TANIUM

# What you don't know can hurt you

## Expert advice on measuring risk.

Industry experts offer insights and guidance for measuring risks in today's fast-moving, highly distributed world.

TANIUM

# What you don't know can hurt you: expert advice on measuring risk

**Industry experts offer insights and guidance for measuring risks in today's fast-moving, highly distributed world.**

## Contents





## Expert advice on measuring risk

### Managing risks begins with measuring risks.

But how do you measure risks in a meaningful way? Should you tally every software vulnerability in the company? Do you need to make a list of all the endpoint devices requiring software patches? Should you report the uptime stats for your company's most critical applications?

When your job is measuring risk, you need to focus on what's meaningful to your audience. And for the most important decisions about risk, your audience is your company's executive team and the board of directors.

In this eBook, three IT industry experts share their wisdom on the practice of measuring risk in the most practical, comprehensive, and actionable way.

At the end of the eBook, we include a checklist summing up the advice presented by these experts. *Let's get started.*

# Measuring what matters: aligning risk measurement with corporate goals and objectives

If you ask most IT security experts, risk is everywhere. It's in unpatched endpoints, new malware variants, phishing attacks, shadow IT cloud services, laptops left on park benches — the list goes on. With so many technical details contributing to risk, your risk team might be wondering how to approach the important work of measuring risk in your company.

Of course, no one measures risk simply for the sake of measuring risk. Risk assessments are conducted to provide information to decision-makers. So the real question is this: How do you measure risk in ways that help your organization's leaders—the executive team and the board of directors—understand risk so they can make the right decisions to reduce it?

## Measuring risks that matter to your company's leadership

To answer this question, let's start at the top. The executive team and the board of directors are responsible for setting the strategic direction of your company. And part of their job is ensuring that decisions and investments made throughout the organization support the company's high-level, strategic objectives.

No matter what business your company is in, those high-level objectives almost certainly include the following:

- Business continuity
- Data confidentiality, integrity, and availability (data CIA)
- Regulatory compliance

Let's consider each of these in turn.

## Measuring risk associated with business continuity

Business continuity means keeping the lights on, keeping employees productive, keeping any manufacturing and shipping operations humming along, and ensuring that any other types of operations, whether it's pumping oil or delivering a SaaS product, can continue working, no matter what.

Disaster recovery falls into this category. So does protecting business-critical services from cyber threats.

## Measuring risk associated with data confidentiality, integrity, and availability

In every industry, people recognize the importance of data — it's the "new oil" of the digital economy — as well as the importance of protecting data that is confidential.

The challenges of securing that data have increased. For one thing, sensitive data is being accessed from more locations than ever before in the world of a work-from-home (WFH) workforce — a workforce that increasingly relies on bring-your-own-device (BYOD), rather than laptops and desktops tested and provisioned by the IT department.

But no matter where or how employees access data, companies need to ensure data confidentiality, integrity, and availability (or as it's known in some IT circles, "data CIA").

## Measuring risk associated with regulatory compliance

When we think about data privacy, we naturally think about regulations such as the GDPR and HIPAA, which mandate personal data protection.

But there are other regulations, too, covering everything from financial reporting to racial discrimination, that companies cannot afford to violate. Regulatory failures can result in hefty financial fines, contract cancellation, and bad publicity that lasts for years.

To measure risk effectively, you need to know which regulations matter to your company's leadership. Then you track IT assets and processes that help determine whether your company complies with these regulations.

## Framing risk with strategic objectives

It's the job of the executive team and the board of directors to lead the company to achieve core objectives about business continuity, data privacy, and regulatory compliance. Of course, they might lead the company to achieve other objectives, such as an objective about a certain percentage of annual growth or an objective about company culture.

If you want to get the attention of these leaders, frame your discussion of risk measurements in terms of your company's board-level objectives. In other words, identify and weigh your company's various technical, regulatory, and other risks, and show how they relate to your company's high-level, strategic goals.

You'll find that framing your risk measurements this way helps focus your work. And it makes your work more likely to be understood and appreciated by business leaders who set the course for your company's future.

CHAPTER 2:

# Measuring risk by identifying value supply chains

In this chapter, we go into more detail about measuring risks to company objectives discussing the importance of weighted scales for various risks and even for the objectives themselves.

## Identifying risks associated with strategic goals

The work of measuring risks begins by identifying your company's strategic goals and then exploring the people, processes, and technology that support your company's pursuit of those goals.

Think of it as supply chain analysis. You're tracing the flow of data, people, and operations from a high-level goal down to specific IT systems and processes that help the company realize that goal. Those systems and processes function as a kind of supply chain for the goals themselves.

To measure risk, identify dependencies in this supply chain, and trace them as far as makes sense for your company's goals and capabilities. To compare risks within the supply chain itself, everything within the supply chain needs to be assigned a score.

## Building a weighted scale for risks

Even the strategic goals themselves need to be compared and weighted. It's rare for a company to treat all its strategic goals equally.

Once you've identified those goals, assign them scores on some kind of scale, such as 1 to 10. For example, based on conversations with the executive team, you might assign continued revenue growth of at least 10% CAGR a score of 10, and regulatory compliance a score of 7.

Next, identify people, processes, and technology involved in supporting each strategic objective, and rank the importance of each of those supporting factors.

To provide further nuance, you might estimate the likelihood of a particular type of failure occurring. For example, imagine your company has a web server supporting a business-critical mobile app. The odds of that server delivering unacceptably slow performance during a period of peak usage are probably higher than the odds of that same server succumbing to a power outage that crashes both the main and backup power systems.

By multiplying a score for the strategic importance of the server (say, 7 out of 10) by the likelihood of a specific risk (say, 50% or 0.5), you can begin ranking risks and identifying risks that require more immediate action.

For example, the server delivering slow performance might have a likelihood of 40%, and the server crashing in a catastrophic power outage might have a likelihood of 2%. If the server's importance is 7 out of 10, then the risk score for the slow performance scenario would be 7 times .40 (which yields 2.8). The risk score for the power outage scenario would be 7 times 0.02 (which yields 0.14). The slow-performance scenario, which has the higher risk score, is obviously the risk that needs attention first.

## The importance of collaboration in measuring risk

Performing this type of risk assessment requires collecting detailed information about people, processes, and technology across the company. The IT department is going to have to reach out for help.

My advice? Ask for help from every department whose processes and technology you're evaluating. For example, if you really want to understand the risks surrounding the HR department's applications, talk to people in the HR department. They might know things about an application's importance that the IT operations team has overlooked.

When you're talking to people outside the IT department, minimize the use of technical jargon. Also, never tell somebody how to do something without first asking them how they think it should be done. If you impose a solution on people, you might miss out on a creative alternative. You might also find that people balk at following a new policy that affects them directly without ever taking their ideas into account.

## Risk management is a company issue, not an IT issue

When people outside the IT department realize that you trust them and that you're genuinely interested in what they have to say, they'll communicate with you more freely. They're also more likely to take ownership of the risk management solutions you put in place together.

This ongoing collaboration is one of the benefits of taking a "supply chain" approach to measuring risk. You'll not only discover the details you need for measuring risks more precisely. You'll also educate stakeholders across the organization about the importance of risk measurement and risk mitigation. And you'll get the opportunity to collaborate with these stakeholders on developing solutions to minimize the risks you've both identified.

CHAPTER 3:

# Modernizing risk assessments for today's distributed enterprise

Measuring risk used to be a special event undertaken with consultants. With real-time data and automation, companies now measure risk more accurately, continuously, and effectively.

Last year's sudden shift to a WFH model changed many things in enterprise IT, including how IT teams conducted risk assessments.

In this chapter, we look at how companies traditionally performed risk assessments. Then we consider how many companies have been conducting them since the pandemic began and offer some best practices for modernizing risk assessment to better serve today's highly distributed enterprise.

## How risks and risk assessments changed in the pandemic

Traditionally, many organizations performed risk assessments just once a year. Risk assessment teams produced detailed reports that tried to sum up all the organization's risks in areas such as IT security, disaster recovery and compliance.

To gather information for their reports, the teams visited data centers and distributed questionnaires. Even if the visits were scrupulous and the questionnaires thorough, the assessments invariably reflected risk at a single moment in time.

If, five minutes after the team left the data center, a new software upgrade suddenly jeopardized the integrity of the company's financial reporting, the risk assessment report didn't reflect that increased risk.

For many organizations, the tenuousness of these risk assessments increased during the pandemic. Emailed questionnaires replaced in-person inspections. Stakeholders dutifully completed forms, even if no one could say with certainty which devices employees were using remotely or what software was running on them.

Is there a better way of conducting risk assessments? I've spent a lot of time in my career focused on the practice of risk assessments, and I think there is.

## Bringing risk assessment into the age of cloud computing and WFH

The first thing to change about risk assessments is their timeliness. If reports are based on data collected once a year, they're going to be inaccurate most of the time.

We all know that the pace of business is faster than ever. Data, devices, software, business relationships — all these things are continually in flux. Risk assessments need to reflect that flux.

Fortunately, IT departments have new tools that can help improve the accuracy of risk assessments. Real-time endpoint monitoring, for example, can report on the location, IT health, and activity of endpoints at any location, including in home offices. This monitoring works over standard internet connections without requiring VPNs.

With these modern tools, IT organizations can collect ever more comprehensive, up-to-date, and accurate endpoint data than they could when most endpoints were still on internal networks and being monitored only sporadically by traditional endpoint management tools.

The second thing to do is measure risk over time. Executives want to know if the risk mitigation measures that have been put in place are working. Risk teams should track the metrics that indicate whether or not the company is achieving its goals for managing risk.

The third thing is to have data-driven conversations with the executive team about risk. Here's where that more timely and comprehensive data pays off. With improved visibility into endpoints and other IT assets, you can have a more meaningful discussion about which investments work and which don't.

## Four key elements of risk management

Keeping your organization's strategic goals in mind, here are four steps for managing risk in a modern enterprise.

### 1. Data collection

This means collecting all data necessary to measure risks related to your organization's strategic goals. That obviously includes endpoint data, as well as environmental and user data.

### 2. Analysis

Once you've collected data, analyze it, preferably using as much automation as possible. Your analysis is more likely to be time-consuming and error-prone if your analysis depends on multiple Excel spreadsheets and printouts. If you've created scorecards for assessing risks, you can automate tabulations and make analysis an ongoing process rather than a once-a-year snapshot.

### 3. Reporting

This step involves synthesizing risk metrics and analysis for executive-level reports. These reports will guide your organization's discussions about risks, priorities, investment decisions, and more. In these reports, frame risk analysis in terms of the strategic goals your executive team and board focus on continually.

### 4. Remediation

There are two types of risk remediation. First, there are actions taken daily by IT security and IT operations personnel to respond to threats, such as malware infections. These actions don't require executive approval. Second, there are actions taken by the IT and business leaders in response to executive-level reports created in the first three steps of this process. Companies should undertake both forms of risk remediation.

Over the past year, many companies reinvented themselves as more agile, more geographically distributed organizations. Now companies have the chance to reinvent their risk assessment processes as well.

By taking advantage of real-time data and automation, companies can reduce risks and improve the security of their remote workforces at the same time.

CHAPTER 4:

# The importance of making risk assessment an ongoing process

Measuring risk is complicated work. Fortunately, new technology can help make risk assessment an automated process.

Every organization is threatened by risk but assessing that risk is harder than ever before. In this chapter, we explain what makes risk assessment so difficult and how taking a top-down approach to measuring risk can streamline this work and help organizations make better decisions.

## Why measuring risk has become more difficult

Why is measuring risk so difficult these days? Here are four reasons.

### Difficulty #1: Disparate, varied IT assets

Twenty years ago, IT risk assessments mostly consisted of counting employees' PCs and the servers in data centers, looking at likely vulnerabilities for various models of hardware, and producing a report.

Today, the IT assets to be cataloged and analyzed might be distributed over, say, 50 offices, 500 data centers (most which belong to other companies), and 10,000 home networks. And a significant portion — probably at least 20% — of that distributed architecture consists of "shadow IT" — that is, products and services employees have adopted without formal approval and continuous oversight of the IT department.

In this highly distributed, difficult-to-catalog IT environment, traditional risk-measurement tools and approaches simply won't work.

## Difficulty #2: IT complexity

A second reason why risk assessment is difficult is IT complexity. It's not just that there are more devices; how software is built and works has changed.

The age of large, monolithic applications is over. Today's IT infrastructure comprises lots of small and medium-size components working together to create a greater whole.

For example, a mobile banking application might rely on 75 different IT components to work. Those components might range from UI code to multiple back-end databases. The risks associated with each of those components affect the risks of the application overall. That's why it's critical for companies to have a **real-time software bill of materials.**

## Difficulty #3: Sophisticated security attacks

Third, businesses are under attack by a growing collection of cybercriminals, many of whom have access to highly sophisticated technologies.

Twenty years ago, attackers were mostly mischief-makers, computer programmers interested in finding ingenious ways to cause trouble. Today, attackers include nation-states, criminal syndicates, and malicious "script kiddies" willing to spend 50 bucks on the Dark Web to buy a malware or a credential-stuffing script and a list of corrupted credentials.

## Difficulty #4: Shared responsibilities

A final difficulty? A recent trend in risk management calls for sharing risks more broadly with business units. The IT organization might lead an organization's risk assessment project. But now, executive teams and boards of directors ask business-unit leaders to step up and take responsibility for the risks affecting their operations.

To address these difficulties, take a top-down approach to measuring risk, as my colleagues described in the earlier chapters of this eBook. Identify "supply chains" supporting each strategic goal and collect as much real-time information about the status of each supply chain as necessary.

## Measuring risk is an ongoing strategic activity

You'll know if you have an effective practice in place for measuring risk if it provides ongoing guidance for making business decisions. To provide that guidance, your best practice for measuring risk should be:

### Ongoing

Your organization's risk assessments should be continuously updated with information about your IT environment's current state. When risk data is current, you can trust that you're basing decisions on the technology and vendors you work with now, not a different set you worked with three months ago.

### Prioritized

Your risk-assessment practice should make it easier to prioritize risks and risk mitigations in terms of your organization's strategic goals. You have risk scoring in place so that you can compare, for example, the risk of moving a data repository from on-premises to a trusted cloud provider to save money.

### Accessible

You can easily access risk assessments whenever necessary. You don't have to dig through 43 Excel spreadsheets to find the analysis you're looking for. You've got risk reporting that you can access quickly as part of the company's ongoing decision-making.

Business is moving faster than ever. IT environments are vast and complex. By adopting a top-down approach to measuring risk and taking advantage of real-time data collection and automation, you can build the risk measurement practice you need for guiding your organization through growth and transformation in the years ahead.

## Essential guide for measuring risk

1. Meet with your company leaders to understand their long-term strategic objectives for the company.
2. Assign these objectives scores to understand the relative importance of each.
3. Identify the people, processes, and technologies that support each objective.
4. Explore uncertainties about each supporting factor in an objective's "supply chain."
5. Whenever possible, rely on automation to collect data, such as data about the operating status of endpoints.
6. Meet with stakeholders in various departments to understand their concerns about risks and to collaborate on recommendations for reducing those risks.
7. Assign each uncertainty a score in terms of importance and a percentage in terms of likelihood. Multiply scores by likelihood to derive a risk score for a particular person or team, process, or technology in an objective's supply chain.
8. Tally the results of your measurements and organize them in a way that relates each risk to a strategic objective.
9. Meet again with your company's leadership for a data-driven discussion about risk. Help them understand existing risks and decisions that can be made to reduce them.
10. Now that you have a risk measurement framework in place, continue updating it, using automation whenever possible so that risks can be assessed in detail at any time.

Risk, as defined by *ISO 31000,* means uncertainty about objectives. In this eBook, we shared wisdom about which objectives matter and how to measure their uncertainty for the best possible outcome: reducing risks that jeopardize a company's mission.

Company endpoint devices play an important role in risk management. The Tanium Converged Endpoint Management (XEM) platform can help give organizations more visibility into their security metrics, so they can identify risks and remediate them in real time. Tanium Benchmark is the only solution that provides real-time risk comparisons to industry peers.

Learn more about **Tanium Benchmark.**