ESG Solution Showcase

Information Governance Considerations in the Financial Services Sector

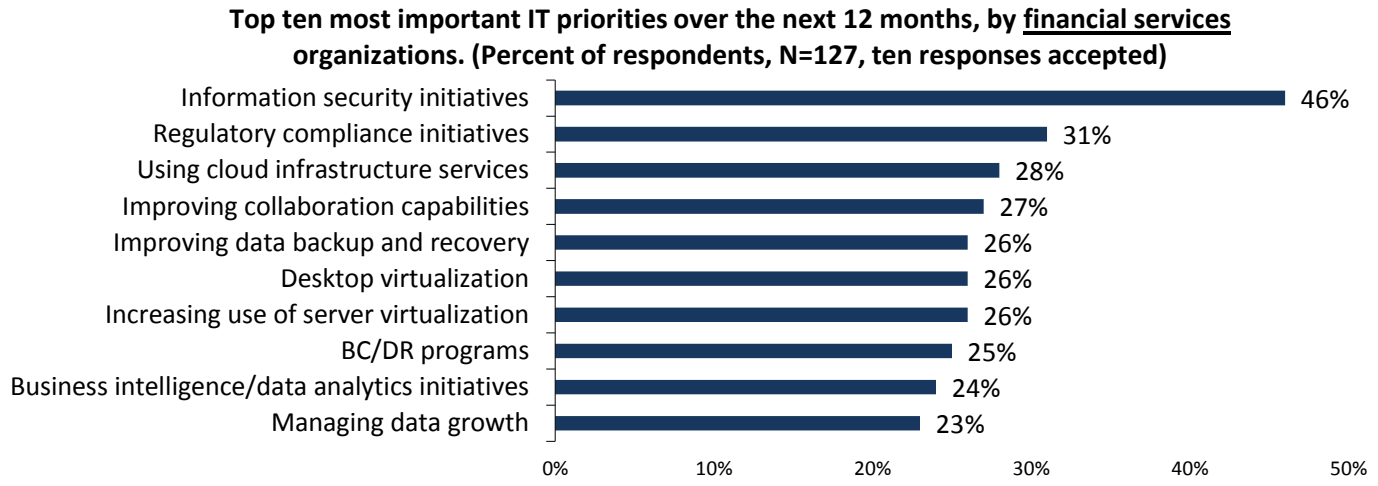
Date: June 2015 **Authors:** Jason Buffington, Senior Analyst; Dan Conde, Analyst; Monya Keane, Research Analyst

Abstract: Translating compliance and information governance concepts into actionable strategies can be challenging for financial services organizations. But it is definitely a priority. Facing the challenge involves following a phased approach encompassing communication, a degree of "cultural evolution," and of course, leveraging good technology.

Overview

For IT managers working in financial institutions, regulatory compliance is clearly a priority (see Figure 1).[1] In such a highly controlled industry, any effort tied to data protection, disaster recovery, or business continuity will be sufficient only when good information governance and compliance protocols also are in place.

FIGURE 1. Top Ten IT Priorities Among Financial Services IT Managers

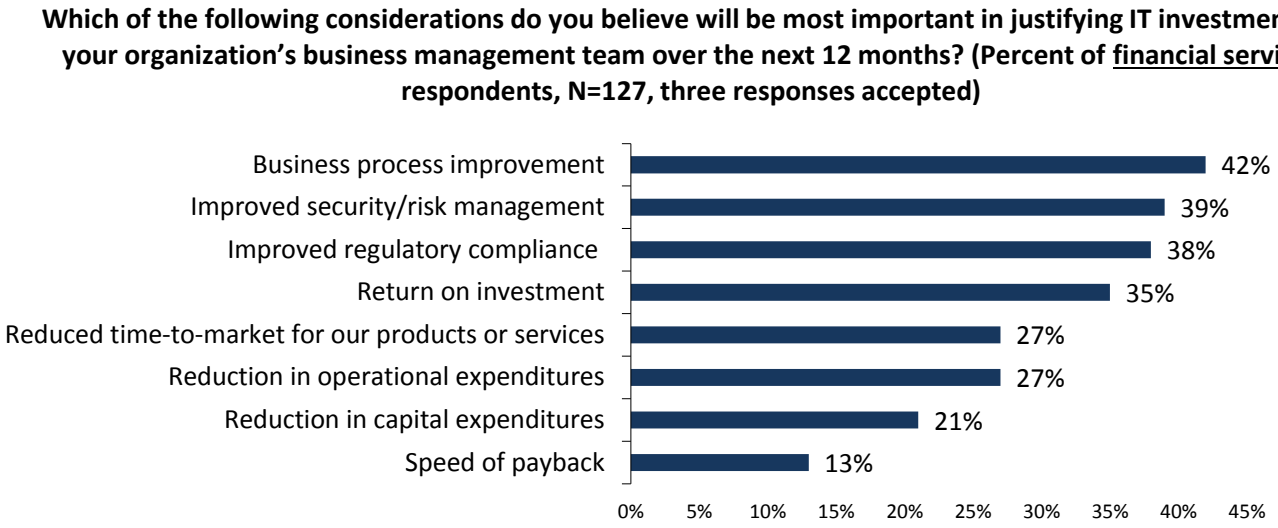


Source: Enterprise Strategy Group, 2015.

However, regulatory compliance (and information governance in general) aren't exclusively technology-centered priorities. Compliance/governance considerations also factor into the business-level decision-making process whenever financial organizations' IT managers investigate whether or not to make an IT investment (see Figure 2).[2]

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.
[2] ibid.

FIGURE 2. Most Important Considerations for Justifying IT Investments in 2015 Among Financial Services IT Managers



Source: Enterprise Strategy Group, 2015.

What Governance and Compliance Mean to Financial Services Organizations

Multiple federal/state regulatory and independent industry bodies monitor the operational behavior of banks, mutual fund companies, securities firms, annuity providers, and other financial institutions. But translating myriad compliance and information governance rules into *actionable strategies* can be challenging for compliance, risk, legal, and IT departments. For example:

- Internal groups responsible for information governance and regulatory compliance are not always (or only) IT people. They work in different groups and thus use different vocabularies. To a bank's backup administrator, compliance may translate as "proper data retention." To its compliance officer, compliance may mean "mitigating regulatory risk."

- A company's size or age can affect its approach to information governance. A large, mature brokerage house will be more accustomed to following mandates and will approach the challenge with relatively more preparation, sophistication, and breadth. Smaller/newer financial firms may have fewer resources and less experience, but they still have an obligation to meet compliance requirements. (Fortunately, every financial organization already has elements it can build upon.)

Why Pursue Information Governance?

Records management, archiving, e-discovery, file analysis, data protection, and related efforts boil down to managing information proactively. The emphasis is on gaining mastery over data and deriving insight/value from it using technology that can identify the data, permit or restrict access to it, and retain or delete it according to compliance and governance mandates. The effort is worthwhile because appropriate information governance:

- Alleviates data hoarding. No organization should keep all its data forever, but identifying and preserving the right data is crucial.

- Supports e-discovery. No one likes to be reminded of the costs and risks associated with a legal discovery procedure. However, preparation can make the process less painful while reducing costs.

- Supports productivity. Good information governance helps any financial institution operate more efficiently and can even improve individual productivity.

Within the financial services sector, information governance is especially vital. Consider that:

- Scrutiny by regulators is increasing.
- Auditors need comprehensive context to examine/reconstruct a financial event properly.
- Any non-compliance that auditors do find can result in significant penalties and sanctions.
- Investors and other financial services clients are highly averse to even a hint of impropriety. Regardless of whether an issue is real or a just matter of "appearances," to them, it's a crisis.
- Operational impediments due to an inability to produce data are disruptive and can hamper important initiatives.

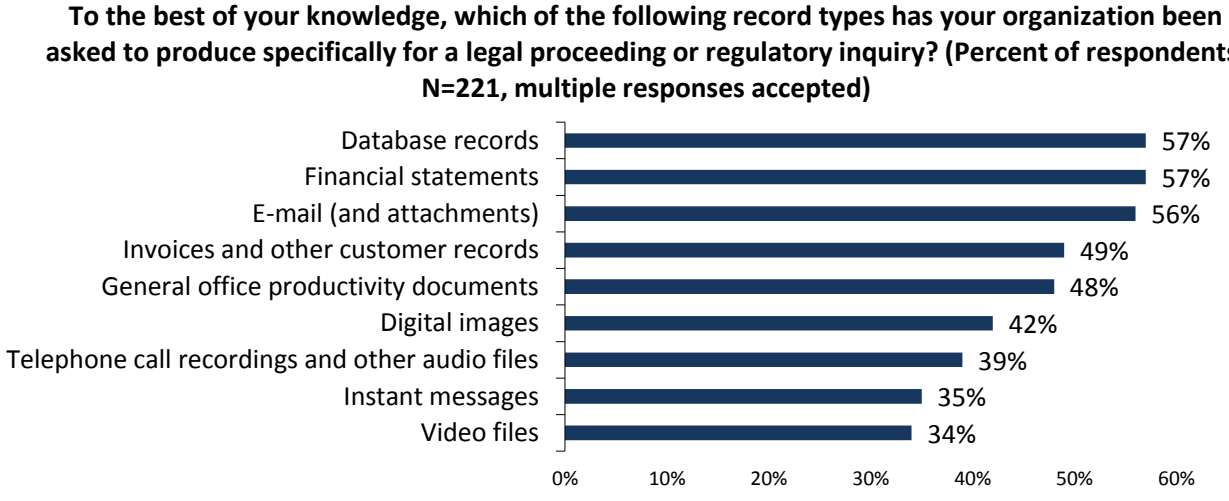
The need to be thorough is underscored by regulations such as SEC 17a-3. On the books in the U.S. for decades, part of the statute lays out preservation rules for paper and digital documentation pertaining to securities transactions. But even in the absence of a formal mandate such as 17a-3, financial firms must define and enforce policies that *support the business's requirements*. Striking that balance is no small task.

What Is the Right Information to Govern?

Many financial institutions use a governance, regulatory, and compliance (GRC) system to help them manage governance efforts, but then they learn that automation alone isn't enough. Good governance often requires human intervention—for example, someone may have to make a decision to increase password-strength parameters or draft a procedure defining how to make certain data available to auditors while protecting it against all other external/unauthorized access.

In general, people who work in financial institutions need to know what data they have—governance must encompass more than just e-mail messages or basic financial records. As an example, the data types listed in Figure 3 are frequently requested during e-discovery or regulatory-inquiry events and thus need to be governed properly.[3]

FIGURE 3. Types of Data Specifically Requested for a Legal Proceeding or Regulatory Inquiry



Source: Enterprise Strategy Group, 2015.

[3] Source: ESG Research Report, *Backup and Archiving Convergence Trends*, April 2014.

In the financial services industry, the threat of very large monetary penalties can be a significant impetus to compliance. Less quantifiable (but no less serious) are the reputational penalties and potential loss of revenue associated with poor information retention or gaps in data-access protocols.

Facing the Challenge

Governance and compliance involves retaining the right data, in the right manner, for the right reasons. By now, most financial institutions have some level of capability to manage their information. Unfortunately, many are still relying on legacy and sometimes manual systems and processes to attempt to govern their data. As a result, they often have difficulty quickly responding to regulator requests, mitigating compliance risks, and controlling costs.

Responsible information governance may sound daunting. But it becomes less so by following some easy steps.

Step One: Communicate

Information governance is not IT driven; it is committee driven. All relevant technical and non-technical stakeholders must take part to ensure that governance requirements *across the organization* are met. Stakeholders include:

- Records managers and data protection specialists who understand archiving and preservation principles.
- IT operations administrators who know the server infrastructure in use.
- Backup administrators responsible for overseeing the mechanisms by which digital data is protected.
- Application admins who understand their production platforms and the data to be protected/deleted.
- Legal employees responsible for litigation readiness and responsiveness.
- Compliance officers responsible for adhering to corporate, industry, and regulatory requirements.
- Risk managers responsible for identifying and mitigating any risks presented by the business information.
- Business unit leaders who understand the organization's requirements for and usage of their information.

Step Two: Cultural Evolution

In finance, some undertakings are tactical. Others, such as governance, are strategic-level activities with long-term implications. Pursuing any strategic initiative takes planning, preparation, and in some cases, outside expertise. However, in the case of governance, the thinking may need to progress from a tactical "check-box-driven" starting point to something more nuanced and impactful.

After everyone is communicating, a shared culture shift is the logical next step for financial institutions that want to establish or improve their approach to information governance. It's the responsibility of the risk management team to ensure adherence. The IT team is responsible for quite a bit of the execution. The leadership team is responsible for communicating the requirements. A lot of teams have responsibilities; it would be unwise to assume that one discrete "compliance team" is going to handle all of the tasks. Additionally, upper management may need to retain consultants capable of assessing the current situation; they may have to authorize a gap analysis, and they may have to approve and initiate risk assessments to uncover vulnerable areas. Clearly, this is a cultural evolution, not an "IT-only" endeavor.

Step Three: Technology

The technologies involved in IG or RC are more than just "backup." Actually, they have two defining characteristics.

Intelligence About the Data

When it comes to governance and compliance, financial organizations need to understand what data they have. ESG believes that by 2016, one key differentiator for data protection and data management/information governance solutions will be the *quality of the catalog.* Knowing what resides in all the information repositories makes the organization smarter about how to retain it. For instance, it might seem tempting to just "keep everything" to satisfy governance requirements, but that route is impractical and even risky from an economic and operational perspective. When the organization knows what data it has, what it should retain, and what it should delete, then it will be able to shrink CapEx (i.e., storage footprint) and reduce OpEx (i.e., the operational costs of managing that storage hardware).

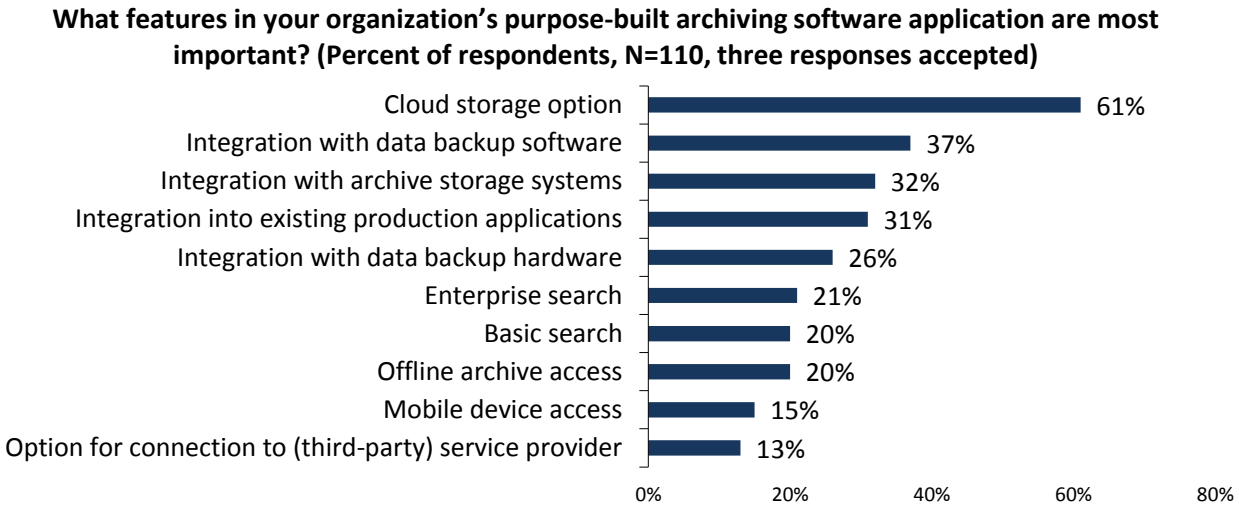
In addition to the data, one must also store and manage metadata, which is additional information about the data that assists in the retrieval, indexing, audit, and use of the data. Without appropriate metadata, it is difficult to determine how to properly identify the data and apply proper lifecycle management to it. Therefore, metadata provides context to the data.

Financial services IT teams should be thinking about how to gain deeper insight about the many data types that could be part of an audit or regulatory event—and have software in place to ensure that the data is easily discoverable and deliverable to internal users and outside compliance professionals.

Easy Integration with the Environment

An information governance solution that satisfies financial regulatory requirements cannot exist in a vacuum. According to ESG research, five of the top six most-cited features needed in a long-term data retention solution involve integration with some aspect of an existing IT architecture (see Figure 4).[4] Integration with GRC systems may be necessary if data is used to provide evidence for complying with regulations.

FIGURE 4. Most Important Features of Purpose-built Archiving Software



Source: Enterprise Strategy Group, 2015.

[4] ibid.

Financial firms need to think about how their data preservation and information governance software/hardware will coexist with the production IT infrastructure to ensure agility and full compliance. Neither the production systems nor the employees should be burdened.

The Bigger Truth

Information governance is a conceptual term that really just boils down to *storing the right data for the right reasons*—reasons that are especially weighty for financial services organizations because of the outside scrutiny they are subjected to and the punishments they might receive for failing to govern digital information correctly.

That being said, governance and regulatory compliance are "hard" only because IT professionals don't always have the full perspective and business insights necessary to govern that information all by themselves. Like any other IT-oriented business transformation, good governance requires that IT and non-technical stakeholders communicate: They must engage with business unit leaders and application owners who oversee platforms that generate data mandated for retention, and any other internal group that may be audited, too.

After each stakeholder is aware of and aligned to the organization's requirements, IT, together with the other departments, can implement technology that powers good information governance (or compliance). The solution they choose must include a rich catalog that lists what data resides within the organization. It also must integrate easily with the IT framework already in use.

Governance and compliance are "hard" only while they remain foreign and unfamiliar. When an organization collectively gets more comfortable with the requirements and establishes access to a comprehensive catalog, governance rapidly becomes more "doable." And with that technology in place and communication ongoing, adherence to governance and compliance mandates eventually just becomes part of how a financial services organization functions organically.