WHITEPAPER

Modernizing Your GRC Program

Why maturing your program is essential today

It is a different business world today in terms of risk and compliance. Industries and companies face Information Technology (IT) threats like drive-by pharming and session hijacking that did not exist a few years ago. Reporting regulations related to the environment and human rights have exploded. Governance, risk, compliance (GRC) platforms have evolved in the last 20 years from single purpose to multi-functional and from a company focus to an enterprise-level perspective.

Whether it is regulations or economic headwinds or cybersecurity concerns, running a company is more challenging than ever before. And previous solutions to minimize risk no longer work. To keep up with today's volatility, companies must modernize their GRC programs. While that may sound intimidating, in reality, program modernization is more realistic and attainable than you might imagine. And today it can be done with little to no IT involvement. Program goals for modernization are achievable in months rather than years. Progress is measured in weeks.

This whitepaper will help you assess your current GRC program and then help you map out the necessary step towards a modern program where compliance, IT risk, vendor management, risk management, third-party risk, audit, and more are streamlined and efficient with integrated communication and collaboration tools.

A modern GRC program goes beyond checkmark compliance or a seemingly never-ending integration process. Modernness offers quick start and real-time visibility deep into a company's risk landscape with automated tools featuring ones triggered by prescribed events.

Imagine a single source of truth available in real-time and accessible by internal stakeholders, executives, and anyone else who is given access.

Before you can experience a modern GRC program, you must identify and review your current GRC capabilities.

SAI360
RISK FROM EVERY ANGLE

Assess your current setup for risk management and compliance

Based on our experience working with organizations trying to modernize, current programs fall into one of four categories:

1. In-house developed GRC technology

When organizations consider the needs of the business, GRC technology developed in-house may look like the right call compared to standard software. In-house developers know the company and how it operates. They can custom-build how teams and processes run.

However, in-house technology can be a burden for organizations to maintain. The continuous evolution of technology and regulatory changes is difficult and costly to follow. What's more, when software development is not the organization's primary focus, companies using in-house GRC technology often muddle through until a regulation or adverse event forces a change.

Additional downsides to in-house technology include it being very engineered; generalist developers may struggle to identify key challenges or the best way to deliver optimal outcomes.

2. Point solutions for specific purposes

Many organizations employ point solutions for specific tasks like managing vendors or complying with IT risk requirements. These solutions work well in organizations operating in silos. Compliance does their thing. Human Resources does theirs, and so on.

Point solutions are beneficial, but only in situations where you operate in silos and maturity levels significantly differ between silos. It is critical to break these silos down, disseminate knowledge, and raise the collective maturity level of everyone together.

Point solutions fall short when issues are broader and deeper, like a cyber incident that disrupts operations. Or if a risk needs to be monitored closely. A point solution can assess vendors but change often occurs between assessment periods. Monitoring risk would alert management to the issue where it could be proactively addressed.

The same is valid with IT risk. A point solution can manage the company's cybersecurity program, but it will not train your workforce to spot phishing attempts.

3. Spreadsheets and SharePoint

Many organizations still rely on the venerable spreadsheet or collaborate on spreadsheets using SharePoint. Spreadsheets offer many advantages, like how everyone across an organization can seamlessly use and share them across teams. With something so useful and accessible, why not use a spreadsheet for regulatory compliance and managing risk and take advantage of collaboration with SharePoint? This can work, like in the case of a vendor program managing a handful of vendors.

How David Young engages the Panasonic Energy executive team

David Young manages Panasonic Energy's business continuity program and uses the SAI360 platform. Young is a big believer in the executive interview process. Says Young:

"It's not just to understand each executive's perspective and concerns, but also as a team, I gained an aggregate understanding of what they put weight on and importance to."

Young also made the most of the time before the executive meeting.

"I distributed a survey in advance of the executive meeting. It allowed the executives to score topics on a scale of one to ten. I then had survey results to share and some interesting findings that contributed to the discussion. I use that short amount of time with the executive team to create interaction, show value, and get buy-in."

Get buy-in and collect feedback from stakeholders and playmakers

Modernizing your company's GRC program is necessary to keep up with changing regulatory requirements and the evolving business environment. Any modernization effort requires change management and involves multiple decision-makers and influencers. You will meet them here.

It's about removing silos, establishing the right tone from the top down, and engaging the front line for agility.

Senior management

Senior management sets the tone and ensures the organization's GRC program is aligned with its overall strategic goals and objectives. They are also responsible for allocating the necessary resources and budget for the modernization effort.

Having a champion on the senior management team can go a long way to getting the green light to move forward. This executive knows how to package the program to win over the executive team and the board. For the GRC team, identifying and recruiting a champion is priority one.

GRC professionals

GRC professionals make up your GRC team. They include risk managers, compliance officers, and internal auditors. They are responsible for managing the daily GRC processes and implementing the changes required to modernize the program. In addition, your GRC team needs to elect a leader who will serve as a point person for the program and represent the group in meetings.

Business unit leaders

Business unit leaders operationalize the GRC program in their respective areas and ensure that their teams are aware of and comply with policies and procedures, as well as push using the GRC software chosen. For the GRC team, treat business unit leaders like internal customers. Be responsive to their needs and be a sponge when they express challenges.

IT professionals

The IT department is involved even if the GRC technology does not require programming or local support. A GRC program uses software, so IT is involved by default. GRC technology automates and streamlines GRC processes, so it is helpful to have friends in IT during configuration.

Employees

Employees play a critical role in the success of a GRC program. They follow policies and procedures, report issues and concerns, and can support a risk-aware culture. Training and events like lunch-and-learns can help employees feel a part of a major initiative underway at their company. The visibility of the GRC program can generate a groundswell of support.

External stakeholders

External stakeholders like regulators and auditors may provide requirements that must be incorporated into the GRC program. These two stakeholder groups are on the front lines for reviewing and assessing the program's effectiveness. Modernizing a GRC program is integral to being operationally sound. Regulators and auditors excel at stress tests.

Effective communication and collaboration with these stakeholders are essential for modernizing a GRC program.

Challenges encountered in modernizing a GRC program

Building bridges with stakeholders will make perfect sense after reviewing the likely challenges faced when modernizing a GRC program. A stakeholder can remove a roadblock, play devil's advocate, serve in the test group, shake down the program, and countless other ways of making the program invaluable.

Here are frequent challenges organizations may face when modernizing their GRC program:

Lack of resources

Modernizing a GRC program takes a significant investment of time, money, and resources. Organizations may struggle to allocate the necessary resources and budget for the effort. This is where the GRC champion earns their stripes, convincing decision-makers to fund the program to meet goals.

Resistance to change

Humans are hardwired to resist change. For many, it is the fear of the unknown. Employees may resist modernization, particularly if they have been accustomed to existing GRC processes and procedures. As you educate and communicate program benefits, keep the adoption cure in mind. The adoption process starts with innovators and early adopters, followed by the early/late majority and then laggards. Winning people over to a cause starts slow and then grows over time and with repeated effort.

Siloed GRC functions

For companies organized by departments, it is understandable that GRC functions, like risk management, compliance, and internal audit are also siloed within an organization. Point solutions take advantage of this and reinforce an organized department structure.

A Forbes 2022 State of Supply Chain survey found 76 percent of executives "pointed to disparate silos of materials data and lack of knowledge as possible hurdles to a digitally transformed approach to materials management."

A modern GRC program integrates all GRC functions and connects departments and vendors—the entire enterprise. It is a holistic view stakeholders must be open to and ready to have it work for them.

The complexity of regulatory requirements

Regulatory requirements are constantly evolving with new regulations and updated ones. For example, in Europe, the Digital Operations Resilience Act (DORA) is a new regulation focused on strengthening the IT security function of financial entities. Keeping up with these changes can be challenging. The GRC team must be thorough in their procurement process to choose GRC technology that can handle the complexity of regulatory requirements.

Data quality and availability

GRC programs rely on accurate and timely data, which may be difficult to obtain, particularly if data is siloed or stored in disparate systems. If the GRC team has data quality and availability issues, raise this issue as you interview technology vendors. Keep IT looped into these conversations. Your GRC software should be able to pull data from disparate systems.

Lack of executive buy-in

Without senior management, gaining the necessary resources and funding to modernize the GRC program is nearly impossible. A lack of executive buy-in is the kiss of death for any organizational change. Find your champion and secure executive buy-in as early as possible.

Limited technology capabilities

Limited capabilities define your company's current GRC technology, whether it is an in-house solution, a point solution, spreadsheets, or a less capable GRC platform. Your modern GRC program, rich in capabilities and able to automate and streamline GRC processes, will be a game changer.

Overcoming these challenges requires a strategic and collaborative approach that involves engaging stakeholders across the organization, aligning the GRC program with the organization's overall strategic goals, and leveraging advanced GRC technology.

The call for governance

Businesses must stay on top of everything—compliance, regulations, and risks. It is governance, the neglected G in GRC. Governance occurs when the GRC team performs at a high level, and signs are everywhere. Regulation changes are processed long before the deadline. Employees follow a code of conduct that significantly lowers the risk of adverse events. IT incidents happen less often but are contained and triaged. Senior management and the board are pleased when reviewing reports and dashboards.

Following principles of governance is practical and logical. It allows organizations to be proactive rather than reactive, and to see the value of long-term versus short-term stop-gap measures. Governance is made possible with the right tech platform that frees up the company to pursue goals with ethics.

> "It is critical to break these silos down, disseminate knowledge, and raise the collective maturity level of everyone together."

7-point checklist for evaluating solution providers

Technology plays a critical role in modernizing a GRC program. Get it wrong and lose time and waste resources using software that does not operate as your company does. Get it right, and the program will thrive and make a difference in helping move the organization forward. To ensure the latter happens, here is a 7-point checklist for evaluating software vendors. The more yeses, the better the fit for helping modernize your company's GRC program.

1. Does the software deliver broad-based GRC capabilities?

□ YES □ NO

Unlike point solutions that focus on an aspect of GRC like audit, GRC technology that modernizes your program should deliver an integrated approach to governance, risk, and compliance. The solution should equip users to comply with regulations and manage all types of risk.

2. Does the software vendor offer a path to expand based on needs?

□ YES □ NO

Your organization may require starting with one use case and succeeding before expanding elsewhere. Look for GRC software that offers a modular or step-up approach. David Young, who manages Panasonic Energy's business continuity program, recommends selecting a vendor who appreciates your vision, works with you, and offers a path to get there.

3. Does the software come ready to work out of the box or require customization?

□ YES □ NO

Some GRC software programs talk up working right out of the box. Other providers tout customization, but will the customization delay using the solution or hurt adoption among users? A nice alternative is a pre-configured solution with low or no code alterations.

4. Does the software provider have use cases like yours?

□ YES □ NO

There is comfort in knowing other companies with similar demands as yours are experiencing good outcomes from using the software. Look also for future use cases that might impact your program.

3. Does the software provider have professional services if needed?

□ YES □ NO

Some organizations need more assistance with integration. It is not required but a nice-to-have if your company needs a team on the ground to help with the startup phase.

4. Does the software provider have a history of innovation?

□ YES □ NO

Look for firsts and milestones in the software provider literature. Do they have a reputation for bringing out new features and capabilities? The software provider is your technology partner. The expectation is that they are constantly adding value by delivering something new and exciting every quarter, every year, whatever your measuring stick.

5. Does the software provider have an education and training arm?

□ YES □ NO

Education and training are often overlooked in software procurement. Think beyond user training for new software. Training should also be available to help employees adhere to the code of conduct, for example, or on how to be better equipped to spot cyber phishing attempts.

IT IS TIME TO MODERNIZE

If you have made it to the end of this whitepaper, it is safe to assume you see a need at your organization to modernize your GRC program. The business world is changing, and your company must modernize to keep current, operate more efficiently, and be resilient to whatever challenges come.

If not now, when? If you need help, visit SAI360.com.

Interested in learning more about SAI360's solutions for Modernizing Your GRC Program?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360

RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle. Visit www.sai360.com.