Galvanize

9 STEPS to IT Audit Readiness

Using Data Automation for Exceptional Performance and Oversight

Table of Contents

IT audit readiness 3

01 Identify and assess IT risks 6

02 Identify controls 8

03 Map controls to a master control framework library 10

04 Plan, scope, & stress-test micro risks with controls 12

05 Assess effectiveness of existing controls 14

06 Capture, track, & report deficiencies 16

07 Monitor & automate controls testing 17

08 Flag exceptions, review, investigate, & remediate 19

09 Ongoing improvement of control & monitoring processes 21

Bonus Step: Predictive IT risk trending 23

Bonus Step: Integrate IT risk management processes into enterprise risk management 24

IT audit readiness: It's a win-win-win 26

IT audit readiness

The global IT risk & regulatory environment is increasingly complex. And to make things more confusing, there's an unprecedented number of business devices, systems, & data—creating even more ever-changing risks.

We've outlined nine key steps to make your risk management and compliance activities smarter, quicker, and less resource-intensive. Follow the steps and you'll be able to better manage and reduce IT risks, reduce the complexity and pain of IT management, and start contributing better insights to executive management.

THE CHALLENGES OF TODAY'S IT MANAGER

Depending on your industry and region of operations, there's an "alphabet soup" of compliance regulations and frameworks to deal with, like SOX, OMB A-123, PCI, GLBA, HIPAA, COBIT, COSO, ISO, and SSAE 16 SOC 1. Auditors and compliance specialists—both internal and external—look to the IT department to identify control issues.

This creates a huge amount of work for the often limited resources of the IT team. However, there's a very real risk that a data security breach or critical IT system failure could result in major damage to the organization.

Given all of these responsibilities, the idea of achieving and maintaining a state of IT audit readiness may seem like a pipe dream. But there are processes that can be put in place to result in up-to-date and meaningful risk assessments, well documented and managed controls, and minimal negative findings from audits. The problem is that getting organized so audits are not a dreaded occurrence can be difficult.

Like many business functions, implementing the right technology can mean the difference between success and failure. Some organizations try to manage their IT risk, controls, and compliance processes with generic tools and technologies—or ones that are simply not made for the job. You're way more likely to transform how IT controls and compliance processes are managed when you implement technologies that are purpose-built. As you make your way through these nine steps, you'll also see that we've included a technology checklist for each one so you can be sure you've got the right tools for the job.

Why does IT need to be audit-ready?

While the long list of regulatory and internal compliance requirements may seem like an exercise in rule-making and bureaucracy, there's a reason why they exist. Regulatory and internal compliance requirements protect the organization, help it achieve its goals, and protect the public and third parties.

This obviously has huge relevance to the world of IT, given the fact that most businesses are now entirely dependent upon IT systems for daily operations and achieving their overall strategic objectives. When things go wrong in IT, the consequences can be disastrous—as past events at companies like Target and Sony have shown us.

The goal of audit readiness initiatives is to make things work better. Audit readiness means that controls—including IT-related controls—become more effective, and financial reports are more reliable and accurate.

As an IT manager, you need to manage IT risks; efficiently deal with an IT security, control, or compliance audit; and avoid surprises in a report of audit findings.

If you can spend less time dealing with audits by always being ready, you'll have way more time available for mission-critical work in infrastructure and business system upgrades.

GATHER YOUR PEOPLE

Process and technology are two key parts of the equation. The third essential component is people. No audit readiness initiative can succeed if people don't understand why you're doing it, or if they're not prepared to buy into the objectives and activities.

It often makes sense to start by putting together a cross-functional or multi-disciplinary team to help design and drive the process. Since IT connects with so many different aspects of the organization, this likely means gathering expertise with representation from functional areas including financial controls, operations, internal audit, and roles within IT itself (e.g., security and data specialists).

And finally, make sure you have leadership support for the objectives of audit readiness, and someone who can help overcome any obstacles that might pop up.

Now you're ready to get started.

01

Identify and assess IT risks

Start with the risks that have the most strategic impact, including regulatory, operational, and emerging risks. This step is critical and at the core of any risk management process.

To identify and build your risk universe, first classify risks by impact. Some examples:

- **Major impact:** Cybersecurity failure leads to theft of customer database; new ERP system implementation failure.
- **Medium impact:** Fines from failure to comply with European data privacy regulations.
- **Low impact:** Employee fraud committed by use of super ID access.

Next, link your risks to the potential impact they would have on achieving your organization's overall strategic objectives. Remember that risks should always be:

- Quantified in terms of potential financial or other impact
- Assessed in terms of probability
- Ranked relative to other risks.

Risk assessment should be an ongoing process throughout the year, as it depends on the existence and effectiveness of controls intended to mitigate the risks.

NEW AND EMERGING RISKS

This step also includes an ongoing process of identifying new and emerging risks. This means staying on top of the ever-changing collection of IT regulations and compliance requirements.

This process requires a mixture of critical thinking skills and knowledge, and where practical, data analysis to help you monitor changing risk trends and outliers. Typical examples of datasets to indicate potential IT risks include network and database access logs, authorization tables, and file transfer logs.

CHALLENGES AT THIS STAGE

- Having confidence that your range of risks and regulatory requirements are comprehensive enough.
- Normalizing and assessing risks identified in different areas using conflicting methods and technologies.
- Staying current with the collection of IT regulations and compliance requirements.
- Gaining insights into new potential risks without analysis technology.

TECHNOLOGY REQUIREMENTS

- Rank and report risks by multiple criteria.
- Compare strategic risks relative to other risks.
- Link risks to strategic objectives and the entities they impact.
- Link risks to relevant regulatory and compliance requirements.
- Link risks to IT, risk, or regulatory and compliance frameworks.
- Record risk descriptions, categories, assessment ratings, quantification, and probability.
- Access and analyze a wide range of system and data files.
- Generate statistics and indications of anomalies and outliers.
- Provide visual analysis to help indicate trends and risk factors.

02

Identify controls

Risks that you identified in step one should now be matched with controls that prevent or reduce the chances of risk occurring.

Not all risks will necessarily have a corresponding control. You may need to accept the risk of a negative event occurring, usually when the cost of an effective control is expected to exceed the potential loss. During this process, you should consider the corporate risk appetite, as defined by senior management.

A FEW CONTROL EXAMPLES INCLUDE:

- Firewalls to prevent external systems access.
- Access and authorization tables to restrict user capabilities.
- Methodologies to reduce likelihood of failure in new system development projects.

At this stage, controls and risk reduction procedures (currently in place or to be implemented) are defined and documented. Consideration can be given to estimating the cost of implementing and maintaining a control. The description and documentation of controls should be sufficiently detailed to support independent audit and review.

CHALLENGES AT THIS STAGE

- Like step one, it can be painful to find and review all of the mitigating controls from a wide range of sources across the organization.

TECHNOLOGY REQUIREMENTS

- Record controls in a centrally managed, re-usable framework with sufficient detail to support audit and review processes (e.g., support text, graphics, flowcharts).
- Map controls to risks (both strategic and micro).
- Enable easy change management to update controls centrally, and cascade changes out to IT project templates, as well as for internal or external auditors to review.

03

Map controls to a master control framework library

Closely connected to the process of identifying mitigating controls is that of mapping them, where possible, into an overall control framework library. This provides a structure to the relationships between controls, control owners, and regulatory requirements.

Third-party control frameworks are maintained independently and are updated to reflect new and changing regulatory requirements, as well as best practices.

CHALLENGES AT THIS STAGE

- Having confidence that your range of risks and regulatory requirements are comprehensive enough.
- Normalizing and assessing risks identified in different areas using conflicting methods and technologies.
- Staying current with the collection of IT regulations and compliance requirements.
- Gaining insights into new potential risks without analysis technology.

TECHNOLOGY REQUIREMENTS

- Rank and report risks by multiple criteria.
- Compare strategic risks relative to other risks.
- Link risks to strategic objectives and the entities they impact.
- Link to relevant regulatory and compliance requirements.
- Link to IT, risk, or regulatory and compliance frameworks.
- Record risk descriptions, categories, assessment ratings, quantification, and probability.
- Access and analyze a wide range of system and data files.
- Generate statistics and indications of anomalies and outliers.
- Provide visual analysis to help indicate trends and risk factors.

04

Plan, scope, & stress-test micro risks with controls

Controls are designed to address risks at many levels and they can become increasingly detailed (micro) to reflect specific possibilities and vulnerabilities. Part of effective risk management is knowing when it's reasonable to accept a particular risk, and how far to go in implementing a control.

At some point, the costs of reducing risk can outweigh the likely extent of damage. But to manage this effectively, you'd need to consistently assess the extent of risks relative to the controls that are designed. It also means being able to communicate the overall impact of accepted risks, as well as of control failures to senior management.

CHALLENGES AT THIS STAGE

- Quantifying the risk assurance that IT provides the organization.
- Taking appropriate action if a micro risk is assessed at high impact and high likelihood.
- Understanding the risk posed to an organization if a control fails.
- Inconsistencies in data and huge efforts to consolidate and report on overall risk and control picture.

TECHNOLOGY REQUIREMENTS

- Assess and weigh the effectiveness of IT controls that are designed to mitigate micro level risk.
- Collect, blend, and normalize data from multiple sources.
- Quantify risk assurance by control, control objective, and IT project.

05

Assess effectiveness of existing controls

A major part of audit readiness is making sure that controls are actually working as intended. Data analysis is key when it comes to assessment of control effectiveness, so you can query and examine entire datasets to see what happened during a defined period.

Controls can also be self-assessed by control owners through regular questionnaires. In some cases, the activities of control owners can be part of a certification process that contributes to senior management's sign-off on the implementation of effective control systems.

Controls assessments are usually performed on a periodic basis. However, it should be considered in conjunction with step six, in which key controls are monitored using ongoing automated techniques.

CHALLENGES AT THIS STAGE

- Determining if the controls are actually working or not.
- Determining if your controls are being ignored or circumvented.
- Keeping track of who is responsible for which controls and making sure they don't drop the ball.

TECHNOLOGY REQUIREMENTS

- Automate and analyze surveys and questionnaires.
- Visualize aggregated data across many tests to illuminate outliers.
- Test for a wide range of types of control breakdowns.

FOR MORE ON HOW WE CAN HELP, VISIT WEGALVANIZE.COM

06

Capture, track, & report deficiencies

When control deficiencies are identified, it's important to respond quickly to fix and improve the control process. In many cases, recurring data analysis can be used to strengthen controls or to create an additional layer of control.

For example, if controls over access to sensitive data don't appear to be fully effective, regular data analyses can be run to identify instances of risky access. By identifying this early on, it can be dealt with before it escalates into a major problem.

CHALLENGES AT THIS STAGE

- Making controls truly effective.
- Resistance from people who "just want to get the job done" and bypass controls.

TECHNOLOGY REQUIREMENTS

- Ability to centrally track responses to identified control deficiencies.
- Identify risky transactions according to a wide range of testing criteria.

07

Monitor & automate controls testing

All of the steps in the audit readiness process are important, but monitoring adds a critical component, giving you an up-to-date assessment of the effectiveness of existing IT risk management and control activities. Plus it can help to identify indicators of new risks for which no controls are currently in place.

In almost every case, data analysis is effective in testing controls and assessing risks. Consider running similar forms of data analysis on a regular ongoing basis—daily, weekly, monthly—whichever makes the most sense for you and your organization.

MONITORING ANALYTICS CAN BE APPLIED TO MANY IT ACTIVITIES

- Use of admin and special systems access.
- Segregation of duties.
- Control overrides/changes.
- Firewall changes.
- Critical data changes.
- Network logs.
- Physical access logs.

CHALLENGES AT THIS STAGE

- Quantifying the risk assurance that IT provides the organization.
- Taking appropriate action if a micro risk is assessed at high impact and high likelihood.
- Understanding the risk posed to an organization if a control fails.
- Inconsistencies in data and huge efforts to consolidate and report on overall risk and control picture.

TECHNOLOGY REQUIREMENTS

- Assess and weigh the effectiveness of IT controls that are designed to mitigate micro level risk.
- Collect, blend, and normalize data from multiple sources.
- Quantify risk assurance by control, control objective, and IT project.

08

Flag exceptions, review, investigate, & remediate

The previous step, monitoring, uncovers indicators of potential problems, signaling that a control is not working effectively or that a specific risk is increasing.

These red flags need to be investigated and resolved by individuals familiar with the underlying process and the controls that are meant to be in place.

During this process, often referred to as exception management or issues management, keep in mind that some red flags will be false positives, while others may indicate control breakdowns that require action.

This action could include addressing the problem that occurred (e.g., dealing with an employee's unauthorized access to sensitive data) or fixing the control to reduce the chance of the problem happening again.

Many false positives can be eliminated by adjusting testing and analysis configurations so that non-risky items are not reported.

CHALLENGES AT THIS STAGE

- Issues management can be overwhelming, especially when addressing the extremely wide range of IT regulatory and compliance requirements.
- Large volumes of false positives can lead to overlooking indicators where there's an actual control problem.
- Large volumes of exceptions generated across multiple systems can be resource intensive and difficult to manage.
- If control weaknesses and risky transactions are identified but not addressed, management will be unaware of the extent of problems.

TECHNOLOGY REQUIREMENTS

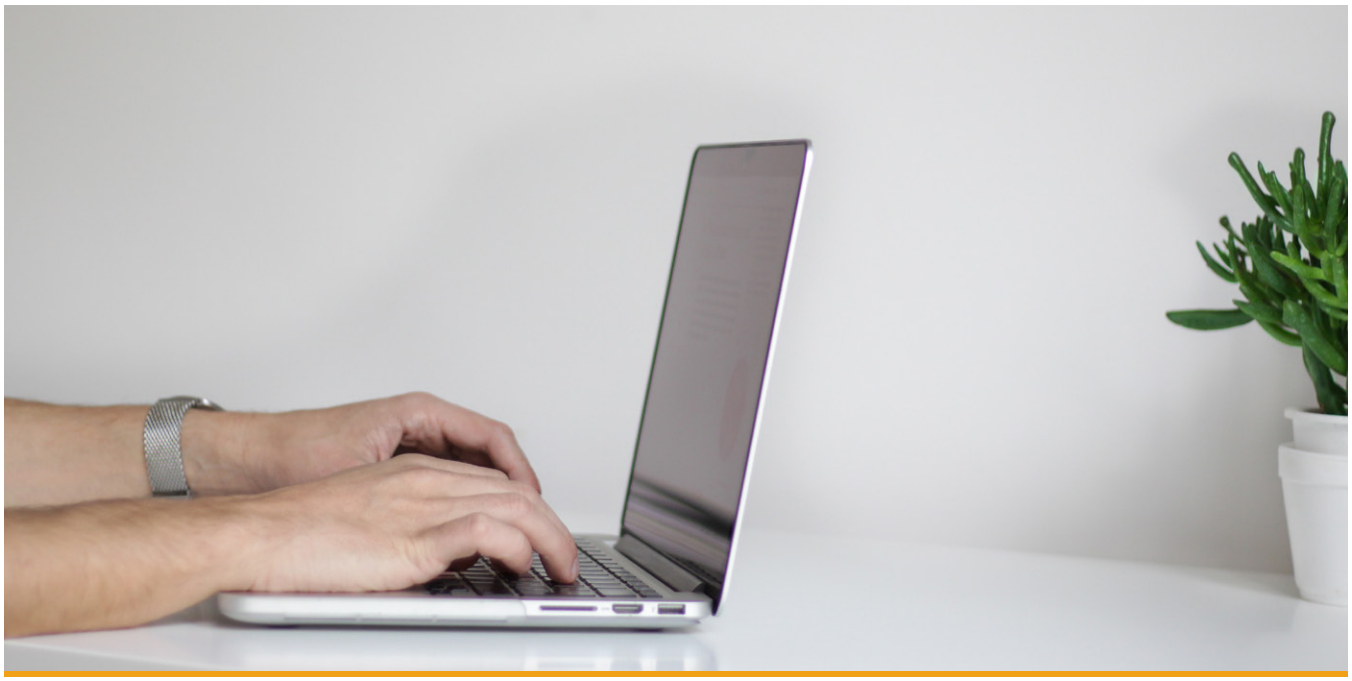
- Adjust testing procedures so no-risk or low-risk activities aren't reported as exceptions.
- Easily establish and modify workflow procedures.
- Automatically escalate exceptions and risky transactions for senior management review.
- Report the status of exception management activities.
- Report the extent of existing risk based on the results of investigating exceptions.

09

Ongoing improvement of control & monitoring processes

Over time, risks are reduced and the entire control process improves through a continuous cycle of testing, monitoring controls, and addressing exceptions issues.

Now, the likelihood of adverse audit findings has been greatly reduced so that when IT is subject to scrutiny by audit and compliance functions—internal or external—there won't be any surprises.



CHALLENGES AT THIS STAGE

- It can be difficult to manage all the moving parts and stay focused on the most significant risks and important controls.
- Using manual methods or a range of home-grown systems, often based on spreadsheets, is time-consuming and not particularly effective.

TECHNOLOGY REQUIREMENTS

- Support all the stages in the risk/control assessment and monitoring process.
- Create reports that provide insights into the overall state of audit readiness across the entire IT infrastructure.

Congratulations! You are now in that highly coveted state of audit readiness!

↳ FOR MORE ON HOW WE CAN HELP, VISIT WEGALVANIZE.COM

BONUS STEP

Predictive IT risk trending

You've achieved audit readiness—now it's time to take it to the next level. Move beyond just making sure IT control systems are working properly and start reporting the results of the entire process.

Using dashboards and heat maps, you can provide visual and quantifiable evidence of the analysis and testing procedures performed, together with the results. These high-level reports show trends over time for risk/control issues, categorized by criteria like region, business function, or manager. Plus you'll be able to spot areas that are most likely to develop into problems and require more immediate action before a negative event occurs.

CHALLENGES AT THIS STAGE

- It's a lot of work to collect information from various sources across the organization and present it in a way that makes sense at both a technical level and for senior management.
- It's difficult to provide context for risk and control issues, and the nature and extent of monitoring and testing activities, without specialized technology.

TECHNOLOGY REQUIREMENTS

- Accumulate data on nature and volume of testing activities, results, and follow-up responses.
- Report comprehensively on the status of activities performed, including the quantified extent of tests, results, and responses.
- Link testing and response data to underlying risk and controls.

BONUS STEP

Integrate IT risk management processes into enterprise risk management

Sometimes the primary goal of achieving IT audit readiness is so you can better manage departmental control & compliance responsibilities. In other cases, it makes sense to look at IT's processes for risk management, control, and compliance in the context of wider enterprise risk management activities.

By taking a broader approach, corporate or organizational senior management is able to look at IT risks alongside those of other key functional areas and risk categories.

Another benefit of taking a more widely integrated approach is that it's easier to show how risks and controls are interrelated. IT risks rarely exist in isolation, but should often be considered alongside risks and controls within specific financial and operational systems.

CHALLENGES AT THIS STAGE

- Different entities involved in risk management and control within an organization may assess risks and control issues in different ways, making it difficult for management to obtain a meaningful comparative picture.
- Organizations may use a variety of technology and approaches for assessing risk/control issues and audit readiness in different areas.
- Creating a comprehensive view of audit readiness across a range of functional areas isn't easy.

TECHNOLOGY REQUIREMENTS

- Address a wide range of different audit, risk, and control activities in different organizational areas.
- Integrate with other risk and control management technologies.

IT audit readiness: It's a win-win-win

And that's why it's worth doing right & employing the right technology.

These nine steps will help you transform what can often be a painful, frustrating, and inefficient process into something that requires far less effort and significantly reduces overall resource costs.

There are many technologies available to support the IT security and control process. But one of the greatest challenges is managing the entire process in a consistent way, to get a comprehensive view of the state of IT risk and compliance in a single place, with a range of technology capabilities that are designed to work together.

Galvanize's HighBond platform integrates your IT framework, giving you the structure you need to make sure your IT security environment is robust, well-governed, and aligned with strategic risks.

KEY BENEFITS

- IT audit readiness benefits the IT function as well as the organization overall.
- You know that your IT risks are truly being well-managed.
- Regulators and auditors are way happier, with fewer negative things to report.
- IT management improves the insights and assurance they provide to the executive suite.
- The likelihood of an IT control or compliance issue causing significant damage to the organization is significantly reduced.

About the Author

John Verver

CPA CA, CMC, CISA

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.