Lecturer, Writer, & Advisor

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC) processes. He is a sought-after keynote speaker, author, and advisor on risk and compliance issues around the world and is noted for being the first analyst to define and model the GRC market for professional services and technology.

With more than 15 years of experience, Michael's objective is to assist organizations in defining GRC processes that are efficient, agile, effective, accountable, and transparent.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group ([www.OCEG.org](http://www.OCEG.org)) and chairs OCEG's Technology Council. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in "Governance and Compliance: Saving the Planet and the Corporation." Most recently, in October 2008, he was recognized as a "Rising Star in Rocky Times: Corporate America's Outstanding Executives Under the Age of 40."

During his career, Michael has worked in the market analyst, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and 'top analyst' at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael's educational experience consists of a Juris Doctorate from the Oakbrook College of Law & Government Policy and a Bachelor of Science in Business from the University of Phoenix. Michael is currently in the Master of Divinity program at Trinity Evangelical Divinity School.

### About Brainloop

Brainloop provides a highly secure online work space that helps companies mitigate information risk, meet compliance objectives and increase process efficiencies when sharing confidential documents inside and outside the enterprise. Major organizations that use it include BMW, Deloitte, Eurocopter, Fujitsu Siemens, T-Mobile, and Zurich Financial Services.

Brainloop's secure online work space acts as a virtual safe where sensitive documents reside and can be viewed and edited by authorized users, whether inside or outside the network. The application protects documents against unauthorized access, forwarding, saving or printing, and provides a tamper-proof audit trail that ensures that every activity is recorded and traceable. Automatic versioning, change notification and alerts, workflow / task management and document format conversion support collaboration and process efficiency, thus promoting user acceptance.



### CONTACT

#### Europe

Brainloop AG  
 Franziskanerstr. 14  
 81669 München · Germany  
 T: +49 (89) 444 699 0  
[info@brainloop.de](mailto:info@brainloop.de)  
[www.brainloop.de](http://www.brainloop.de)

#### USA

Brainloop Inc.  
 One Broadway, 14th floor  
 Cambridge, MA 02142 · USA  
 T: +1 (800) 517 3171  
[info@brainloop.com](mailto:info@brainloop.com)  
[www.brainloop.com](http://www.brainloop.com)