Grant Thornton

How to tailor integrated risk management

Find the right fit for your business and market

Risk management used to depend on theories and rules alone — but integrated risk management (IRM) goes farther.

Traditional governance, risk and compliance (GRC) activities were mostly reactive. Reactive approaches do not continuously sense and monitor risk and control postures. It doesn't adapt to the constantly evolving risks that most organizations face today. Many organizations have tried to accelerate their GRC activities with automation, but that only accelerates a reactive approach.

Instead, organizations need a proactive approach that breaks down risk silos and reorders risk management practices, empowering collaborative risk governance and risk harmonization to drive the best responses.

IRM combines the enterprise, operational, privacy, business continuity, vendor and other risk management components across an enterprise. It integrates risk management and risk responses, and it can foster a culture of mitigating risks and informing decisions every day.

New risks, growing regulations and other complexities are forcing many organizations to reconsider their risk management. Traditional mitigation activities might no longer be efficient and effective enough. So how can organizations reapproach risk management, to integrate it into their businesses for maximum efficiency and effectiveness?

Align with 7 IRM considerations

When risk management becomes more integrated, it must become more customized to multiple unique use cases within an organization. That means there is no single approach that will work for every industry, organization or business unit.

As organizations define the details of their IRM and its ongoing management, they should weigh 7 strategic considerations:

1 Move from one use case to many

"Many organizations only enabled one use case when they first moved from nothing to something — that is, from a spreadsheet to a risk management plan, around 2002," said Grant Thornton Cyber Risk Managing Director Sudhakar Sathiyamurthy. This single model meant that organizations tried to align all their activities with one model so that they could see and manage all their risks with "one pane of glass."

"Having a one-pane-of-glass view is actually phenomenal," Sathiyamurthy remarked. "But, at the same time, one use case is not a sustainable model because everyone has their own methodologies and processes." To force everyone into one use case means that some teams cannot use the risk management model efficiently, or to its fullest value.

"People are moving away from this central-platform model, to a more collaborative play," Sathiyamurthy added. "You may have two or three models, but you can have some common capabilities synchronized. It's a more federated integrated risk management model."

> "Many organizations only enabled one use case when they first moved from nothing to something — that is, from a spreadsheet to a risk management plan, around 2002."
>
> **Sudhakar Sathiyamurthy,**
> **Cyber Risk Managing Director, Grant Thornton LLP**

2 Consolidate data

Organizations cannot manage the risks they cannot see. "Data is going to be everything," Sathiyamurthy noted. It's important for businesses in every sector to identify the data that plays a role in risk management and to consolidate a comprehensive view of the data. "Regardless of whether there's one solution or multiple solutions, the consolidation of data is extremely critical to support their risk-based decision-making process. Everything rolls up into analytics or an organizational platform that provides leaders with the right level of insight, foresight and hindsight."

3 Include stakeholders

Stakeholders might initially have a variety of questions or challenges for an IRM solution. "People sometimes gravitate toward the cheapest solution," Sathiyamurthy stated. "Or, some see the value and some push back on the budget. Plus, every company has its camps, and one camp may not want to move away from an existing process or solution."

The best answer might be one that orchestrates the best of existing solutions with new capabilities and insights. This combination can help drive leader support and user adoption. "The cultural change management aspect of bringing stakeholders and users on board is going to play a big role," Sathiyamurthy remarked.

4 Design for usability

Usability can be subjective. When an organization's user base is accustomed to one process or solution, that becomes a reference point for usability — even if it's not intuitive.

"Almost every organization has some solution," Sathiyamurthy said. When organizations try to shift to new IRM solutions, they often generate user fatigue. "The reason is that they haven't designed with the end in mind, and they have not adequately considered the usability requirements of their unique user base. But the user experience is going to be one of the key differentiators of what works in each market."

5 Plan for scalability

An organization's IRM solution will ultimately require scalability. "Of course, organic and inorganic changes might factor into scalability," Sathiyamurthy said. "But one of the key factors for solution selection is how the solution aligns to an organizational outlay and the projected changes for the next one to three years."

Sathiyamurthy also identified two sides to that equation — solution and content. "The scalability of the content is extremely important. Content is how firms demonstrate defensibility to regulatory compliance obligations, and sense, manage, and respond to the risk scenarios that might apply to them," he added.

6 Establish long-term support

Perhaps the biggest risk in IRM is that many organizations do not sufficiently plan beyond the initial implementation. "People often think about it as a point-in-time project," Sathiyamurthy observed. "They think that, once they implement the solution, everything is mostly taken care of. They haven't planned in advance who's going to help them to sustain this and how the solution is going to be managed." Small and mid-size organizations can be the most likely to lack long-term support from IT and other internal teams to create and manage user groups, access rights, data integration, and other tasks.

7 Model a phased approach

Since IRM can be a long-term investment, many organizations look for ways to spread out the cost and effort over time. "I've seen a few organizations take a big-bang approach, but most look for a way to break the effort into phases," Sathiyamurthy said.

A project modeler can help organizations choose the most critical use cases, then look into the second-wave or third-wave use cases. "An effective modeler is going to deconstruct the projected roadmap into what they have to do now, do next and then do later. That can depend on incremental value or the priority updates they want to make. At the same time, it lets an organization correct its course," Sathiyamurthy said.

> "An effective modeler is going to deconstruct the projected roadmap into what they have to do now, do next and then do later."
>
> **Sudhakar Sathiyamurthy, Cyber Risk Managing Director, Grant Thornton LLP**

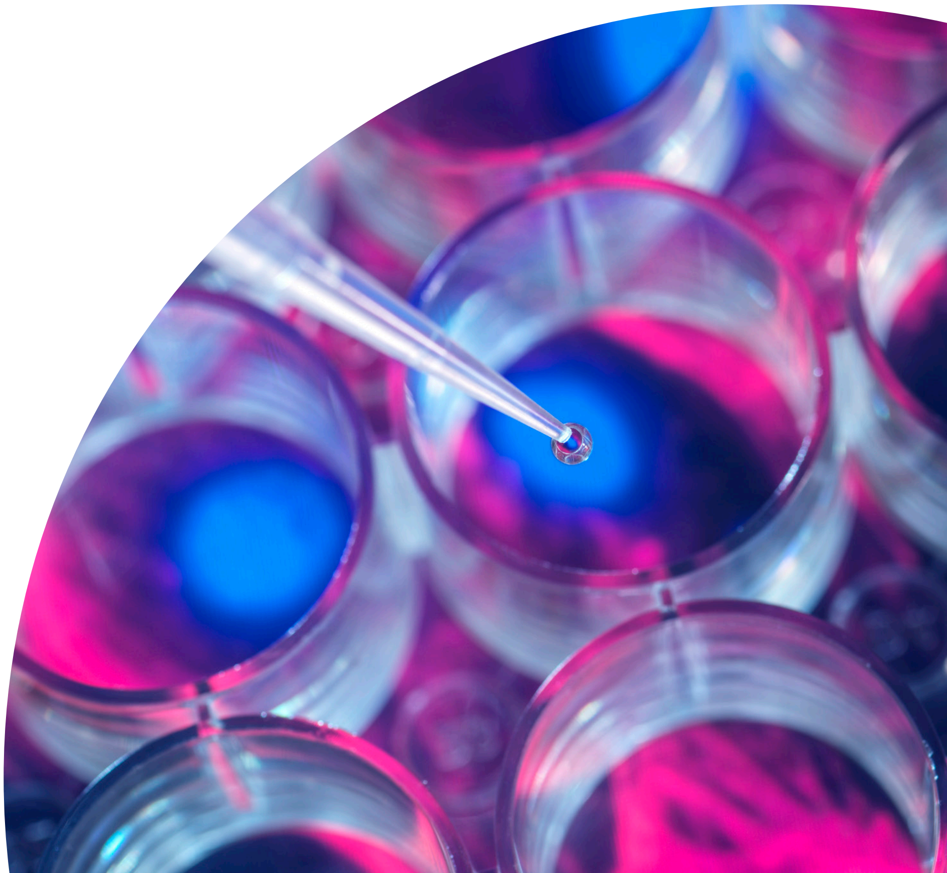
Identify IRM use cases

Every organization has a unique risk profile, with different use cases and priorities for risk management. To define the best use cases for an organization, start by recognizing the most critical IRM use cases within the industry.

For instance, healthcare and life sciences companies often have unique risks to manage. "IRM is extremely critical for medical equipment manufacturers, so getting them into an IRM architecture is going to give them a lot of value," Sathiyamurthy noted. From another perspective, organizations in the financial sector face significant risks from data becoming compromised or lost.

Critical IRM use cases by industry

- **Life sciences**
  - Compliance management
  - Requirements change management
  - Third party management
  - Issue management
  - Resiliency management
  - Security operations
- **Finance**
  - Compliance management
  - Audit management
  - Policy management
  - Security operations
  - External feeds
  - Access groups and user roles



- **Manufacturing**
  - Compliance management
  - Requirements change management
  - Third party management
  - Issue management
  - Resiliency management
  - External feeds

- **Retail**
  - Audit management
  - Policy management
  - Security operations
  - External feeds
  - Access groups and user roles

- **Public sector**
  - Compliance management
  - Audit management
  - Issue management
  - Policy management
  - Security operations
  - Access groups and user roles

In heavily regulated business sectors, risks can include negative reputational impact along with regulatory penalties. IRM can play a vital role in reducing risks on both sides of the equation. Risks can also vary over time and be triggered by events like mergers that change an organization's content profile, business model or regulatory landscape.

Tailor your IRM approach

An organization can use three tools to understand its unique risk profile, identify the related use cases and tailor the most effective approach to IRM.

Wireframe models

IRM has powerful potential, but the ability of an IRM solution to achieve its potential ultimately depends on its ability to meet an organization's unique needs and users. To properly prioritize those needs, organizations need a tool that puts them up front in real terms. Wireframe modeling is part of an approach that initiates early discussions of the end product and its requirements.

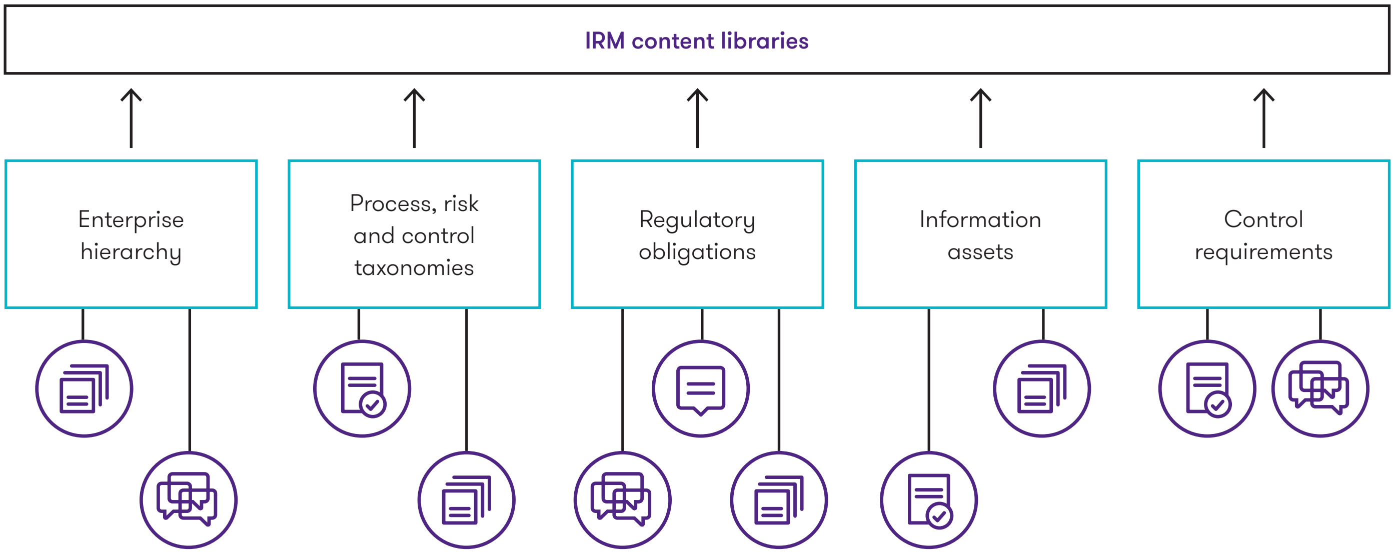
"Accelerators such as the wire frames help organizations model what the end state needs to look like up front," Sathiyamurthy said. "They can help identify data needs as well. That way, they don't have to wait until the end solution is built out."

Content libraries

An IRM can only be as effective as its content. That's why an organization's data consolidation is so important to the success of its IRM. But some of the critical content for risk management is actually not proprietary.

Most organizations can empower their IRM with content libraries that are already populated and engineered for effective access. "An integrative control library or control framework can combine hundreds of laws, regulations, leading practices and other content from authoritative sources into a consolidated and accessible chunk, deconstructed by industries," Sathiyamurthy said. "That gives organizations a huge kickstart on their journey, from a compliance assessment perspective."

IRM content libraries

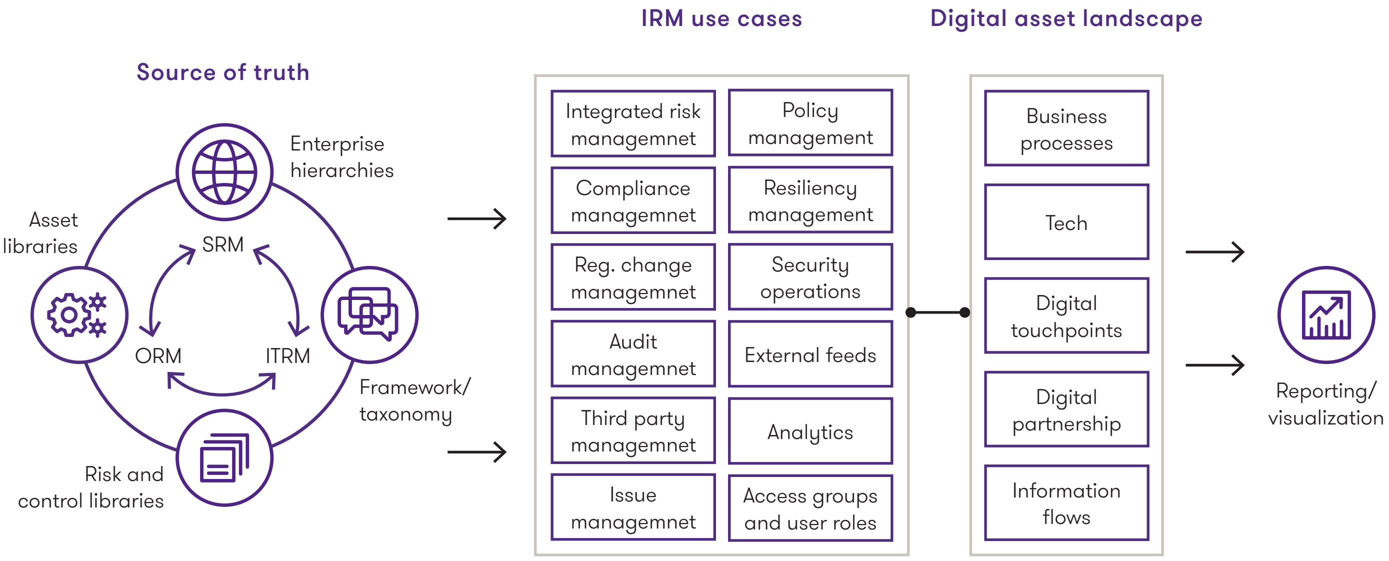


Industry insight and use cases

Organizations can accelerate their progress, improve their architectural decisions and reduce their mistakes by calling upon insights from other IRM implementations — especially others in the same industry.

By combining content libraries with known use cases and industry insights, organizations can save significant time and cost while quickly moving ahead of efforts by competitors. An organization's content, use cases and needs will define the digital asset landscape that the organization can use to report and monitor risk.

IRM architecture

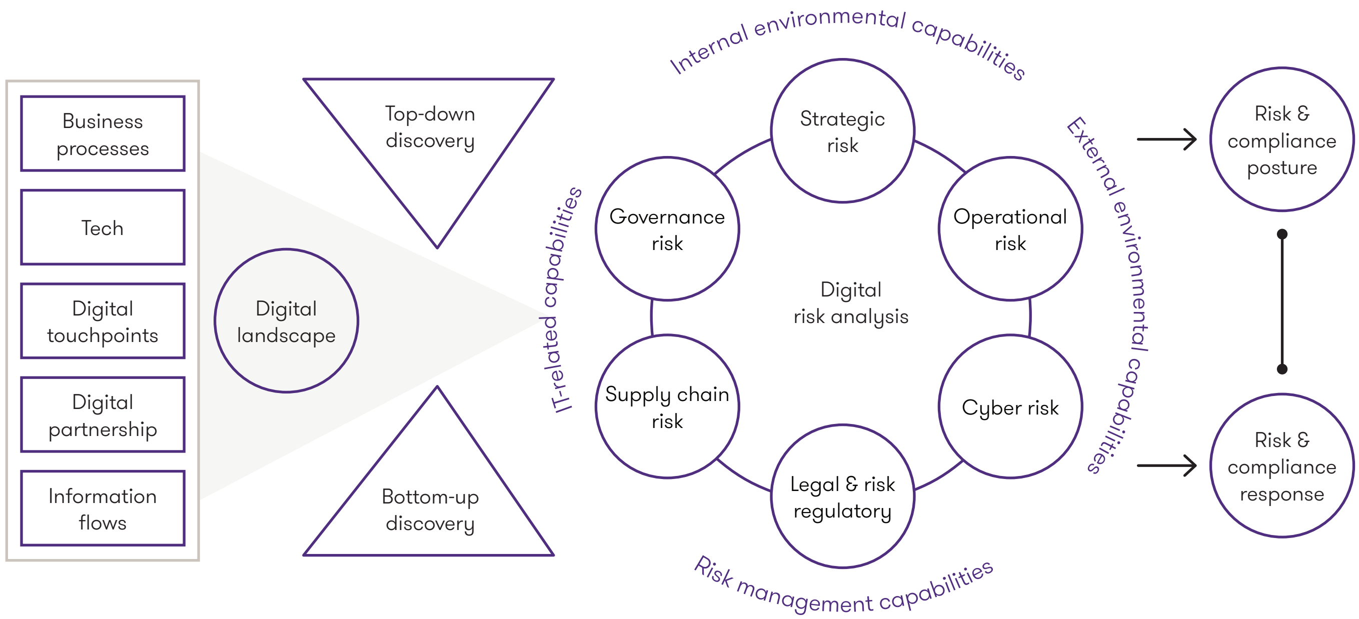


Accelerate with automation

IRM requires continuous monitoring and reporting of risks. This continuous effort is proactive and effective, but it might not be feasible with purely manual processes. In that respect, effective IRM requires technology, often including the acceleration of automation.

Ongoing risk management can require an organization to bridge multiple data sources, business areas, or even divergent risk management systems and processes.

IRM reporting and validation



This can include labor-intensive processes that are often excellent candidates for automation:

- Digitizing information
- Gathering data from multiple systems
- Consolidating data into one view
- Visualizing data to enlighten perspective and help drive decisions
- Tracking specific trends or issues and triggering alerts

When an organization has identified its content, use cases and the digital landscape for reporting and monitoring risk, it can outline the continuous activities that will truly bring effective IRM to life. Automation can help ensure the speed and cadence of these activities, so that they provide proactive information, become integrated in business decisions, and ultimately drive true cultural change.

Contacts

Derek Han
Principal and Leader,
Cybersecurity and Privacy
T +1 312 602 8940
E derek.han@us.gt.com

Sudhakar Sathiyamurthy
Managing Director,
Cyber Risk
T +1 312 602 8585
E sudhakar.sathiyamurthy@us.gt.com

Grant Thornton

© 2021 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd. In the U.S., visit gt.com for details

GT.COM