THE ULTIMATE GUIDE TO IT AUDIT READINESS:

11 steps to winning back your time & reducing IT risk

acl™

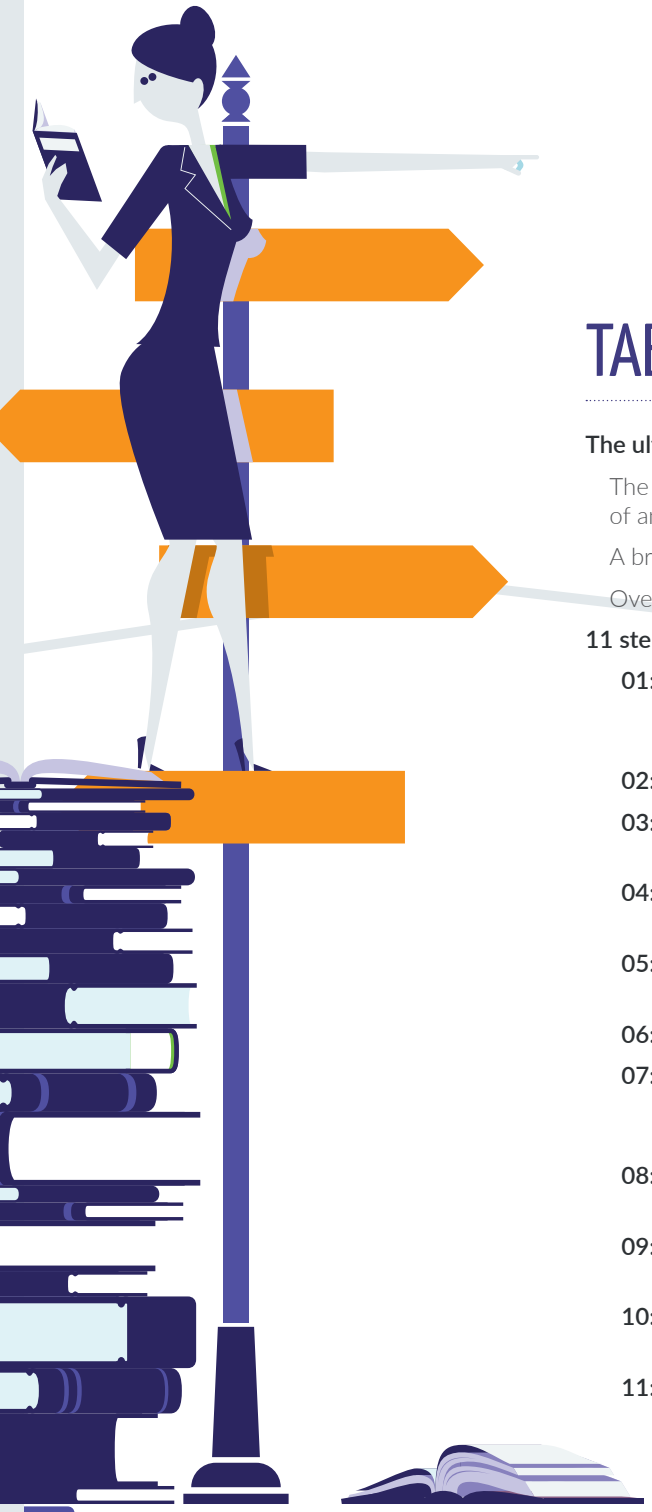


TABLE OF CONTENTS

The ultimate guide to IT Audit Readiness 3

The challenges and demands of a day in the life of an IT manager 3

A brief history of Audit Readiness 4

Overcoming the pain of IT compliance requirements. 5

11 steps to IT audit readiness 6

01: Identify and assess IT risks, starting with those that are strategic in impact, including regulatory, operational and emerging risks 8

02: Identify control objectives that will help mitigate IT risks . . 10

03: Map control objectives into a master control framework library 12

04: Plan scope and stress test micro risks within control objectives 14

05: Assess the effectiveness of existing controls. 16

06: Capture, track and report deficiencies to improve controls 18

07: Monitor! Automate testing of IT controls to free up IT resources and provide better IT risk coverage across the organization. 20

08: Manage issues by flagging exceptions, reviewing, investigating and remediating through issue lifecycle.. . . . 22

09: Ongoing improvement of control and monitoring processes = Audit Readiness 24

10: Define KRI metrics to run risk analytics for predictive IT risk trending 26

11: Integrate IT risk management processes into overall ERM . 28

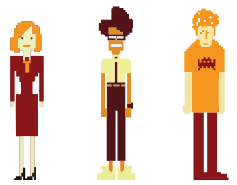
IT Audit Readiness: it's not just about audit.. 30

At-a-glance: IT Audit Readiness process 31

Conclusion 33

Quick-start: technology requirements for IT Audit Readiness . . . 34

About the Author: 36



THE ULTIMATE GUIDE TO IT AUDIT READINESS:

As if the job of an IT manager or leader was not already challenging enough, today's IT risk and regulatory environment is constantly increasing in complexity. Alongside this, there is an unprecedented proliferation of business devices, systems and data, creating more and ever-changing risks.

The challenges and demands of a day in the life of an IT manager

Depending on industry and region of operations, there is an "alphabet soup" of regulations and frameworks that require some form of compliance or adherence. Auditors and compliance specialists, both internal and external, come to the IT department checking to see whether there are issues of control and compliance with one or many of SOX, OMB A-123, PCI, GLBA, HIPAA, COBIT, COSO, ISO, SSAE 16 SOC 1, and a seemingly endless list of other acronyms. While this generates a huge amount of work for the IT team's often limited resources, at the same time there are very real risks that a data security breach or critical IT system failure could result in major damage to the business or organization overall.

How to deal with all of this? The whole concept of being able to achieve and maintain a state of "IT Audit Readiness" may seem like a pipe dream. But what if processes could be put in place that result in up-to-date and meaningful risk assessments, well documented and managed controls and minimal negative findings from audits? While it may well already be on your radar to get things organized so that audits are not a dreaded occurrence, the reality is that this can be difficult to achieve.

As with many critical business functions, implementing the right technology can make all the difference between success and failure. Some organizations try to manage their IT risk, controls and compliance processes through generic tools and technologies, or ones that are simply not very good for the job. However, the chances are that those that achieve the greatest success have implemented technologies that are designed for the purpose—and transform, for the better, the ways that IT controls and compliance processes are managed.

This eBook outlines 11 key steps, incorporating aspects of people, process and technology, to make your risk management and compliance activities work in a way that is smarter, quicker, simpler and less resource-intensive—to help you to better manage and reduce IT risks. Not only will these steps help to reduce the complexity and burden of IT management, but help you to contribute more and better insights to executive management around the nature of IT risks.

A brief history of Audit Readiness

The concept of "audit readiness" started in the U.S. Federal Government, a body in which there had historically been no requirement for independent audits of financial statements. All of a sudden a range of government entities had to struggle with implementing processes that would help to lead to a clean audit opinion. After a while, it became apparent that while audit readiness was a goal that needed to be achieved, the real issue was not about keeping auditors happy and getting clean audit reports. The result of audit readiness initiatives was that many things just worked better. Controls, including those that are IT-related, became more effective and financial reports became more reliable and accurate.

Comparable benefits are obtainable outside of the public sector. Although the long list of regulatory and internal compliance requirements may at times seem like an exercise in rule-making and bureaucracy gone mad, there is a reason why they exist.

Ultimately, they make good sense in terms of protecting the organization, helping it to achieve its goals, as well as protecting the public and third parties. The challenge, and perhaps one of the most important things to be able to do from a risk management perspective, is to put things into context. This means really understanding the importance and impact of different risks, as well as ways to respond to them in a way that focuses efforts and avoids inefficient, resource-consuming activities that really are of benefit to no one.

All of this has huge relevance to the world of IT, particularly given that virtually every business and organization is now entirely dependent upon IT systems for daily operations and for achieving their overall strategic objectives. When things go wrong in IT, the consequences can be disastrous—as recent events at major corporations such as Target and Sony have proven.

As an IT manager you know this already. What you probably want to know is how to make sure you are really managing IT risks well, are prepared to deal efficiently with any audit of IT security, control or compliance requirement, as well as having no surprises in a report of audit findings. If you can spend less time actually dealing with audits by always being "ready," you will have more time available for mission critical work in infrastructure and business system upgrades.

Overcoming the pain of IT compliance requirements

Since IT is at the core of so many different aspects of corporations and government organizations, it is not surprising that there are so many regulatory and other compliance requirements, both internally and externally driven, that are focused on IT. Just dealing with an organization's own risk and control framework and the multiple sub-categories of application controls and IT general controls can be a hugely resource-intensive challenge. Then add in the demands from regulations and standards such as SOX, GLBA, FISMA, PCI DSS, or ISO, as well as the industry specific compliance requirements such as those for HIPAA, EFTA, ITC or HSA, and things start to get really interesting!

Dealing with internal process management can also be a very daunting task. Just getting control owners to self-assess controls and provide dependable responses can seem like herding particularly awkward cats! Then when the external regulators and auditors arrive, the demands get even tougher, with having to address seemingly endless questions and produce a myriad of compliance reports and forms of documentation. All of this can involve countless hours of time and scarce resources.

Even though every step may not apply to your organization or meet your most urgent needs, we hope they give you ideas about how the combination of people, process and the right technologies can make a real difference in what may well be one of the larger pain points in your world of IT management.

11 STEPS TO IT AUDIT READINESS

Here are 11 primary stages in the process of implementing more effective systems for risk management, control and compliance that will lead to a state of audit readiness. In each stage we will describe what is involved in the process, as well as outline the technology requirements.

But, first things first...gather your people

Of course, process and technology are only two parts of the equation. The third essential component is people. No audit readiness initiative can succeed if people do not understand or are not prepared to buy into the objectives and activities involved.

Although the topic of people roles, responsibilities and resources is important throughout the audit readiness process, it often makes sense to start by putting together a cross-functional or multi-disciplinary team to help design and drive the process from the beginning. Since IT connects with so many different aspects of the organization, this likely means gathering expertise with representation from financial controls, operations and internal audit, as well as roles within IT itself, such as security and data specialists.

Along with all of this, there also needs to be leadership that supports the objectives of audit readiness and is prepared to help overcome any obstacles that arise.

Now, let's get started!

1 IDENTIFY AND ASSESS IT RISKS, STARTING WITH THOSE THAT ARE STRATEGIC IN IMPACT, INCLUDING REGULATORY, OPERATIONAL AND EMERGING RISKS

In 2013 there were

29,000

regulatory changes recorded in a single year. That's a whopping

125/day

Of course, not all of these will relate to every commercial or government agency, but it is a significant challenge to keep on top of regulatory changes and then to successfully apply relevant ones to an IT control framework.

This stage is the critical one—and is at the core of any risk management process. It involves building a "universe" of risks, set as far as possible in the context of key strategic risks. Risks can range from those with **major impacts** (e.g., cyber security failure leads to theft of entire customer database, new ERP system implementation failure), to the relatively **low impact** (e.g., employee fraud committed by use of super ID access) and **much in between** (e.g., fines due to failure to comply with European data privacy regulations).

As much as possible, risks should be:

(a) **quantified** in terms of potential financial or other impact

(b) **assessed** in terms of probability

(c) **ranked** relative to other risks

Risks should also be linked to the potential impact on achieving overall strategic objectives or government missions.

This stage also includes an ongoing exploratory process in which the objective is to identify new and emerging risks that may need to be included in the overall risk universe or repository of risks being monitored and assessed. It involves being on top of the ever-changing mass of regulations and compliance requirements that impact IT. The process is dependent upon a mixture of critical thinking skills and knowledge combined, where practical, with the use of data analysis to monitor changing risk trends, as well as outliers that indicate potential risks not previously considered. Typical examples of datasets to indicate potential IT risks include network and database access logs, authorization tables, file transfer logs.

Risk assessment should be an ongoing process throughout the year, as it also depends on the existence and effectiveness of controls that are intended to mitigate the risks (**see Steps 3-8**).

Things that can make this stage challenging:

- It is often hard to be confident that a comprehensive range of risks and regulatory requirements have been gathered and are considered in one place.
- If risks are identified in different areas using different methods and technologies it can be a painful process to accumulate and assess risks in a consistent way.
- Remaining current with the mass of regulations and compliance requirements for IT and related areas.
- Gaining insights into new potential risks, without using analysis technology, is a bit of a game of "you don't know what you don't know."

What capabilities need to be considered for this step? Technology checklist:

- ❑ Linking to IT, risk, or regulatory and compliance requirements frameworks
- ❑ Records risk descriptions, categories, assessment ratings, quantification, probability
- ❑ Ranks and reports risks by multiple criteria
- ❑ Compares strategic risks relative to other risks
- ❑ Linking to strategic objectives and the entities which they impact
- ❑ Linking to relevant regulatory and compliance requirements
- ❑ Accesses and analyzes a broad range of system and other data files
- ❑ Generates statistics and indications of anomalies and outliers
- ❑ Visual analysis to help indicate significant trends and risk factors

2 IDENTIFY CONTROL OBJECTIVES THAT WILL HELP MITIGATE IT RISKS

IT Hierarchy Influencing Control Objectives

IT Organization & Structure

- ☐ IT structure and management
- ☐ Agency or business unit/ geographical organization
- ☐ Strategy for managing technology and applications

IT Entity-Level Controls

- ☐ "Tone from the top" and culture
- ☐ Overall IT controls, risk assessments, communications and monitoring
- ☐ IT architecture
- ☐ Identify application and data owners

IT Process-Level Controls

- ☐ General IT processes
- ☐ Application and data owner controls (e.g., SoD, Logical Access)
- ☐ Configurable application controls

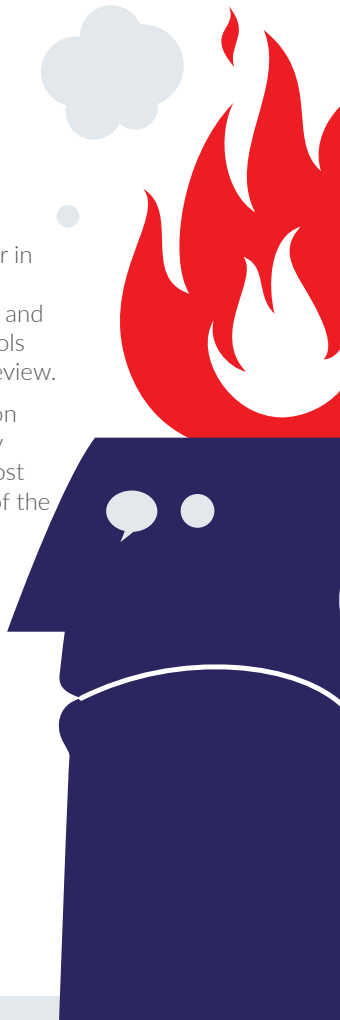
Every risk identified in **Step 1** should be considered in terms of the nature of a control that would prevent or reduce the chances of the risk occurring.

For example:

- 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 (that are either in place or need 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.

Not all risks will necessarily have a corresponding control. A decision may be taken to accept a risk of a negative event occurring, usually when the cost of an effective control is expected to exceed the most likely potential loss. During this process, account should be taken of the corporate risk appetite as defined by senior management.



Things that can make this stage challenging:

- As with Step 1, identification and review of a wide range of mitigating controls gathered from a wide range of sources across the organization can be a painful process.

What capabilities need to be considered for this step? Technology checklist:

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

3

MAP CONTROL OBJECTIVES INTO 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. These provide 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.

Things that can make this stage challenging:

- Maintaining visibility into current control structures
- Rapidly responding to changes and reflecting them throughout the control structures
- Managing the process manually and through spreadsheets becomes time-consuming and very difficult to maintain dependability

What capabilities need to be considered for this step? Technology checklist:

- Real-time and rapidly updated views of the entire IT control landscape
- Re-usable templates and frameworks
- Easy change management to cascade control updates across linked areas

4

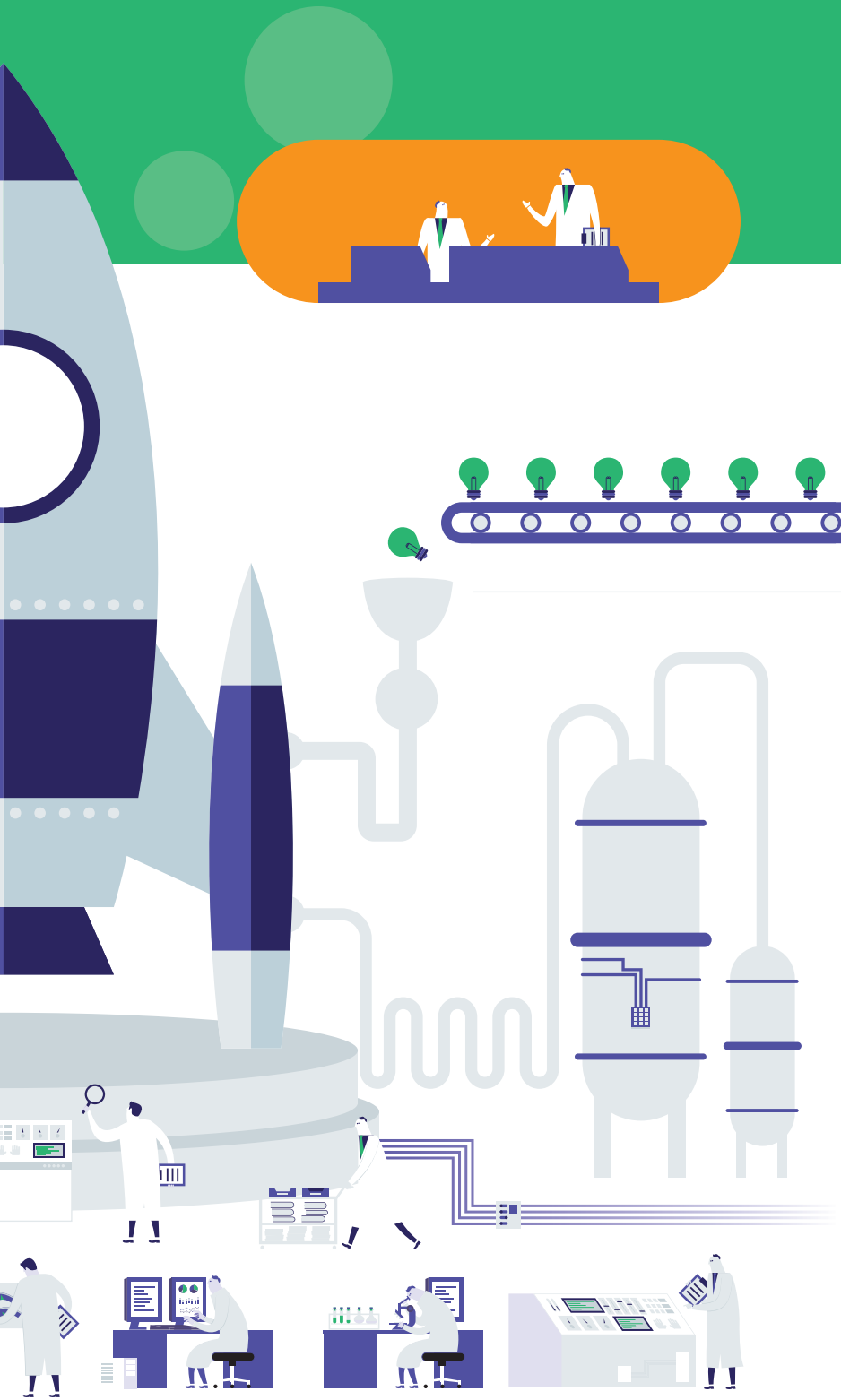
PLAN, SCOPE AND STRESS TEST MICRO RISKS WITHIN CONTROL OBJECTIVES

Controls are designed to address risks at many levels and become increasingly detailed (i.e., “micro”) to reflect specific possibilities and vulnerabilities. Part of effective risk management is knowing when it is 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 that could be caused. But to manage this effectively means being able 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.

Things that can make this stage challenging:

- How do you quantify the risk assurance that IT provides the organization?
- If a micro level risk is assessed at high impact and high likelihood, what does that mean? And if a control fails, what risk does that pose to the organization?
- Dealing with these issues through conventional processes and spreadsheets can easily result in inconsistencies, as well as large amounts of effort to consolidate and report on the overall risk and control picture.



What capabilities need to be considered for this step? Technology checklist:

- Ability to assess and weight the effectiveness of IT controls that are designed to mitigate micro level risk
- Quantification of risk assurance by control, control objective and IT project

5 ASSESS THE EFFECTIVENESS OF EXISTING CONTROLS

A key aspect of the audit readiness process is to determine that controls that are meant to be in place are actually working as intended. Assessment of controls effectiveness in many cases should be supported by the use of data analysis to examine entire datasets and test what has taken place during a defined period.

Controls can also be self-assessed by control owners, who regularly complete 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 systems of internal control.

This stage of controls assessment is usually performed on an occasional periodic basis. However, it should be considered in conjunction with Step 6 in which key controls are monitored using ongoing automated techniques.

Things that can make this stage challenging:

- This can be one of the most difficult but important steps stages in the process. Identifying the controls that mitigate risks is obviously important, but...
  - What if the controls are not actually working?
  - How do you know if they are being ignored or circumvented?
  - How do you know who has accepted responsibility for a control operating as intended?

What capabilities need to be considered for this step? Technology checklist:

- Data analysis tools and techniques designed to test for a wide range of types of control breakdowns
- Automated survey/questionnaire and response system
- Analysis of survey/questionnaire responses
- Visualization of aggregated data across many tests to illuminate outliers that may otherwise not appear to be problematic

6

CAPTURE, TRACK AND REPORT DEFICIENCIES TO IMPROVE CONTROLS

When control deficiencies are identified, it is important to respond—in a timely way—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 do not appear to be fully effective, regular analyses can be run to identify instances of risky access and dealt with before they escalate into a major problem.

Data Analysis TIP

Using data analysis to determine what has actually happened and to indicate whether there is a real problem resulting from control failures can be a uniquely effective way of compensating for a tendency to work around controls.

Things that can make this stage challenging:

It can be very difficult to make controls really effective. There is often resistance from people who "just want to get the job done" and bypass controls as something that get in the way and slow down the process.

What capabilities need to be considered for this step? Technology checklist:

- Central tracking of responses to control deficiencies that have been identified
- Specialized data analysis tools and techniques that identify risky transactions according to a wide range of testing criteria

7

MONITOR! AUTOMATE TESTING OF IT CONTROLS TO FREE UP IT RESOURCES AND PROVIDE BETTER IT RISK COVERAGE ACROSS THE ORGANIZATION

While all the stages in the overall audit readiness process are important, monitoring adds a critical component by:

- supporting an up-to-date assessment of the effectiveness of existing IT risk management and control activities
- looking for indicators of new risks for which no controls are currently in place

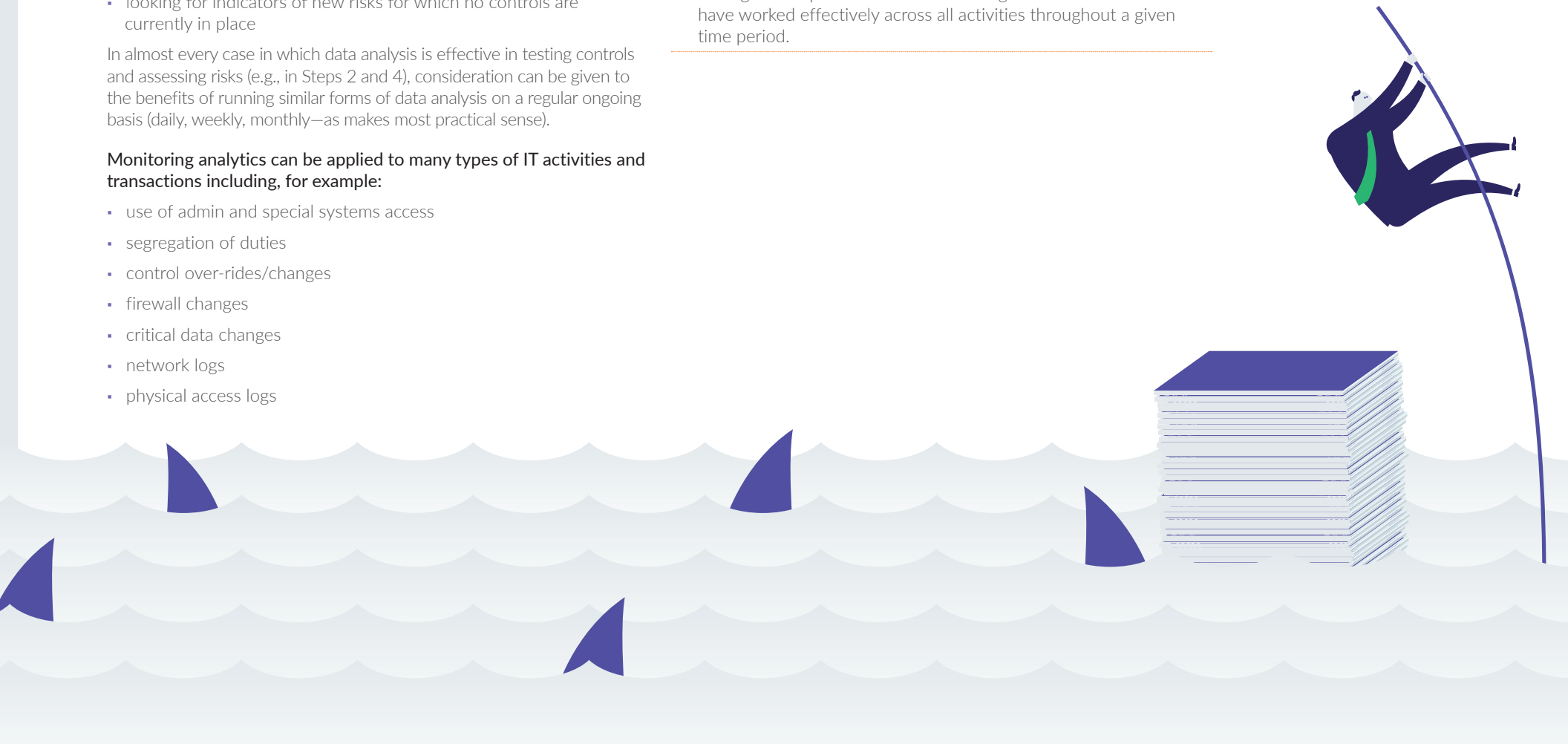
In almost every case in which data analysis is effective in testing controls and assessing risks (e.g., in Steps 2 and 4), consideration can be given to the benefits of running similar forms of data analysis on a regular ongoing basis (daily, weekly, monthly—as makes most practical sense).

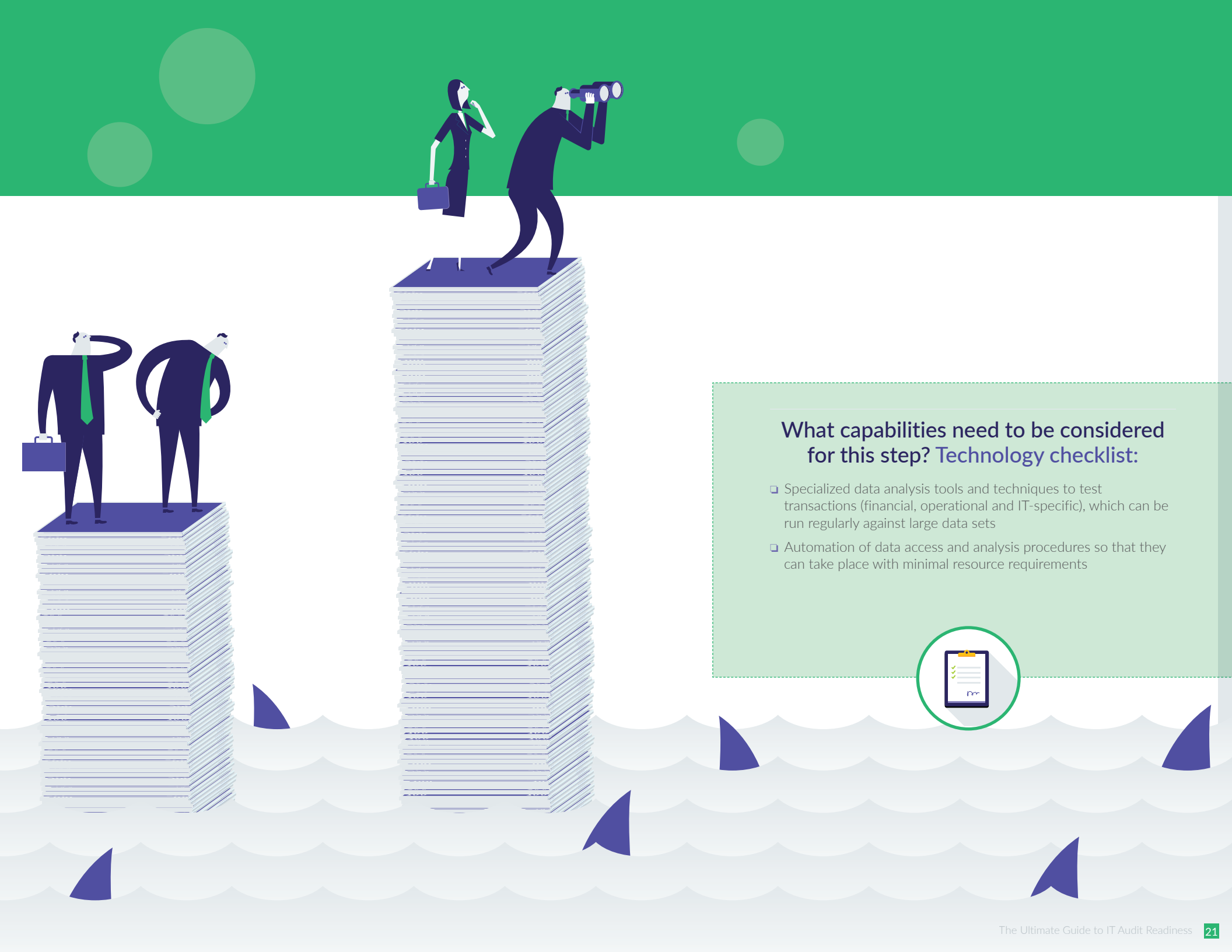
Monitoring analytics can be applied to many types of IT activities and transactions including, for example:

- use of admin and special systems access
- segregation of duties
- control over-rides/changes
- firewall changes
- critical data changes
- network logs
- physical access logs

Things that can make this stage challenging:

- The traditional approach to monitoring control effectiveness involves manual methods such as checking documentation and control procedure "walk-throughs." These forms of point-in-time testing do not provide assurance or insight into whether controls have worked effectively across all activities throughout a given time period.





What capabilities need to be considered for this step? Technology checklist:

- Specialized data analysis tools and techniques to test transactions (financial, operational and IT-specific), which can be run regularly against large data sets
- Automation of data access and analysis procedures so that they can take place with minimal resource requirements

8 MANAGE ISSUES BY FLAGGING EXCEPTIONS, REVIEWING, INVESTIGATING AND REMEDIATING THROUGH ISSUE LIFECYCLE.

The monitoring process results in 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 controls that are meant to be in place.

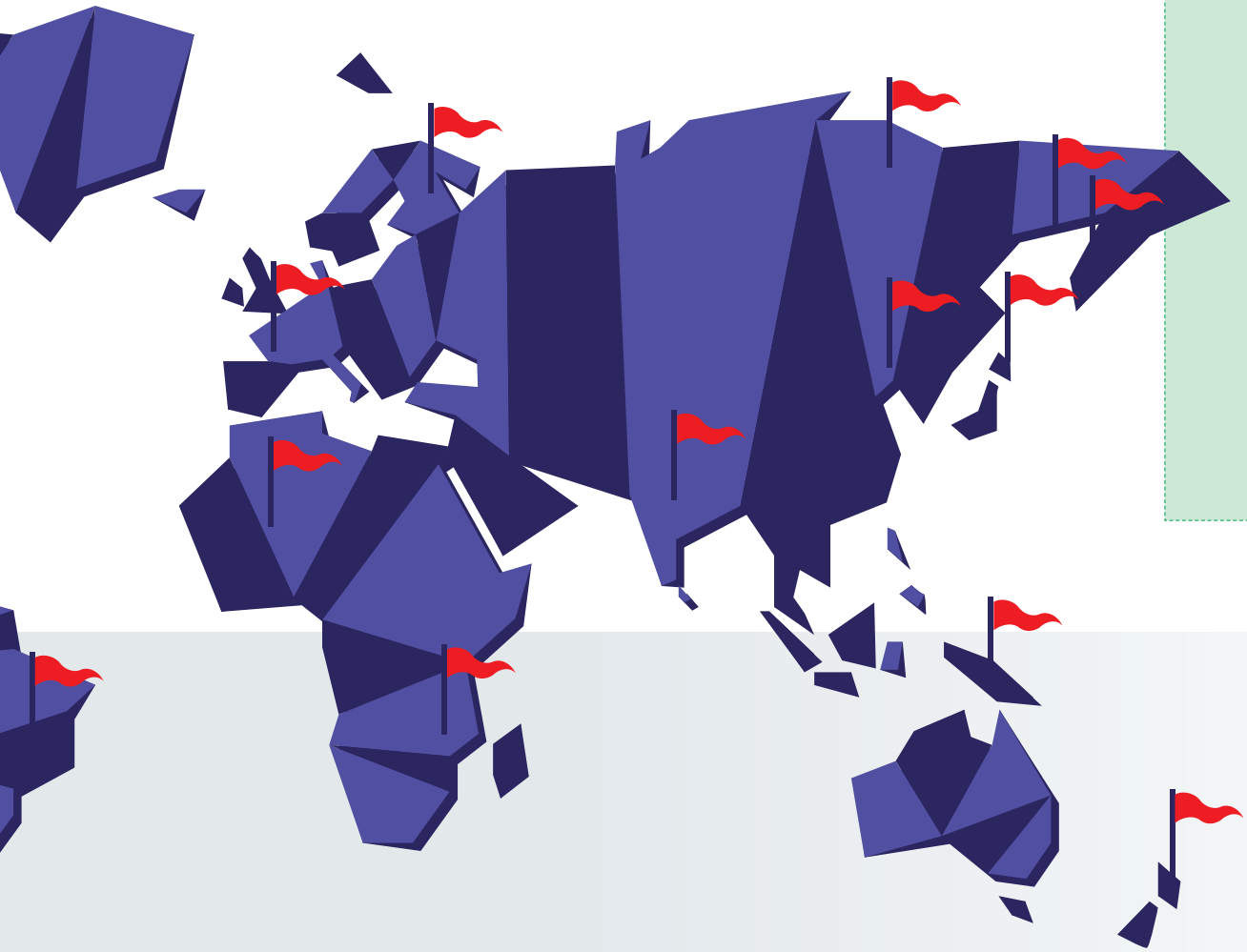
This process, often referred to as Exception Management or Issues Management, should take account of the likelihood that some red flags will be false positives, while others may indicate control breakdowns that need response in terms of:

- addressing the problem that occurred (e.g., deal with an employee's unauthorized access to sensitive data)
- fixing the control to reduce the chance of the problem re-occurring

Many false positives can be eliminated through adjustments to test and analyze configurations so that non-risky items are not reported.

Things that can make this stage challenging:

- Issues management overall can be an overwhelming task, particularly in terms of addressing the extremely wide range of regulatory and compliance requirements that impact IT.
- Being overwhelmed with large volumes of false positives can lead to individuals ignoring indicators that there is a real control problem.
- Dealing with large volumes of exceptions generated across multiple systems can be very resource intensive and difficult to manage.
- Control weaknesses and risky transactions are identified but not addressed. As a result, management is not made aware of the extent of problems.



What capabilities need to be considered for this step? Technology checklist:

- Ability to efficiently adjust testing procedures so that no-risk or low-risk activities are not reported as exceptions
- Workflow procedures that are easy to establish and modify
- Automatic escalation of exceptions and risky transactions for more senior management review
- Reporting of the status of exception management activities
- Reporting that indicates the extent of risk existing based on the results of investigating exceptions

9 ONGOING IMPROVEMENT OF CONTROL AND MONITORING PROCESSES = AUDIT READINESS

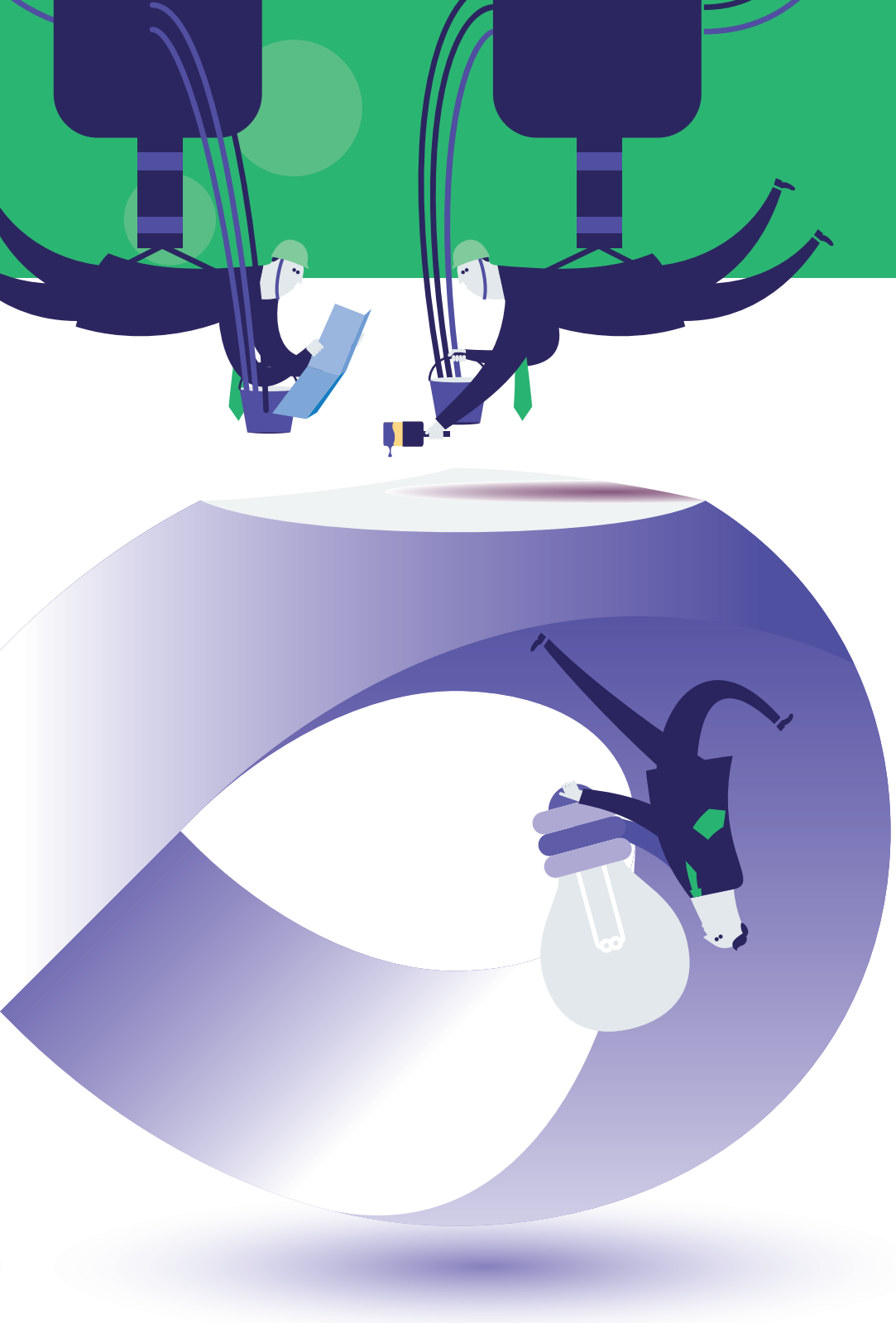
Over time, risks are reduced and the entire control process improves through a continual cycle of:

- testing and monitoring controls
- addressing exceptions, false positives and control breakdowns

This in turn leads to a state of audit readiness in which there is a greatly reduced likelihood of adverse audit findings when IT is subject to scrutiny by audit and compliance functions, whether internal or external.

Things that can make this stage challenging:

- Managing the improvement process and ensuring that attention is focused on significant risks and that important controls are strengthened is not easy. To try and do so using manual methods or a range of home-grown systems, often based on spreadsheets, is time-consuming and often not particularly effective.



What capabilities need to be considered for this step? Technology checklist:

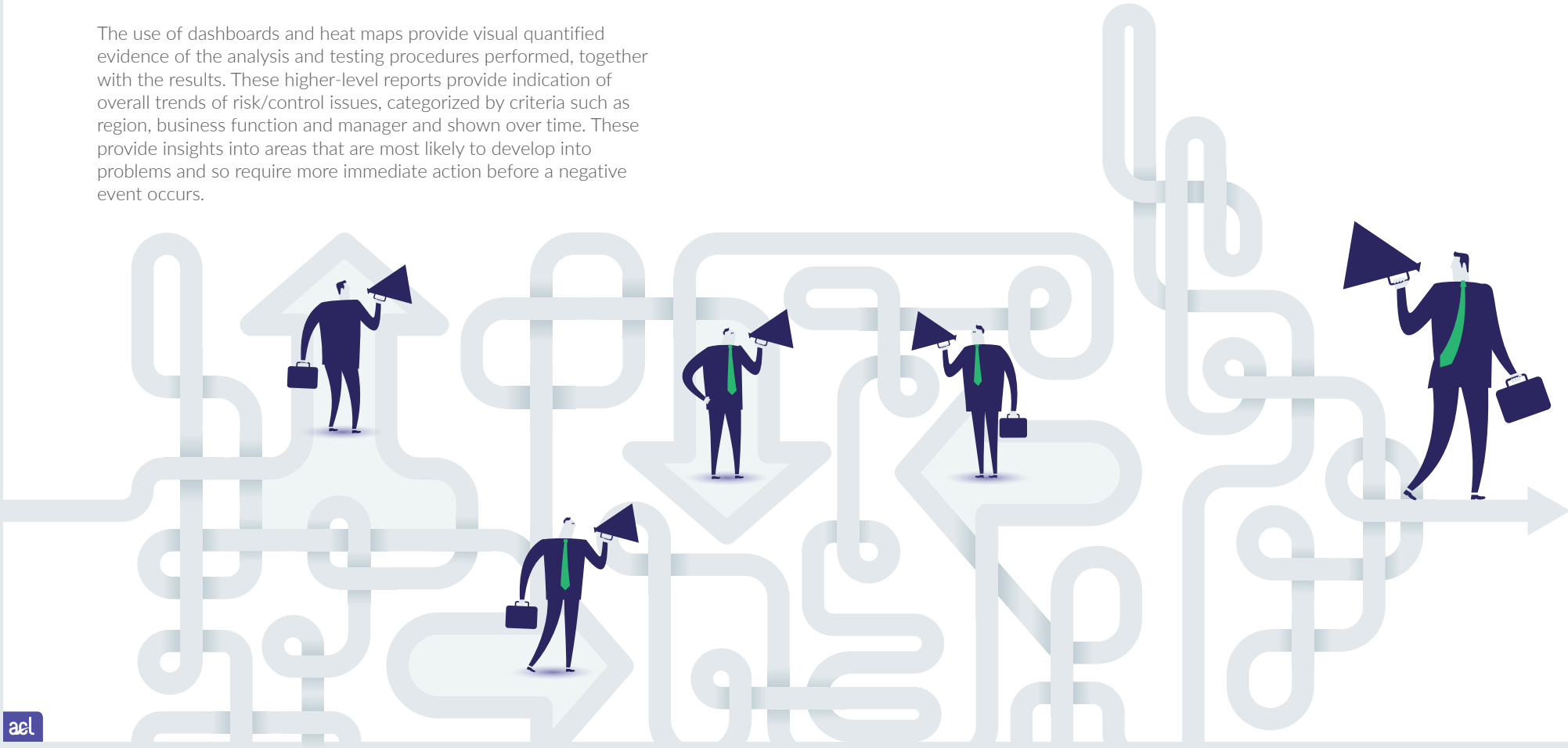
- Integrated system that supports all the stages in the risk/control assessment and monitoring process
- Reporting that provides insights into the overall state of audit readiness across the entire IT infrastructure

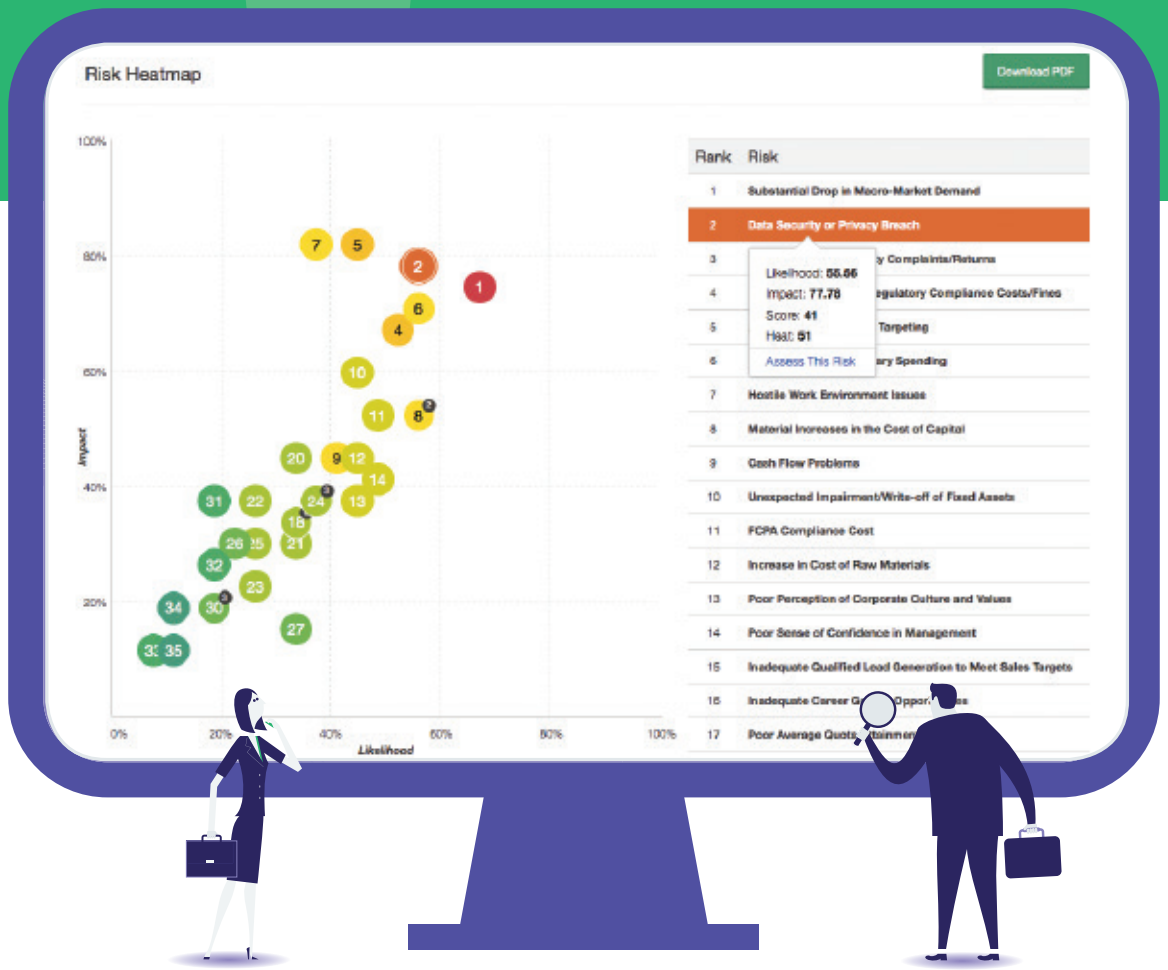
10

DEFINE KRI METRICS TO RUN RISK ANALYTICS FOR PREDICTIVE IT RISK TRENDING

There are additional stages in an audit readiness cycle that move beyond making sure that IT control systems are working as they are intended. When a system is implemented that continually monitors and assesses the integrity of IT transactions and the effectiveness of controls, there is an opportunity to report the results of the entire process.

The use of dashboards and heat maps provide visual quantified evidence of the analysis and testing procedures performed, together with the results. These higher-level reports provide indication of overall trends of risk/control issues, categorized by criteria such as region, business function and manager and shown over time. These provide insights into areas that are most likely to develop into problems and so require more immediate action before a negative event occurs.





Things that can make this stage challenging:

- A typical process to collect information from various sources across the organization and present it in a way that make sense at both a technical level and for senior management review involves a lot of work.
- It is important to provide context for risk and control issues, as well as for the nature and extent of monitoring testing activities. Trying to do this without using technology that is designed to report comprehensively on the status of activities performed, including the quantified extent of tests, results and responses would be an overwhelming task.

What capabilities need to be considered for this step? Technology checklist:

- Accumulation of data on nature and volume of testing activities, results and follow-up responses
- Linking of testing and response data to underlying risk and controls
- Visual and drill down reporting capabilities

11 INTEGRATE IT RISK MANAGEMENT PROCESSES INTO OVERALL ERM

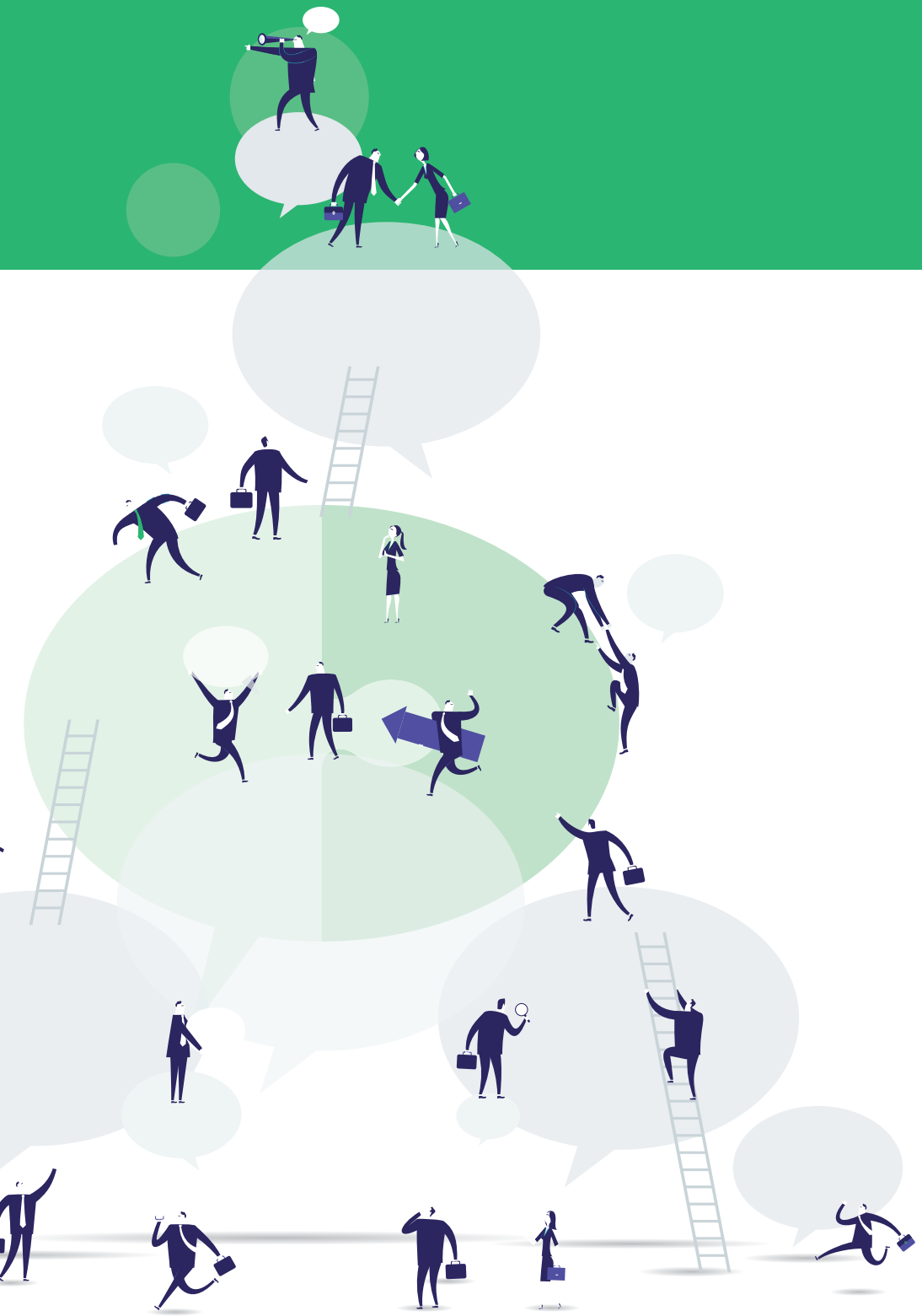
In some cases, the primary objective of moving to a state of IT audit readiness may be simply to better manage departmental control and compliance responsibilities. In other cases, it makes sense to also look at IT's processes for risk management, control and compliance in the context of wider and enterprise 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 is easier to show how risks and controls are inter-related. For example, IT risks rarely exist in isolation, but should often be considered alongside risks and controls within specific financial and operational systems.

Things that can make this stage challenging:

- 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 is not easy.



What capabilities need to be considered for this step? Technology checklist:

- Ability to address a wide range of different audit, risk and control activities in different organizational areas
- Integration with other risk and control management technologies

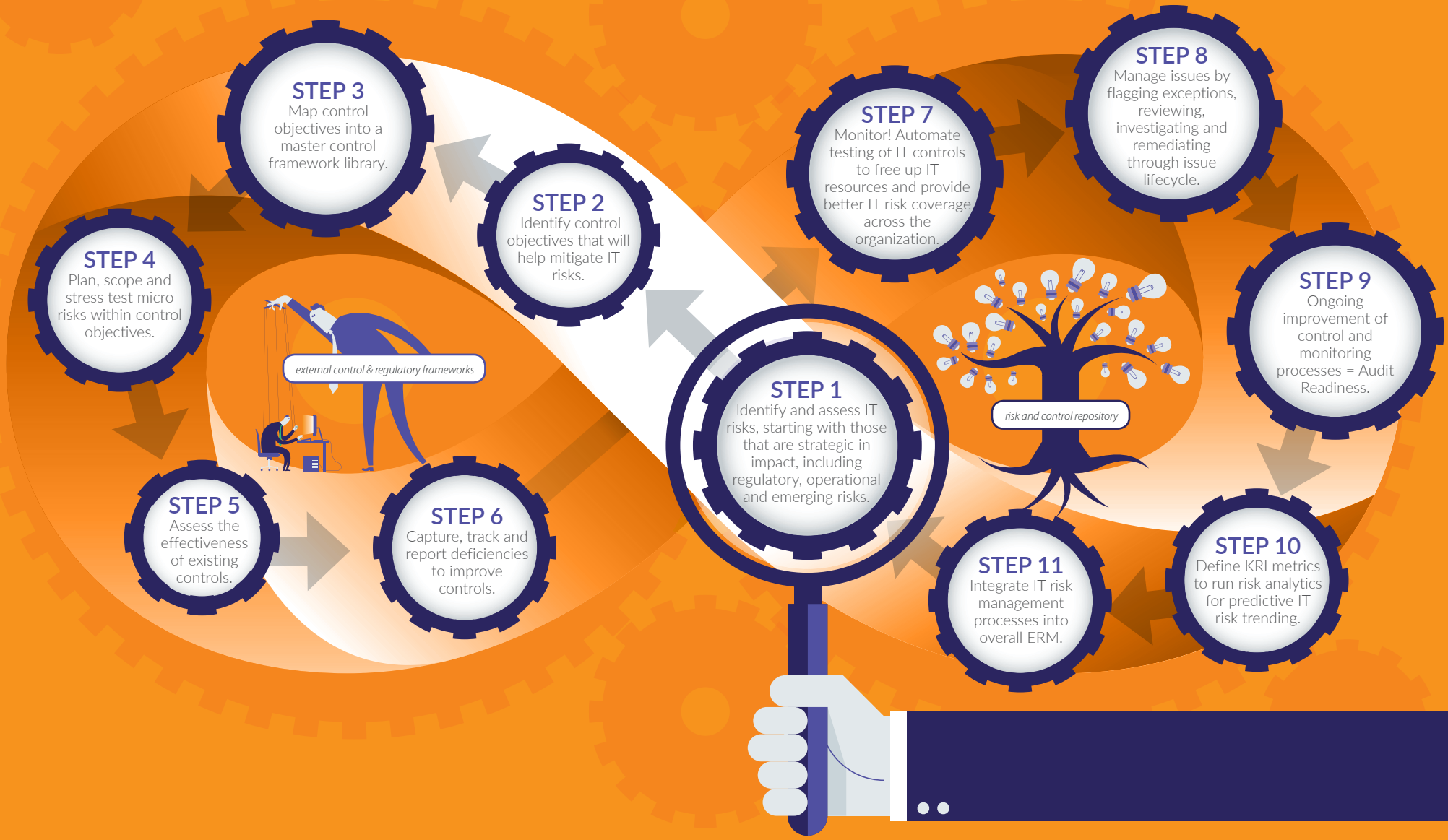
IT AUDIT READINESS: IT'S NOT JUST ABOUT AUDIT.

Being confidently ready for an IT audit or IT compliance scrutiny is a worthy goal in itself. However, getting a clean audit findings report is also a reflection of a more important achievement: to ensure that IT risks are being well managed. And that, because of this, there is far lower likelihood of an IT control or compliance issue causing significant damage to the organization.

We believe that IT audit readiness is an important goal and achievement and that it is really worth doing right, using the right technology and the right approach.

Of course, the end objective is not only a reduction in the risk that bad things will happen, it is also to transform what can often be a painful, frustrating and very inefficient process into something that requires far less effort and significantly reduced overall resource costs. Regulators and auditors, both internal and external, are going to go away happier and with fewer negative things to report. At the same time, IT management is able to improve significantly on the insights and assurance they can provide to the executive suite. IT audit readiness can transform into a win-win for everyone involved.

AT-A-GLANCE: IT AUDIT READINESS PROCESS



"Great—so I can manage this whole process using shared spreadsheets and our in-house data query tool, right?"

Not a good idea!

While spreadsheets are remarkably versatile tools, they have many inherent drawbacks, particularly related to the world of risk and controls. Here are a few things that can be of concern:

- **Spreadsheet management and proliferation:** Dealing with large volumes of interconnected spreadsheets and worksheets can become overwhelming and very inefficient to manage
- **Security over changes**: Spreadsheets are notoriously easy to change, without realizing what has taken place. An accidental or deliberate change can compromise the integrity of information and be hard to detect

Standard query tools and BI reporting software often have the advantage of being readily available to perform data analysis in an organization. However, they rarely have the combination of ease-of-use and flexibility needed to perform the sorts of data analysis that support IT risk and control testing. BI tools for example are generally designed to deal with data from data warehouses, while much of the data involved in IT audit and control testing is sourced from a wide range of types of data files.

On the other hand specialized audit, risk and control data analysis technologies are designed to:

- deal with a wide range of data types
- maintain complete audit trails of all processing performed
- support complex data and transaction testing
- support automation, continuous monitoring and exception management

CONCLUSION

As we said at the beginning of this eBook, arriving at a state of real audit readiness means working out how people, process and technology can all be applied in an effective integrated way. These 11 steps outline the key process steps, and also provide a checklist of the primary technology capabilities that should be considered. While technology is only a tool, it is an extremely useful tool. It is very hard to imagine dealing with the vast range of control and compliance requirements without using specialized technology designed for the purpose.

After all, IT risk and compliance issues are largely about technology and how technology is used in support of an organization achieving its objectives. In many respects, one of the most critical components of a solution for achieving IT audit readiness is to use technology to help control and manage technology-related risks.

Of course, there are many technologies available to support various aspects of the IT security and control process. But one of the greatest challenges is to manage the entire process in a consistent way, so as to get a comprehensive view of the state of IT risk and compliance in one place, with a range of technology capabilities that are designed to work together.

IT audit readiness provides a lot of benefits to the IT function as well as to the organization overall. It is well worth doing it right.

GET YOUR IT HOUSE IN ORDER BEFORE AUDIT DOES.

Are you audit ready? Let us help.

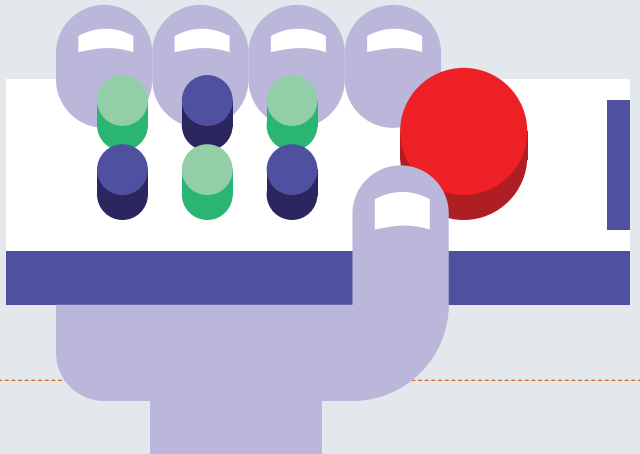
ACL's comprehensive platform can help you easily manage your systems and information security controls in one place to confidently prepare for your next audit.

For a free assessment of how your organization can integrate technology into your IT audit readiness process, call 1-888-669-4225 or email info@acl.com

QUICK-START: TECHNOLOGY REQUIREMENTS FOR IT AUDIT READINESS

To get started, here's a round-up of the big picture technology must-haves:

- Technology **supports the entire IT risk and control process, including process** management, information management, issues management, data analysis, control tests, and information management
- Ability to **quickly and easily get an overview of the status of the entire IT risk and control management process**, as well as to move down to whatever detailed level is appropriate
- **Provides an executive storyboard** that shows all material issues identified across all IT risk and control areas
- **Multiple levels of access control and security** in order to ensure that sensitive data is only available to those who should be involved in a particular part of the process
- **Visual reporting capabilities** that, where needed, can be integrated into an overall risk management dashboard
- User Interface that is **designed for simplification** of audit, risk and control processes
- **Automatic logging** of analysis and monitoring activities in order to support a full "audit trail" and process documentation



01: Identify and assess IT risks, starting with those that are strategic in impact, including regulatory, operational and emerging risks.

- Linking to IT, risk, or regulatory and compliance requirements frameworks
- Records risk descriptions, categories, assessment ratings, quantification, probability
- Ranks and reports risks by multiple criteria
- Compares strategic risks relative to other risks
- Linking to strategic objectives and the entities which they impact
- Linking to relevant regulatory and compliance requirements
- Accesses and analyzes a broad range of system and other data files
- Generates of statistics and indications of anomalies and outliers
- Visual analysis to help indicate significant trends and risk factors

02: Identify control objectives that will help mitigate IT risks.

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

03: Map control objectives into a master control framework library.

- Real-time and rapidly updated views of the entire IT control landscape
- Re-usable templates and frameworks
- Easy change management to cascade control updates across linked areas

04: Plan, scope and stress test micro risks within control objectives.

- Ability to assess and weight the effectiveness of IT controls that are designed to mitigate micro level risk
- Quantification of risk assurance by control, control objective and IT project

05: Assess the effectiveness of existing controls.

- Data analysis tools and techniques designed to test for a wide range of types of control breakdowns
- Automated survey/questionnaire and response system
- Analysis of survey/questionnaire responses
- Visualization of aggregated data across many tests to illuminate outliers that may otherwise not appear to be problematic

06: Capture, track and report deficiencies to improve controls.

- Central tracking of responses to control deficiencies that have been identified
- Specialized data analysis tools and techniques that identify risky transactions according to a wide range of testing criteria

07: Monitor! Automate testing of IT controls to free up IT resources and provide better IT risk coverage across the organization.

- Specialized data analysis tools and techniques to test transactions (financial, operational and IT-specific), which can be run regularly against large data sets
- Automation of data access and analysis procedures so that they can take place with minimal resource requirements

08: Manage issues by flagging exceptions, reviewing, investigating and remediating through issue lifecycle.

- Ability to efficiently adjust testing procedures so that no-risk or low-risk activities are not reported as exceptions
- Workflow procedures that are easy to establish and modify
- Automatic escalation of exceptions and risky transactions for more senior management review
- Reporting of the status of exception management activities
- Reporting that indicates the extent of risk existing based on the results of investigating exceptions

09: Ongoing improvement of control and monitoring processes = Audit Readiness.

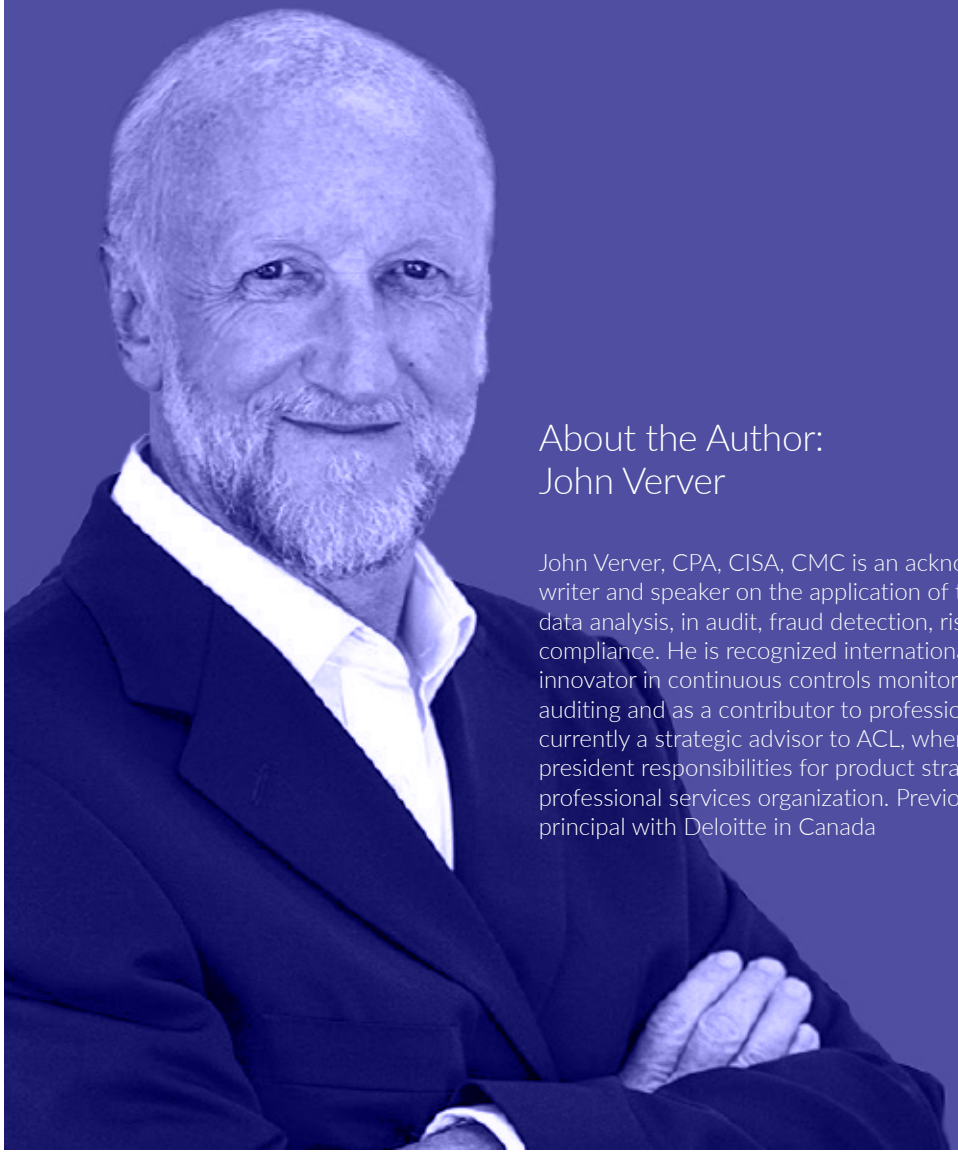
- Integrated system that supports all the stages in the risk/control assessment and monitoring process
- Reporting that provides insights into the overall state of audit readiness across the entire IT infrastructure

10: Define KRI metrics to run risk analytics for predictive IT risk trending.

- Accumulation of data on nature and volume of testing activities, results and follow-up responses
- Linking of testing and response data to underlying risk and controls
- Visual and drill down reporting capabilities

11: Integrate IT risk management processes into overall ERM.

- Ability to address a wide range of different audit, risk and control activities in different organizational areas
- Integration with other risk and control management technologies



About the Author: John Verver

John Verver, CPA, CISA, CMC is an acknowledged thought leader, writer and speaker on the application of technology, particularly, data analysis, in audit, fraud detection, risk management and compliance. He is recognized internationally as a leading innovator in continuous controls monitoring and continuous auditing and as a contributor to professional publications. He is currently a strategic advisor to ACL, where he has also held vice president responsibilities for product strategy, as well as ACL's professional services organization. Previously, John was a principal with Deloitte in Canada

About ACL

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Here are just a few.

Visit us online at www.acl.com