G00299558

Create an Effective Information Risk Framework for Data and Analytics Programs

Published: 7 June 2016

Analyst(s): Saul Judah

Few CIOs and chief data/analytics officers are adequately addressing information risk in their broader EIM or specific data and analytics programs. Implementing an information risk framework will help protect enterprise investment, sustain business value and reduce the threat of reputational damage.

Key Challenges

- Data and analytics initiatives and broader enterprise information management (EIM) programs often do not have an effective framework for addressing information risks. This leads to greater exposure to risk events, such as operational failures and increased costs, that destroy business value.
- Data and analytics teams and information risk and security functions are often disconnected, have differing priorities and are prone to conflict between delivering the business opportunity and adequately addressing information risk.
- In the absence of a fit-for-purpose information risk environment, a flexible, resilient and future-facing digital business is impossible to achieve.

Recommendations

For CIOs, chief data/analytics officers, and data and analytics leaders:

- Implement the information risk framework described in this research as a core part of your formal EIM program or any individual data and analytics initiative.
- Fully establish the information risk management framework in Mode 1 of your bimodal information governance approach, and apply selective parts in Mode 2.
- Recognize that information risk is wider than the scope of your existing data and analytics programs, and engage early and often with information risk and security teams to agree on critical information assets and risk treatment.

- Configure and integrate the information risk framework so that it is fully consistent and harmonized with your enterprise information risk and security approach.

Strategic Planning Assumptions

By 2017, 50% of IT spending will be outside of the CIO's control.

By 2019, 75% of analytics solutions will incorporate 10 or more exogenous data sources from second-party partners or third-party providers.

Introduction

Organizations cannot achieve business growth, operational excellence, cost optimization or meet regulatory and risk requirements without effective enterprise information management (EIM), spanning all data and analytics programs. Initiatives such as business intelligence (BI) and analytics, enterprise self-service provision, master data management (MDM) and information governance are often business-critical components and address critical operational processes (see Note 1). Therefore, the impact to the business would be severe if the high-value enterprise information created, consumed and controlled by these programs failed, was corrupted, or could no longer be trusted or provided at all.

This is not a theoretical risk.[1] In order to address this business risk exposure, organizations must confirm that:

- An effective information risk framework is in place, appropriate for the size and complexity of their organization
- This framework is dynamic/flexible, aligned with business strategy and able to deliver business value while protecting its information investment

Gartner sees many organizations deal with certain risks to data and analytics programs well; for example, risks relating to resourcing skills, interproject dependencies and infrastructure deployment delay.

On the contrary, information risks — such as inadequate information classification leading to information mishandling, inconsistent and inaccurate master data, and conflicting business rules — are addressed less effectively in data and analytics programs. Often, it is assumed that consideration of such information risks is delegated, after the fact, to enterprise risk/security management teams. But the disconnect between these teams often leads to a failure to adequately address key information risks. This can have an operational and financial impact, increasing exposure to reputational damage and, in some industries (e.g., financial services, healthcare), regulatory fines.

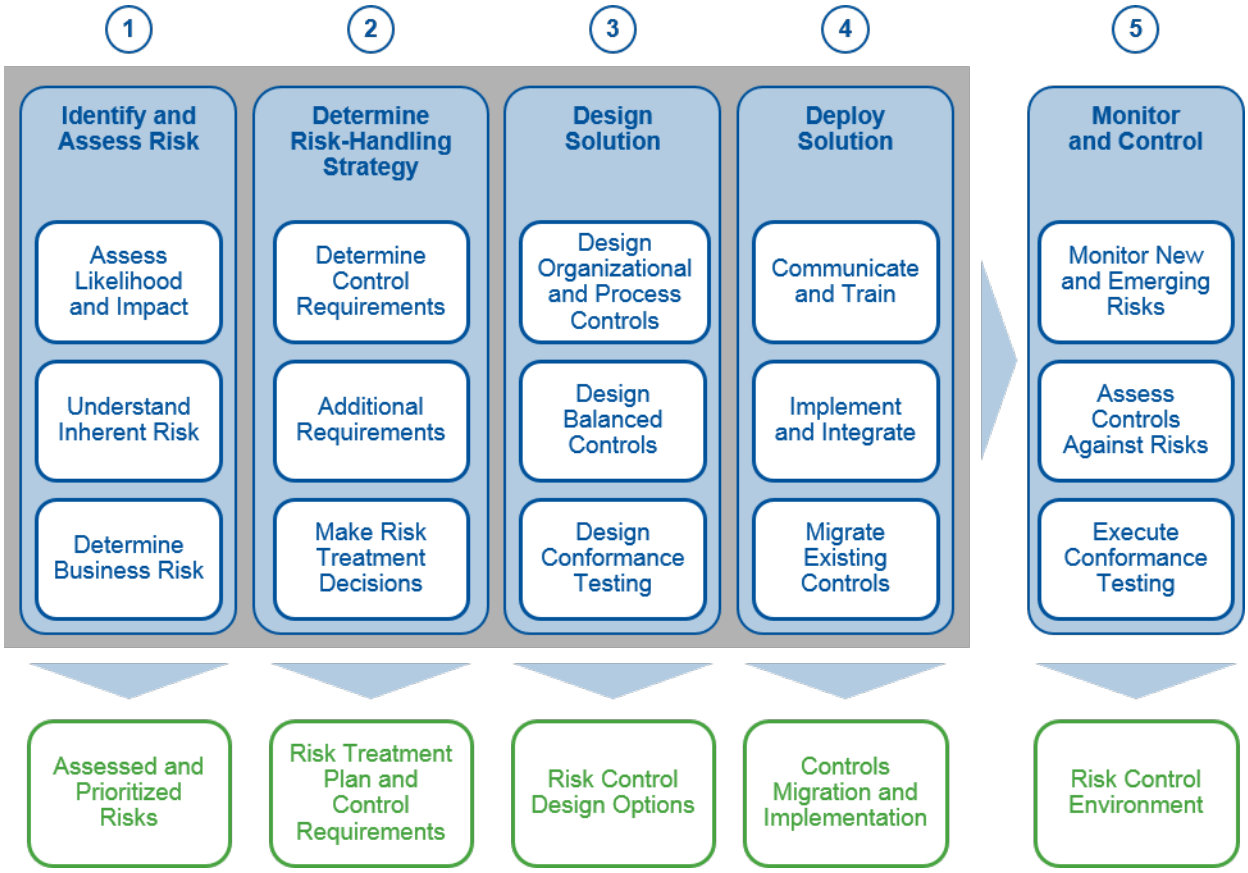
The Information Risk Framework

As illustrated in Figure 1, Gartner's information risk framework for data and analytics programs addresses *information risk,* not information program risk. Each of its five pillars groups together the related risk processes, techniques and outcomes that enable information risk to be identified, evaluated, addressed and managed. When used in conjunction with Gartner's seven building blocks of EIM (see "Strategic Roadmap for Enterprise Information Management"), the framework can be used to treat information risk in all data and analytics programs such as BI and analytics, MDM and information governance.

The framework enables CIOs, chief data/analytic officers, data and analytics leaders, information stewards and enterprise risk teams to use a common framework to understand and address their business exposure to information risk (e.g., failure of identity management components in an MDM environment used in critical business operations).

It should be noted that this framework is primarily designed for Mode 1 scenarios. Mode 2 scenarios would use only some parts of the framework, which are also discussed in this research paper.

Figure 1. The Information Risk Framework



Source: Gartner (June 2016)

Because information risk profiles change over time, the treatment of risk must also be dynamic and managed as part of an effective risk control environment. Implementing the framework in Figure 1 in this manner will enable CIOs, chief data/analytics officers, data and analytics leaders and information stewards to effectively address information risk as a dynamic, ongoing concern, rather than as a set of rigid and static actions taken at a particular stage in the data and analytics program.

Analysis

1. Identify and Assess Risk

It is critical to understand information risk in the context of business outcomes that EIM programs (overarching, strategic and enterprisewide information programs) and specific data and analytics programs (such as BI and analytics or MDM) are aiming to achieve. Data and analytics programs that have been operational for some time may already have a history of risk events — actual occurrences and realized impacts such as customer data privacy breaches resulting in customer complaints, attrition and fines. In addition, analysis of other data points such as previous internal and external audit observations are also valuable inputs to the current risk assessment process.

It is also beneficial to look at the risks and risk events related to other programs, such as ERP and CRM. Any existing IT risk register should be a primary input into the process, though this is likely to have more than just information risk listed.

Similar benefits may be derived from analysis of available architectural reviews of other programs or implementations. It is also strongly advised that external sources of information risk be explored so that insights from other organizations can be gained. Subscription to published threat reports — together with insight from Gartner analysts on EIM program issues and risks that have been seen elsewhere — will be valuable inputs to help determine the information risk landscape (see "Toolkit: Applying the Gartner Risk Assessment Methodology to Critical Enterprise Assets").

Establishing an ongoing dialogue with operational risk and security teams, information governance bodies and information stewards is essential. This will help to ensure that the data and analytics program gains the full benefit of experience, insight, processes and technologies already available, as well as the internal and external data points that are vital in managing information risk. Furthermore, because the operational risk and security teams will most likely have an enterprise understanding of the timescales, schedules and processes for creating and retiring risk and control processes, early engagement is recommended.

Once the landscape of information risk has been identified, assessment of it can be carried out within the appropriate business and technology areas. The business assessment of information risk must be carried out on the basis of its data value as it applies to different areas of the organization. The information classification policy is a key instrument for doing this and enables its scheme (e.g., secret, confidential, internal, public) to drive the way that information is handled to achieve the desired business outcome. For the information risks that have been identified, their assessment in terms of the likelihood of occurrence, level of impact on the organization, value of opportunity and risk appetite can be ascertained.

These risk assessments contribute to an understanding of the inherent risks to be faced, and enable information leaders to understand and communicate the probability of loss to the business if no action is taken to address those risks. In addition to this perspective, the business opportunity (e.g., cost savings by moving customer loyalty management applications to the cloud) must be weighed against the organization's risk appetite for doing so. This enables the assessment of the risk-adjusted opportunity value and the right mix of strategic options (e.g., acceptance, transference, avoidance, mitigation) for prioritizing and treating elements of the information risk (see "The Gartner Strategic Risk Evaluation Approach for Digital Business").

2. Determine Risk-Handling Strategy

The prioritized risks that have been identified are used to determine the actions that must follow. The "Gartner Risk Treatment Model for Digital Business" enables information leaders to approach risk from the balanced perspective of risk and reward. This allows more appropriate risk decisions to be made that result in risk acceptance, transference and mitigation based on business value and opportunity. In the "move customer loyalty to the cloud" example, the risk treatment may result in acceptance of risk for analytics and data quality tools but not for critical customer data. Therefore, the outcome may be provision of SaaS for analytics and data quality, and an on-premises MDM application for customer master data.

Many stakeholders are involved in EIM programs, and it is necessary to first identify and engage the appropriate owners of the identified risks. This may end up being very specific to each individual program or project. In the "move customer loyalty to the cloud" scenario, the chief marketing officer (CMO) may be the principal risk owner, whereas the chief product officer may be the principal risk owner in a "manufacturing automation" digital business scenario. This leads to more informed and appropriate risk decisions being taken and more effective information governance with greater accountability and transparency. The actions needed to address each risk must be defined at a level of detail necessary for the owner of the action to execute it. It is quite possible that the owner of the risk and the owner of the action are not only in different roles, but in different parts of the organization or even outside it. For example, the risk of "customer data loss leading to privacy breach and compliance failure" may be owned by the CMO, while the action, "implement and test preventative and detective controls," may be the responsibility of the IT company hosting and providing SaaS applications to the company.

In addition to the actions needed to address risk, control requirements are also defined. These identify the ongoing need for processes and procedures that must be put in place to control the risk. Solution design is not the aim at this point; rather, a clear statement of what capabilities need to be in place on an ongoing basis to address the risk.

Often, the mitigating actions and control requirements by themselves do not address all of the risks identified, and some residual or secondary risk may remain even after the actions and controls have been implemented. Identifying this residual risk supports a more thorough risk analysis and enables a multilayered response to be taken. It is also often the case that additional requirements (other than control requirements) are needed; for example, technology requirements that support the type of control requirements needed for the formation of a cross-business-area data steward.

This process of risk treatment is carried out in the context of the organization's risk appetite, and it will be a business decision as to whether the possibility of loss is acceptable and within the organization's risk tolerance. For example, a risk may be that information stewards operating in silos are unable to identify cross-domain business data issues, the consequence of which might be a 1:100,000 probability of occurrence with a $1 million financial impact, but no additional loss due to regulatory fines or reputational damage. It is quite possible that some organizations may choose to accept this risk, rather than fund potentially expensive mitigation actions. However, since the business decision to accept the risk is based on the risk data provided, it is critical that the probability, impact, opportunity and appetite are all correctly assessed.

A very different decision may have been reached if the probability was 1:1,000 and the financial impact was $10 million. In this situation, it is more likely that an organization would seek to establish and then monitor a variety of controls, establish a communications and education plan, and obtain insurance against potential loss. Such decisions cannot be taken in isolation; instead, they must be taken in conjunction with the information risk and security teams, and with the involvement of accountable information governance bodies.

3. Design Solution

The solution design takes as its inputs the control requirements, additional considerations identified and the decisions on segregation of risk. For the EIM programs already in place, existing controls, risk acceptance and transference decisions must be reassessed to check they remain fit for purpose against the emerging risk landscape.

For example, as the level and maturity of SaaS technologies increase, risk appetite may allow more applications, processing and related controls to be hosted on cloud rather than implemented on-premises, which reduces cost and supports a more elastic economic model for information. This is important, so that the risk controls and processes that are already effective are maintained and enhanced in the right places and the ones that are not, or are missing, are appropriately targeted. During the activity to determine requirements, the owners of risk and action will not only be identified, but fully engaged. At this stage, activity follows to identify the specific areas of organizational structure and current business processes where information risk controls are required. Engagement with the current process owners and senior managers is necessary, so that appropriate preparation is made for migration of controls into the next stage of the framework.

If an effective risk control environment is to be designed, there must be the right mix of controls. This means that cultural and political considerations are as important as the cost of implementing the right controls. After all, implementing controls that address the risk, but that nobody will follow, cannot result in an effective control environment. Good design, in this case, will adopt the right mix of detective, preventative and monitoring controls. Good solution design needs to consider not only the risks faced in the current environment, but also the near-term and midterm threat horizon. For example, scenarios where an organization is exploring PaaS or SaaS models must consider options such as pervasive internal monitoring and people-centric strategies (see "Prevention Is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence").

Alongside the design of effective and balanced controls, the approach to conformance testing must be defined. Criteria that define "pass," "fail" and the values in between will be specified with

examples. In the case of effective information governance controls, one of the conformance tests might look at the number of senior business stakeholders who attended the information governance steering group, which has oversight of the data and analytics program.

4. Deploy Solution

The process of solution deployment is typically a resource- and time-intensive activity and should not be underestimated. For a CIO and chief data/analytics officer, it is very important to understand how this will be done, by whom, and the parts of the organization that need to be involved. In some organizations, operational risk departments manage and execute this activity with timescales and processes that are well-established. In such cases, the life cycle and latency of existing risk and control processes must be understood, rather than seeking to deploy a separate solution. The migration of new controls and the exit management of existing controls is also often complex and prone to process issues. Sometimes, existing controls have audit observations against them, policy exceptions in place, and issues that are in the process of resolution. In some situations, there may be third parties whose contractual terms are connected with controls that are becoming obsolete; migration to newer controls may also cause delays.

Communication and training are critical activities that can determine the success or failure of the risk control environment. Those affected must understand what is planned, what is happening throughout, how this affects them and how they should operate differently. Communication management and an education and training plan should already be activities that CIOs, chief data/analytics officers, and data and analytics leaders have oversight of, so extending these plans to include the implications of establishing an information risk framework should not be overly difficult. However, if no such plans exist, options should be explored for creating an appropriate communication and training plan for all aspects of the EIM program — not just the information risk management aspects. To be most effective, communication and training should be aligned with existing initiatives, such as data privacy and information security.

5. Monitor and Control

An effective information risk environment for data and analytics programs requires the ongoing monitoring and control of information risks and risk decisions. This means that, for the controls that have been established to address the risk, appetite-related thresholds are used to monitor the performance of operations and processes against established leading and lagging indicators.

For example, in a customer master data record, a social security number/national identity number might have an availability threshold of 98.0% for "green," an "amber" threshold between 95.0% and 97.9%, and a "red" threshold of 94.9% or less (where green, amber and red represent risk tolerance thresholds). Monitoring controls that have been established could identify the downward drift that has its origins in a particular call center and trigger an event that invokes preventative controls — such as a phone alert to the data steward associated with that business area, who can then take immediate action or escalate the issue so that the risk is addressed quickly before it reaches an unacceptable level.

The conformance testing plan created during the design phase must be executed to test the effectiveness of the control environment. If the controls have been well-designed, the data steward will be able to use the ongoing metrics generated to gain a good understanding of the level of conformance in business processes well ahead of formal conformance testing assessments. If internal audit teams have produced guidelines on control characteristics, these should be used as the benchmark to ensure compliance.

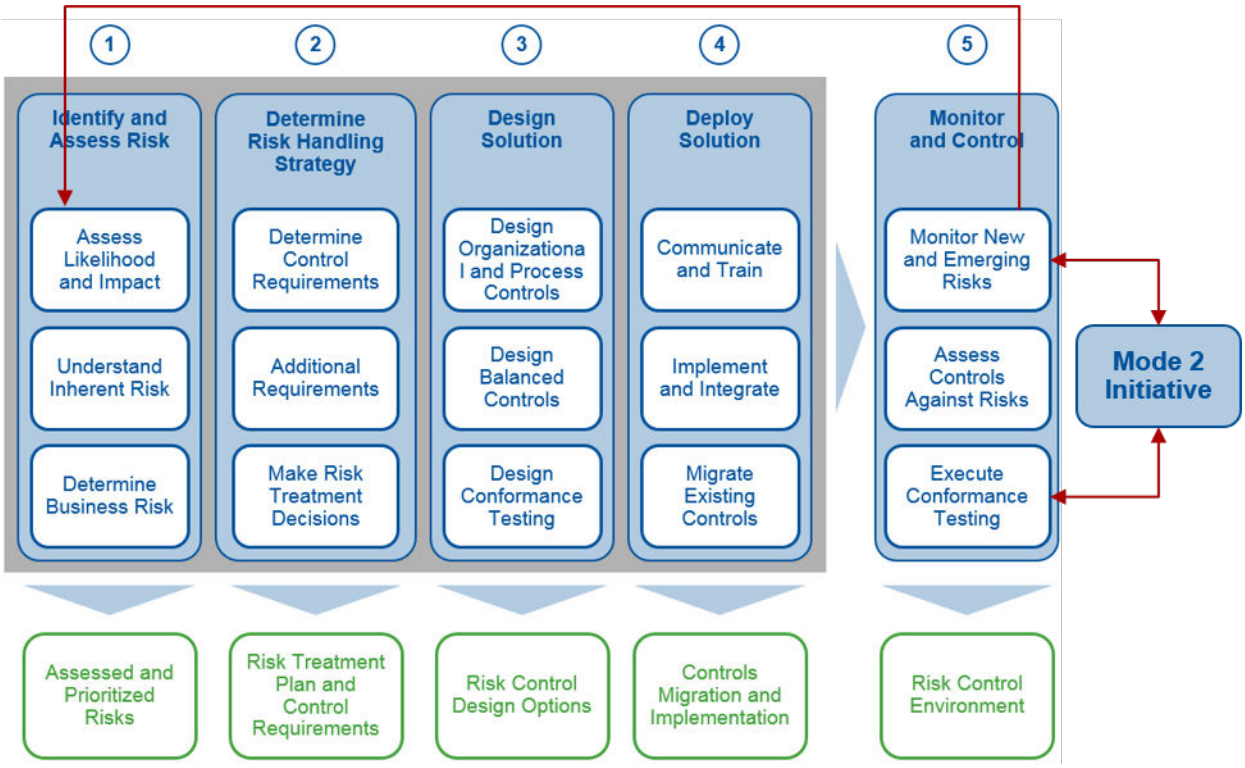
Data and analytics leaders must be vigilant against complacency and review the EIM program and the information created and consumed against new and emerging risks. This does not, typically, require a formal process, but should involve frequent discussions with business stakeholders and IT teams to address questions like, "Has the risk in our organization changed?" and "Do the risk acceptance decisions we have made still make sense."

Reviewing the risk profile is often the hallmark of a risk-aware organization and indicates a higher level of information maturity. Even if the risk control environment is highly effective, it does not necessarily mean that it is secure against new risks that may have emerged as a result of, for example, organizational redesign or new disruptive technologies and opportunities (such as open data) becoming available.

The Information Risk Framework for Mode 2 Scenarios

The information risk framework shown in Figure 1 applies entirely to Mode 1 scenarios. However, its full application in Mode 2 situations is likely to quickly bring any innovation initiative, proof of concept (POC) trial or business area exploratory project to a grinding halt. Mode 2 initiatives for which there is no awareness of the information risks present, or new risks being created as a result of their direct activity, are themselves a threat to the business and must be addressed.

Figure 2. The Information Risk Framework for Mode 2 Initiatives



Source: Gartner (June 2016)

Figure 2 illustrates how the information risk framework can be applied to Mode 2 activity. For example, a bank may have a POC initiative underway, such as an API platform that allows the creation of peer-to-peer banking apps through the use of some of the bank's software components (e.g., an identity and verification service). In this context, it is critical that emerging information risks that are created by this POC trial are understood and monitored.

Furthermore, the new threat landscape must be understood in the context of the risk treatment strategies (including the existing risk approach, controls and culture in the bank). This enables a risk-adjusted assessment of the business opportunity offered by the POC in the full context of what it would mean to the bank's risk profile, if the initiative was brought into production.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Strategic Roadmap for Enterprise Information Management"

"ITScore for Risk Management"

"Aspire: A Framework for Analytic Business Processes"

"Digital Business Forever Changes How Risk and Security Deliver Value"

"The Gartner Strategic Risk Evaluation Approach for Digital Business"

"Prevention Is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence"

"Toolkit: Applying the Gartner Risk Assessment Methodology to Critical Enterprise Assets"

"Protect Your Enterprise Information Assets With Effective Risk Management"

Evidence

The observations, findings and recommendations in this document are based primarily on interactions with IT leaders, focused on MDM and information risk, during Gartner client inquiries over the past 12 months.

[1] A 2016 study by Verizon into successful data breaches showed that "89% of breaches had a financial or espionage motive" and "the time to compromise is almost always days or less, if not minutes or less."

"2016 Data Breach Investigations Report," Verizon, 2016.

Note 1

The information risk framework can be used by all types of data and analytics programs. Apart from those mentioned in the body of the report (BI and analytics, enterprise self-service provision, MDM and information governance), the framework can equally be applied to other programs such as enterprise content management, digital asset management, application integration and application data management.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp