White Paper

Information Management & Governance

Reduce Compliance Risk with Three Best Practices from Those Who Did

Micro Focus® sponsored research with *Compliance Week* to measure the cost of information non-compliance. The results are striking. Despite commitment to information governance (IG) programs, many organizations lack the strategies and tools to deal with a complex and uncompromising regulatory environment. Even more surprising, many organizations are unsure of how, when, or why they've received data governance fines or sanctions.

MICRO FOCUS®

Table of Contents

page

Information governance is the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs.[1]

Quantifying Non-Compliance

Staying compliant with the influx of laws, regulations, guidelines, and specifications has become a chief compliance officer's worst nightmare. Scrutiny and sanctions for information non-compliance is not trivial. In a recent example, the New York Department of Financial Services ordered a foreign financial services company to pay a $180 million penalty and install an independent monitor for violating New York's anti-money laundering laws.[2] The message conveyed from regulators is clear: organizations and individuals that allow security breaches, privacy invasion, data leaks, and information non-compliance will face stern punishments.

But not all sanctions are headline-worthy, and smaller fines occur more than you may think. What's even more important though is that an equal number of organizations avoid information-related sanctions entirely. Understanding the procedural differences between these two segments can provide valuable insight into successful information governance strategies. In this paper, we have taken key learnings from our recent cost of non-compliance research and formulated three best practices to bolster your IG program.

How Are Organizations Coping?

It's a foregone conclusion that compliance professionals must handle more complex and uncompromising regulations than ever before. A *Compliance Week* survey validated this finding as 93% of respondents identified that their organization has experienced information governance compliance challenges.[3]

According to this survey, only about one-third of respondents say they quantify and track the costs of sanctions. Excluding organizations who couldn't share information due to sensitivity, 56% of respondents do not track or were not aware of these costs and sanctions.[4] While a variety of reasons are stated in the graph below, lacking a quantifiable understanding of the risk would make it difficult for those organizations to justify investments for improvement.

1 **www.iginitiative.com**
2 *"Mega Bank fined $180 million for AML violations," by Jaclyn Jaeger,* Compliance Week*, August 23, 2016*
3 *"2016 Cost of Information Governance Non-Compliance,"* Compliance Week*, October, 2016*
4 *Ibid*

Do you quantify and track the economic cost of fines, sanctions and other remedies related to non-compliance with information-related laws, regulations, and other requirements at your organization?

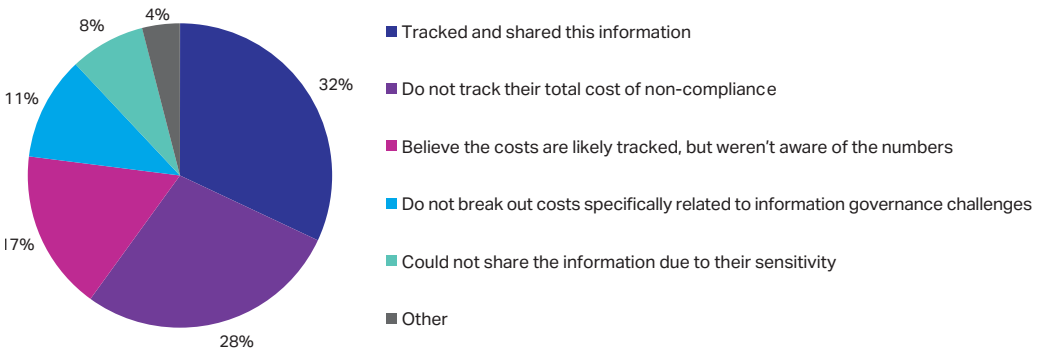

Figure 1. 2016 *Compliance Week* Survey: Qualify and Track

Among those who track the economic cost of data governance non-compliance, the average annual total cost over the past three years was $1.5 million with a median of $159,091 (average of both those fined and not-fined).Of those who suffered fines, sanctions, or remedies, the average annual total cost over the past three years was $2.4 million with a median of $375,000.[4] This average includes headline-worthy fines, which was reported as high as $25 million/year in this survey. Information-related compliance fines pose real risk to the business, and the risks will only grow due to increasingly more complex data governance regulations.

Average annual total cost over the past three years of fines, sanctions, and other remedies related to noncompliance with information-related laws, regulations, and other requirements among the 32% of organizations who tracked and shared this information.

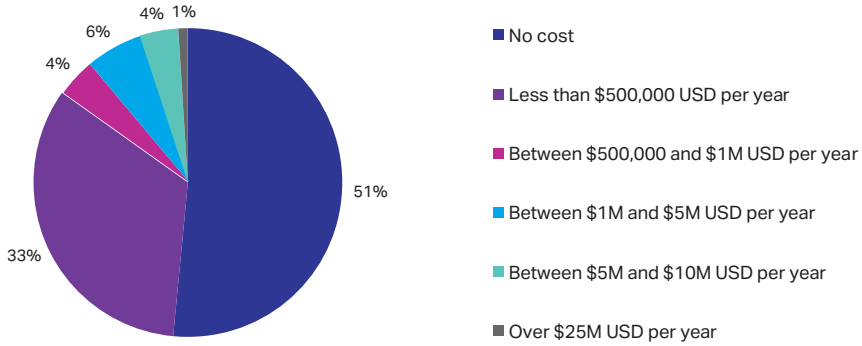

Figure 2. 2016 *Compliance Week* Survey: Average Annual Total Cost

93%
Have experienced information governance challenges

56%
Do not track or were not aware of the costs of fines and sanctions

$2.4M
Average annual total cost of those who suffered fines and sanctions

33
Average hours/month compliance spends on information governance task

Among those who track the economic cost of data governance non-compliance, the average annual total cost over the past three years was $1.5 million with a median of $159,091 (average of both those fined and not-fined).

4 *Ibid*

With the exception of one category, organizations who were fined cited far more challenges than those that were not.64% said providing a complete and comprehensive response to requests for information from courts, regulators, auditors, or other external parties was their top challenge.

Clearly, if an organization cannot consistently quantify non-compliance penalties, then finding remedial actions can be a daunting challenge for compliance professionals. Below are the differences in compliance challenges most frequently stated by those organizations who have received (or avoided) fines.

What kinds of compliance challenges related to information governance has your organization experienced?

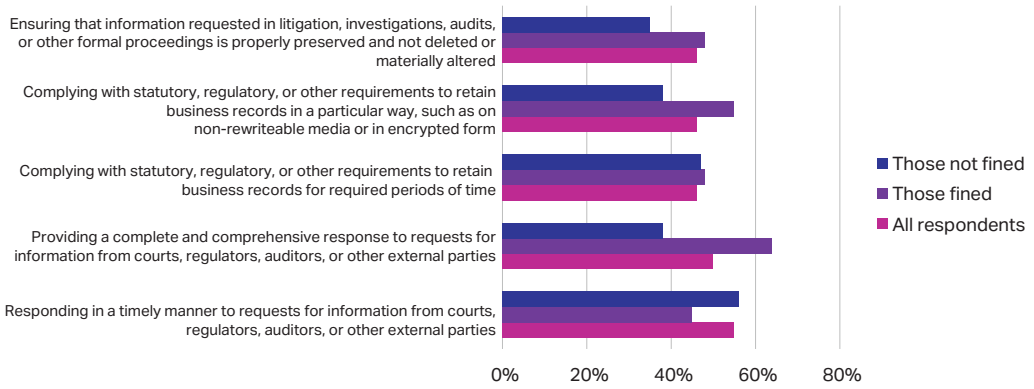

Figure 3. 2016 *Compliance Week* Survey: Differences in Compliance Challenges

With the exception of one category, organizations who were fined cited far more challenges than those that were not.64% said providing a complete and comprehensive response to requests for information from courts, regulators, auditors, or other external parties was their top challenge. It was only 38% for non-sanctioned companies. Responding in a timely manner was a frequently stated challenge for half of all respondents.

How Much Time Should You Spend on Information Governance?

If companies are having difficulty responding to regulators, then it's safe to assume that compliance staff must spend an inordinate amount of time on IG activities. On average, compliance professionals spend 33 hours per month just for information governance compliance, plus four additional hours during audit months. But, without definitive benchmarks, is 33 hours a reasonable amount of time to spend on IG compliance?

Percentage of person hours that a typical employee in compliance, legal, or related department typically devotes to information governance compliance requirements during a month with an audit or litigation event.

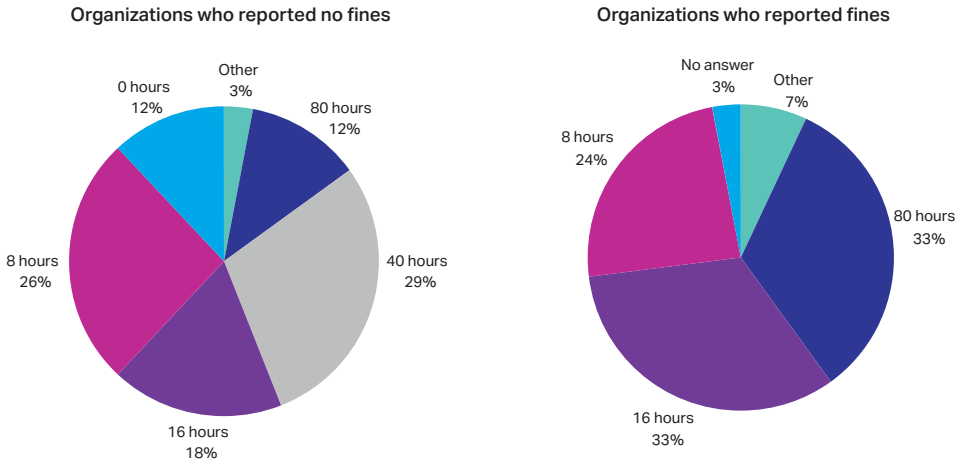

Figure 4. 2016 *Compliance Week* Survey: Time Spent on Information Governance

When comparing the differences between those who received fines versus those who did not, while non-audited months displayed little material difference, audit months showed a dramatic difference in the struggle to comply. On average, those who were fined invested about 11 more hours for audits, while those who didn't receive fines invested only 1.7 additional hours, or roughly 2.5 hours less than the average among all survey respondents. While this number may not seem significant, if you consider a difference of 2279 hours/month[5] of lost productivity across the organization for those who suffered a fine versus those who did not, it's a sizable enough variance to warrant a deeper look at the nature of information governance between the two segments.

When comparing the differences between those who received fines versus those who did not, while non-audited months displayed little material difference, audit months showed a dramatic difference in the struggle to comply.

Top 3 Best Practices among Those Organizations Who Avoided Fines and Sanctions

1. They Search and Investigate across Everything

Today, data is being produced from a seemingly endless array of human and machine-generated sources. Where in past years the flow of data seemed manageable, this is no longer the case—unstructured data from email, chat, and even voice, emanates constantly. The survey found that 74% of those not fined search and collect unstructured data from messaging systems like email, instant messaging, and SMS. For the fined group, it was 58%.

5 *The average respondent's organization in this survey was 245 full-time employees that support information governance compliance requirements as part of their role. The median number was 6.* Compliance Week *Cost of Information Governance Non Compliance 2016 survey*

Energy organizations, who were far less likely to track fines (85%), were far more likely to invest in eDiscovery software (69%).

Identify the locations that your organization typically searches, investigates, and/or collects information from in the course of investigations and other compliance activities.

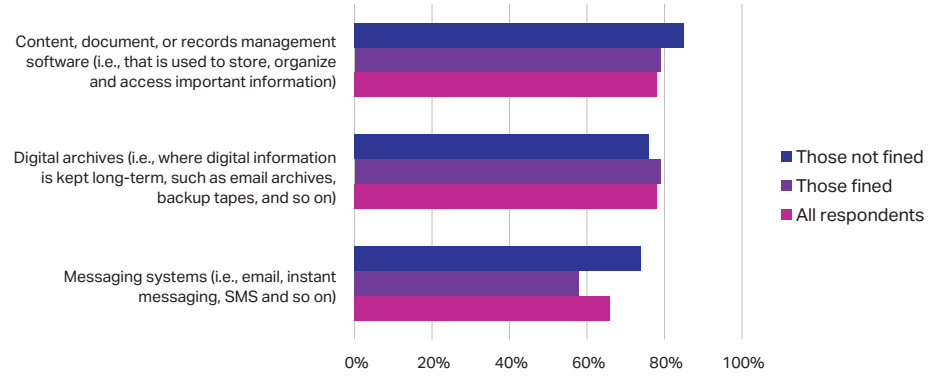

Figure 5. 2016 *Compliance Week* Survey: Compliance Activity Locations

2. They Use Search or Investigation Tools

While not a huge difference, 10% more of those not fined leveraged search and investigation tools, among others, over those fined (and 13% more than the total survey group).Search tools have been on the market for years, so it's surprising that they are not more widely embraced for investigations, particularly in light of the shear amount of structured and unstructured data that organizations must cull through for audits or legal matters. Accuracy has continued to improve as tools have advanced and expanded to search across an array of information—without bias to location or language—using contextual analysis for greater relevancy. With powerful conceptual and visualization capabilities, tools can further analyze and review data for proactive risk mitigation such as fraud detection.

Identify the methods and tools that your organization uses to support information governance compliance activities like searching, finding, collecting, preserving, reviewing, and producing digital information.

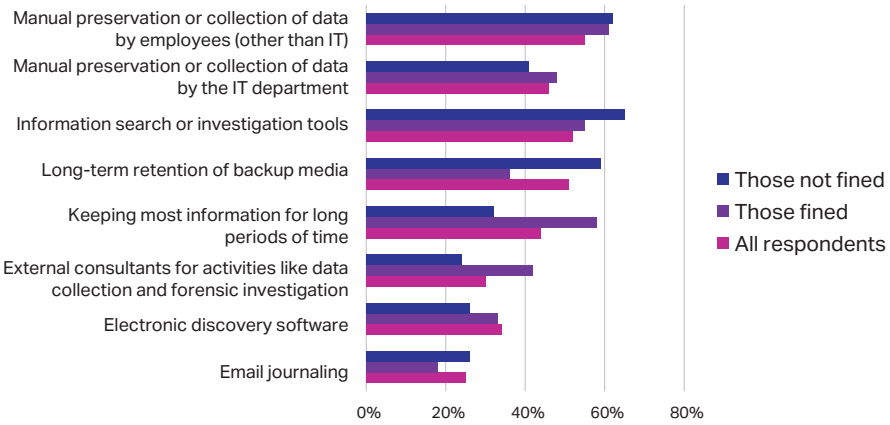

Figure 6. 2016 *Compliance Week* Survey: Digital Information Production Methods

3. They Have Reasonable Policies for Both Retention AND Defensible Deletion

In the same chart, 59% of those who'd not received fines support the long-term retention of backup media, compared to 36% of those fined. Yet only 32% keep most information for long periods of time, compared to 58% of those fined, suggesting that those not fined may have both retention and defensible deletion policies in place. Just, if not more, important are implementing and enforcing those information governance policies, since having a policy on paper only can prove worse in an investigation.

Across all groups, Government agencies were far more likely to keep data (72%) than Energy (15%).[6]

Of the many technologies available on the market today, automated policy management enables consistent and repeatable application and enforcement of policies. Policy management goes far to help your organization address the critical barriers to enterprise productivity and information governance such as large data volumes, multiple data repositories, and the twin disruptors with the cloud and mobility. An organization that gains full control of its information with centralized policy management can see improved:

- Collaboration and productivity across teams
- Ability to comply with regulations
- Preparation for legal and regulatory inquiries
- Ability to protect and secure information
- Support for data retention and defensible disposition

Top 3 Areas to Improve

1. Records and Content Management Matters…If It's Optimized for Information Governance

Content, document, or records management software was the most highly used tool (57%) among those who responded to the survey, however, complying with requirements to retain business records for required periods of time was the top rated compliance challenge (55%).This suggests that organizations may be looking for improved ECM and records management technology for their compliance purposes.

An information governance-based approach to content management helps ensure that authoritative content (such as contracts, personal information, and records) is protected, and that the information contained therein is available for evidentiary purposes and is discoverable in an easy, efficient manner. A governance-based approach can ensure that:

- The structure of the authoritative record and the relationship between the related elements of the record are maintained
- The contextual link between content (i.e., evidence of business activities) and the business process is preserved
- Authoritative content and records meet the requirements of authenticity, reliability, integrity, and usability

6. *2016 Cost of Information Governance Non-Compliance,"* Compliance Week, *September, 2016*

According to a 2015 AIIM survey, 60% of respondents feel that automation is the only way to keep up with the increasing volumes of electronic content. Similarly, 63% feel that improved search ability is the biggest benefit of automated classification.[8]

Identify the software tools that you personally use in your role.

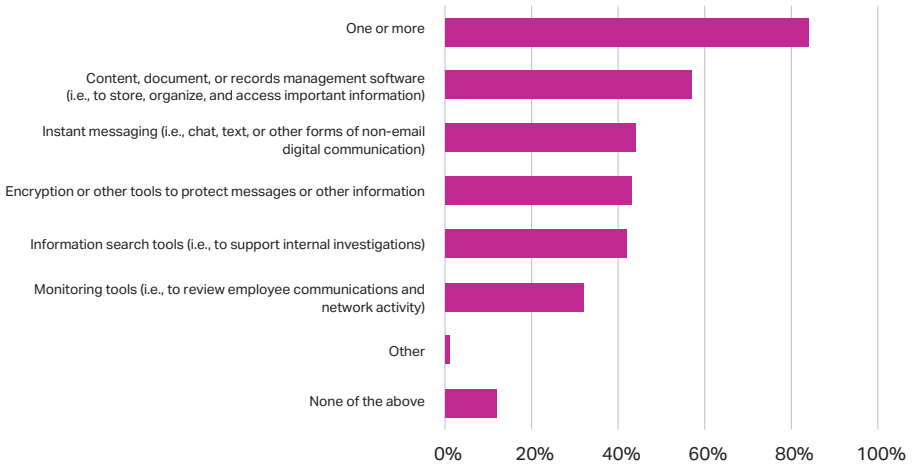

Figure 7. Software Tools Identified

2. More Automation Is Needed to Free Compliance for Strategic Tasks

Data breaches (62%) and Privacy breaches (61%)[8] were by far the most cited areas of compliance focus in the study. As cyber risk explodes and industry privacy regulations become more complex, compliance expertise is in demand. However, manual preservation or collection of data by employees (other than IT) was the highest ranked method (55%) for organizations to support information governance, and as stated earlier in this paper, a fair amount of time is being allocated to IG compliance tasks. This is where automated solutions, such as data classification, can reduce manual tasks associated with IG, and free staff to tackle more strategic tasks.

Through keyword or contextual capabilities, the time-consuming burden to classify information can be automated for retention, deletion, deduplication, backup, and privacy and access controls. Applying these policies in a transparent, consistent manner is a key to automating information governance at scale. A centralized policy layer that will help automate (what were previously) manual actions is required to organize and control data efficiently. Adopting the right technology can offer immediate impact to free up resources that are needed to drive strategic initiatives that protect the business from risk and ensure business continuity.

NUSCALE POWER LLC

NuScale Power, a designer and manufacturer of small modular reactors, needed to modernize from paper-based to electronic records system in order to pass U.S. Nuclear Regulatory Commission (NRC) inspections. Micro Focus Information Governance solutions help NuScale comply with the NRC Regulatory Issues Summaries NIS 2000-18 guidelines for managing electronic records in licensed commercial nuclear plants. Furthermore, they helped:

7 *"Information Governance: Too Important to be Left to Humans," AIIM Industry Watch, December 2, 2015*

8 *"2016 Cost of Information Governance Non-Compliance,"* Compliance Week, *October, 2016*

- Capture, record and report on records annotation rates to help identify and reduce errors in asset classification, document revisions, formatting, etc.
- Shrink record retrieval from 2—7 days to seconds.
- Streamline migration of legacy records from Microsoft SharePoint database; migrate more than 9 TB and enable rapid integration of new records, including test files of up to 500 GB.

More information about NuScale Power and their use of Micro Focus information governance solutions can be found here.

3. Clearly Delegate Leaders and Empower Compliance

As for how respondents believed they could reduce risk of fines, sanctions, and other remedies, clear delegation of leadership (73%) was the top answer. This suggests confusion in organizations as to who actually owns the problem. Leading analysts confirm that the lack of centralized ownership of information governance is a common challenge, particularly for large enterprises.[9] Often times, for lack of a clear designated sponsor, it is relegated to IT, who may, or may not be proactive in managing IG challenges and soliciting executive involvement. Chief Data Officer and Chief Information Governance Offer titles are surfacing in companies to elevate the importance of information governance and management.

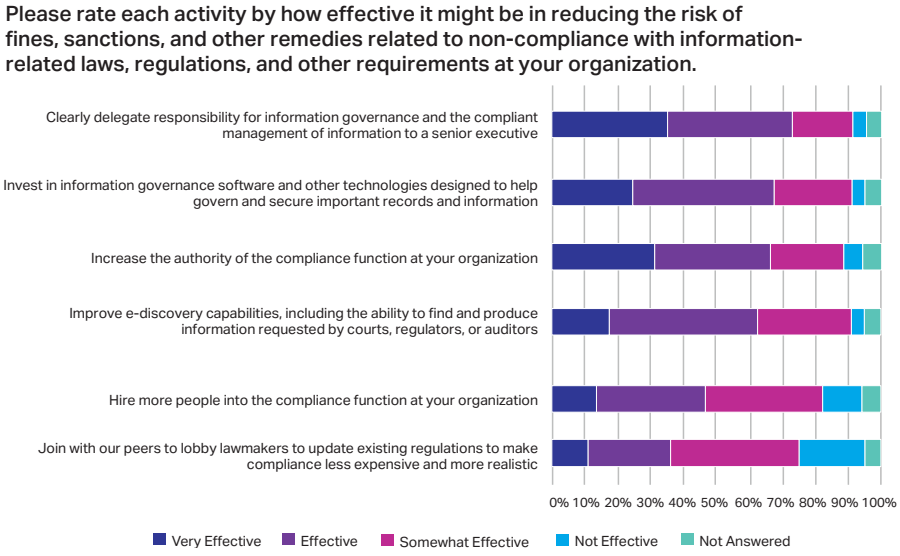

Figure 8. Activity Effectiveness Rating

9 *Accelerate Your Information Management & Governance Initiatives webcast featuring Gartner*

Information Governance Technology Reduces Risk

In examining the best practices and opportunities for information governance improvement, it's easy to see why 68% of respondents rate investing in IG software or technology as effective in reducing risk. Faced with surging amounts of structured and unstructured data and heightened penalties for information non-compliance, selecting a flexible and open technology solution is an absolute necessity. Implementing a modular and repository-agnostic framework across information management and governance applications is important to bridge formerly distinct data silos. Integrated solutions such as file analysis, data protection, archiving, records and enterprise content management (ECM), supervision and surveillance, and eDiscovery are pivotal to information governance and compliance efforts. The automation within these solutions, such as data classification, can provide huge efficiencies to save you time and money. By further incorporating native, in-place data analytics, you can navigate and understand vast volumes of data to proactively address risk.

Information Management & Governance Solutions

Micro Focus addresses the call for a contemporary approach to information governance by delivering a portfolio of modular solutions that help organizations access and understand a wide range information across a variety of sources and repositories. Our approach leverages analytical insight to understand information in its context and organizes and controls this information with a common policy layer that can be applied to all information for uniform management. This allows you to intelligently manage and take action upon information in accordance with varying organizational needs to manage risk and derive value.

Resources

- *Compliance Week* Cost of Information Governance Non-Compliance
- Accelerate Your Information Management & Governance Initiatives webcast featuring Gartner
- Learn more about GDPR and Compliance
- Find out about Micro Focus Digital Safe, a next-generation unified information management and governance solution

Learn More At
www.microfocus.com/infogov

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com

362-000010-002 | 4AA6-7977 | H | 05/18 | © 2018 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.