Diligent

KRI Basics for IT Governance

How information technology & information security can implement this crucial part of risk management

Table of Contents

What You'll Learn

This white paper addresses some of the most common challenges of implementing, managing, and maintaining key risk indicators (KRIs) within your IT department.

By the time you've finished reading, you'll be armed with enough information to start implementing your own KRI program.

Diligent

The Purpose & Role of KPIs, KRIs, & KCIs

Before we dig into KRIs, we first want to look at the type of metrics that well-governed organizations track. These include:

INDICATOR METRIC	WHAT DOES IT MEASURE?	WHAT'S THE PURPOSE?	WHO'S THE AUDIENCE?
Key performance indicator (KPI)	KPIs measure how effectively the organization is achieving its business objectives.	They provide directional insight on how you're progressing toward strategic objectives, or the effectiveness of specific business processes or control objectives.	**Strategic KPIs:** Most often executive management and the board. **Operational KPIs:** Most often managers, operational process owners, and department heads.
Key risk indicator (KRI)	KRIs measure how risky certain activities are in relation to business objectives.	They provide early warning signals when risks (both strategic and operational) move in a direction that may prevent the achievement of KPIs.	**Strategic KRIs:** Most often executive management and the board. **Operational KRIs:** Most often managers, operational process owners, and department heads.
Key control effectiveness indicator (KCI)	KCIs measure how well controls are working.	They provide direct insight into a specific control activity, procedure, or process that wasn't implemented or followed correctly.	Most often front-line control activity owners.

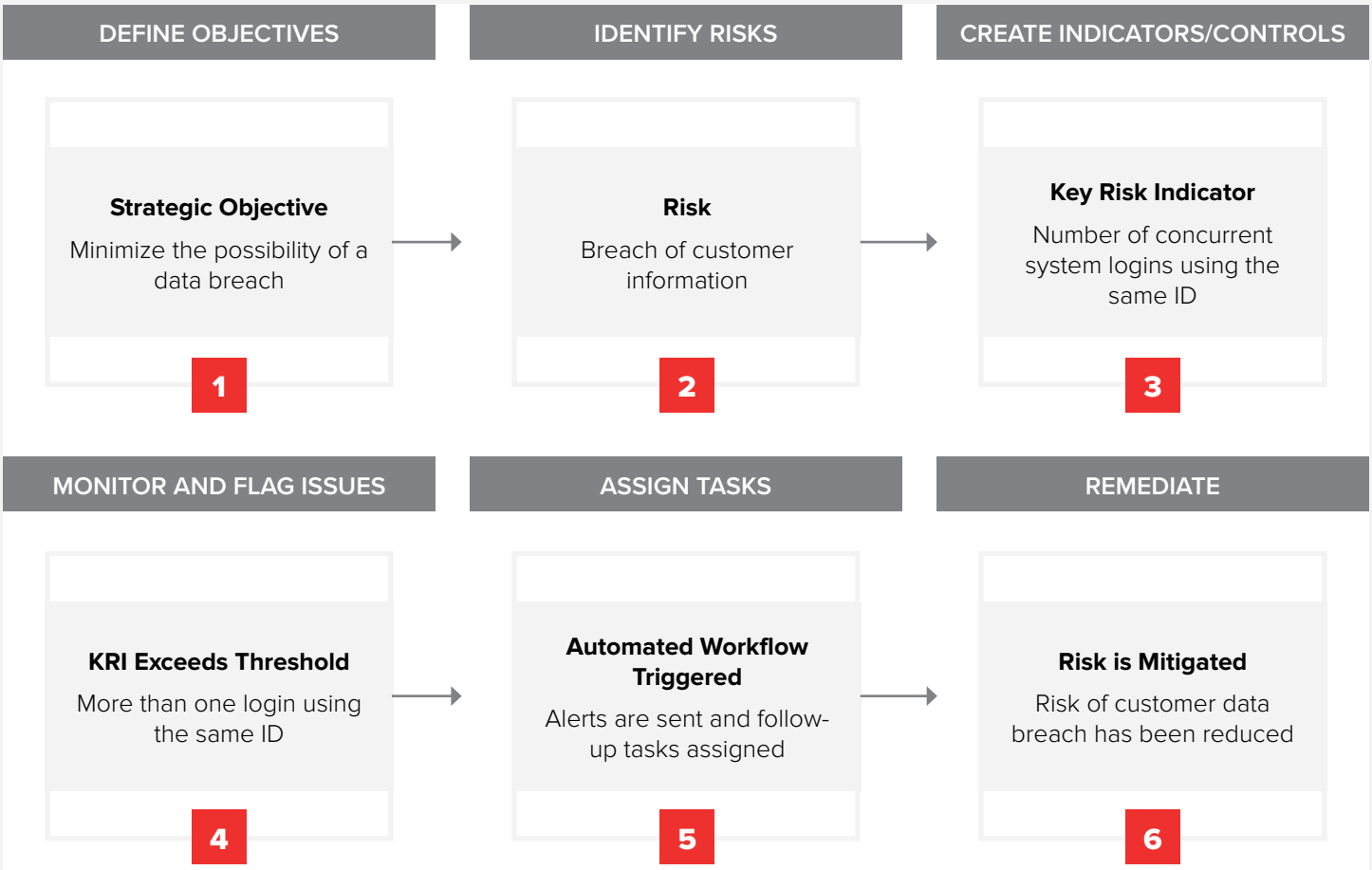
The Institute of Operational Risk states that the difference between risk, control effectiveness, and performance indicators is largely conceptual. "The same piece of data may indicate different things to different users of that data, implying that the nature of an indicator changes depending on its use."

Diligent

What Do KRIs Do?

KRIs help monitor and control risks. They link back to a range of operational risk management activities and processes, including risk identification; risk and control assessments; and the implementation of risk appetite, risk management, and governance frameworks.

Basically, a risk indicator can be any metric used to identify a change in risk exposure over time. They become KRIs when they track a critical risk, or do so especially well because of their predictive value. It's ideal if they do both.



Example:

The organization has a **(1)** strategic objective to minimize the possibility of a data breach. A **(2)** key risk in this case could be the breach of customer information. So, a **(3)** KRI might be the number of concurrent system logins using the same ID. Once a certain **(4)** threshold is met (more than one login using the same ID), **(5)** alerts and follow-up workflows can be set to engage the appropriate people so they will **(6)** take action, which results in reduced risk of a customer data breach.

Diligent

Any number of KRIs can be applied to this model. It's a great way to start automating some more of those repetitive, monotonous (yet critical) tasks.

Leading, Lagging, & Current KRIs

KRIs can be helpful in a number of ways. They can provide information on the current state of your risk, events that happened in the past, or events that might happen in the future. These are classified further as:

1. **Leading indicators.** Emerging risk trends for events that might happen in the future and need to be addressed. For example, the number of employees who click on fake phishing emails.
2. **Current indicators.** Where you currently sit with your risk exposure. For example, the number of staff who haven't completed mandatory security training.
3. **Lagging indicators.** Events which took place in the past and could occur again. For example, the time between employee termination and deletion of accounts.

How Many KRIs Should You Have?

Too much data can be overwhelming. Too little, and you're not going to gain any insight or could be missing critical risk indicators. According to the Institute of Operational Risk, there is no right or wrong answer for how many risk indicators you should have, but they suggest considering the:

- Number and nature of the key risks identified
- Availability of the data needed for the KRIs
- Cost to extract the data
- Intended audience

Good KRI Checklist

Good KRIs share a number of characteristics.

- **Relevant.** The indicator/data helps identify, quantify, monitor or manage risk and/or risk consequences that are directly associated with key business objectives/KPIs.
- **Measurable.** The indicator/data is able to be quantified (a number, percentage, etc.), is reasonably precise, comparable over time, and is meaningful without interpretation.
- **Predictive.** The indicator/data can predict future problems that management can preemptively act on.
- **Easy to monitor.** The indicator/data should be simple and cost effective to collect, parse, and report on.
- **Auditable.** You should be able to verify your indicator/ data, the way you sourced it, aggregated it, and reported on it.
- **Comparable.** It's important to be able to benchmark your indicator/data—both internally and to industry standards—so you can verify the indicator thresholds.

"In my experience, KRIs deliver substantially more value when they're either leading or current. This is because of their predictive nature relative to the business objective or KPI that they support. While current indicator KPIs measure performance, the best KRIs help us predict how to improve that performance."

Dan Zitting
Chief Customer Experience Officer at Diligent

Diligent

“The intended audience and purpose is really the most important thing to consider,” says Dan Zitting, chief customer experience officer at Diligent. “By clearly separating strategic KRIs that support strategy-level business objectives from operational KRIs that support operational or process-level objectives, KRIs become naturally managed into groups that are digestible and useful to the intended audiences.

At the strategic/enterprise level, I’ll typically target having no more than 15–30 strategic risks (depending on the size and scope of strategic objectives in the organization’s strategic plan), and no more than a few KRIs per strategic risk.

So at the strategic level, we often find a KRI library of 20–30 total—one that can cover the strategic health of the enterprise, but also roughly the high end of what can be consumed in the strategy-level executive and board conversation.

At the operational/process level, good value is found in the range of 3–12 operational risks per process, as outside that range probably indicates a process either really isn’t a process, or a process needs to be broken up into multiple processes.

Typically, an operational risk has a one-to-one relationship with the relevant KRI, thus typically no more than 5–15 KRIs per process area. Summary KRIs (i.e., a KRI itself that is the number of positive or negative KRIs below) may be used for business unit managers to get a more holistic perspective on the operational health of their complete sphere of accountability.”

Diligent

Example KRIs to Get You Started

Now you know what KRIs do, what makes a good KRI, and how KRIs differ (and relate to) KPIs and KCIs. The next step is identifying the KRIs that would work for your organization or team. But choosing which KRIs to implement isn't always as easy as picking from a universal set of indicators—especially when it comes to IT governance.

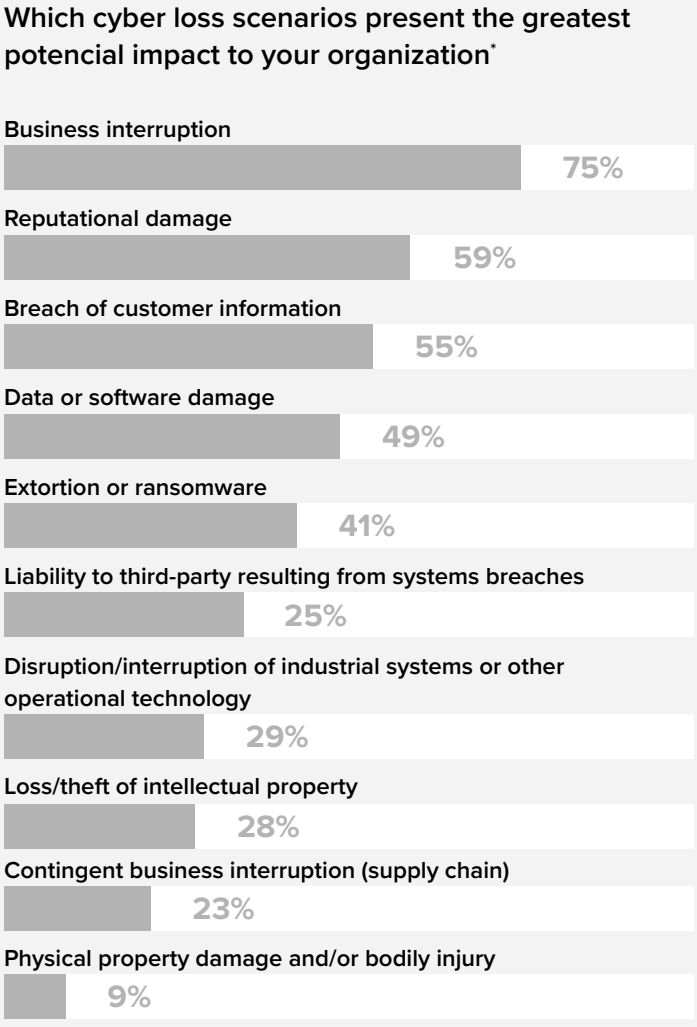
First, each business or organization has a number of different factors that come into play—like objectives, culture, products, processes, and other activities—that will define which KRIs should be monitored. For IT governance, your lists of KRIs will vary based on the products you offer, who you're regulated by, where you're operating, and your organization's unique objectives and priorities.

Second, KRIs aren't static. They need to be monitored and updated as your business objectives change and evolve. This will be unique to almost every organization and the main reason why going off a list shouldn't be your only approach.

To provide some potential KRIs for IT governance, we first looked to the Global Cyber Risk Perception Survey by Marsh and Microsoft to determine what risks are top of mind with IT execs. The data showed that the risks with the highest potential impacts on the business include (in order):

1. Business interruption
2. Reputational damage
3. Breach of customer information
4. Data or software damage
5. Extortion or ransomware
6. Third-party liability resulting from systems breaches
7. Disruption/interruption of industrial systems or other operational technology
8. Loss/theft of intellectual property
9. Contingent business interruption (supply chain)
10. Physical property damage and/or bodily injury

These risks could damage an organization—possibly to the point of collapse. So it's surprising to learn that one-third of IT execs surveyed by Deloitte admit they have little or no IT governance process in place.



*More than one response allowed

Figure 1: Business interruption seen as having the greatest potential impact from a cycle event.

Diligent

While each organization will have unique enterprise or organizational risks, we've defined 15 KRI examples, linked to the top three risks from the Global Cyber Risk Perception Survey by Marsh and Microsoft.

Across the globe, execs are focused on high-impact risks, but one-third have little or no IT governance process.

Business Interruption

ASSOCIATED RISK	MEASURABLE KRI	NATURE	WHY YOU SHOULD TRACK THIS	APPLICABLE
Vendor service interruption	Number of applications currently running in the organization without a service level agreement (SLA).	All	Without an SLA, your organization may be engaging with a high-risk vendor. The vendor may not adhere to your regulations or they could end service at any moment, causing a disruption in the business.	☐
ISP failure	Number of ISP outages.	Leading	High numbers of outages can be an indicator that it's time to change providers. Especially if you provide online services, outages can mean business comes to a full stop.	☐
Loss of data	Number of system backup failures.	Lagging	New or upgraded software can cause backup failure, or there could be misconfigurations due to overly customizable software that result in backup failures.	☐
Lack or misappropriation of IT budget	Total discrepancy (dollars) of IT budget versus actual.	Lagging	Over-spending in IT can mean critical or new tools go unfunded. Under-spending can mean IT is overlooking important investments, or isn't budgeting accurately.	☐
Lack or misappropriation of IT personnel	Average amount of time to resolve IT support requests.	All	Higher time to close tickets can indicate a lack of resources, which may lend itself to larger, undiscovered issues which could cause business interruptions.	☐

Diligent

Reputational Damage

ASSOCIATED RISK	MEASURABLE KRI	NATURE	WHY YOU SHOULD TRACK THIS	APPLICABLE
Terminated employees accessing systems	Average time between employee termination and disabling of accounts/ termination of access to all systems.	Lagging	Allowing terminated employees to continue to access data and systems could lead to serious data breaches.	☐
Unaddressed critical incidents	Time to resolve a critical incident and the number of critical incidents.	Lagging	Extended time to resolve a critical incident may infer that the organization's critical incident procedure requires an overhaul.	☐
Loss of hardware/ physical assets	Number of company-issued phones without monitoring software installed.	Lagging	Monitoring software can locate a lost or stolen phone, and wipe the data before it gets into the wrong hands. All company-issued phones should have this software installed.	☐
Anonymous data leak	Number of active default database administrator accounts.	Leading	Pre-configured default database administrator accounts means if an event were to happen, you can't tie it back to an individual and resolve the issue.	☐
Breach of GDPR compliance	Time to respond to requests for personal data.	Lagging	Massive fines can be issued for organizations who breach GDPR. This could cause serious financial and reputational damage.	☐

Breach of Customer Information

ASSOCIATED RISK	MEASURABLE KRI	NATURE	WHY YOU SHOULD TRACK THIS	APPLICABLE
Shared login credentials	Number of concurrent system logins using the same ID.	Lagging	Could indicate an employee has shared their login credentials with an unauthorized individual who shouldn't have access to confidential information.	☐
Improper security assignments	Total number of users with similar roles but dissimilar security assignments.	All	This could indicate that one employee may be accessing customer data files that they shouldn't.	☐

Diligent

ASSOCIATED RISK	MEASURABLE KRI	NATURE	WHY YOU SHOULD TRACK THIS	APPLICABLE
Malware	Number of employees who click on IT-sent phishing emails.	Leading	By setting up and testing employees with fake phishing emails, you can identify those employees that require additional security training.	☐
Employees unaware of what defines confidential information	Pass/fail results for employee information security training.	Leading	Employees who fail or don't complete security training regularly increase the risk of customer information being shared.	☐
Non-compliance and data breaches	Frequency of review of high, elevated (privileged) permissions on IT systems.	Lagging	These accounts are more likely to be targeted by cyber attackers to gain access to confidential or customer data.	☐

Selecting Your Own KRIs

According to the Institute of Operational Risk, there are two ways to select indicators for your organization.

1. **Top-down.** Senior management and/or directors select indicators to monitor across the business. This is typically the most effective approach for strategic-level KRIs. Top-down KRIs can facilitate aggregation and management understanding in the context of top-level strategy and business objectives.
2. **Bottom-up.** With this approach, the business entity or process manager selects and monitors the indicators they see as relevant within their operational processes. A bottom-up approach ensures that business entity managers select indicators most relevant to the actual operational objectives of their entity and processes.

You might choose to use a combination of bottom-up and top-down approaches, particularly to capture KRIs into the appropriate context of strategic versus operational. We've included a blank worksheet here with an example to help you.

Diligent

KRI Selection (Worksheet):

BUSINESS OBJECTIVES	DEFINE SOURCES OF RISK	ESTABLISH KRI	SET KEY THRESHOLDS	MONITORING FREQUENCY
Minimize the Possibility of a Data Breach	Users Sharing Login Credentials	Number of Concurrent System Logins Using the Same User ID	More Than One Login Using the Same ID	Real-Time

Diligent

Next steps: Workflows & Reporting

Automating Data Analysis & Workflows

Because they have specific, measurable thresholds, all of these KRIs can be dynamically updated through continuous monitoring and analysis. You can use KRIs to automate workflows once thresholds are exceeded, and make sure you're on top of tracking follow-up and remediation.

Reporting & Dashboards

You can also use the data to create real-time storyboards so you can, at any time, get a pulse on the health of your internal controls. This provides you with instant reporting, accessible to your teams and management, to help improve the communication and show the efforts being made to mitigate enterprise risk by the IT group.

Information Technology Governance: Best Practices to Prevent Data Breaches

With each new data breach, it becomes more and more evident that IT governance is critical. Data breaches must be looked at as an organizational risk—after all, they have the power to totally cripple the business and disrupt operations, impacting the bottom line.

About Diligent

Diligent created the modern governance movement. As the leading governance, risk and compliance (GRC) SaaS company, we serve 1 million users from over 25,000 customers around the globe. Our innovative platform gives leaders a connected view of governance, risk, compliance and ESG across their organization. Our world-changing idea is to empower leaders with the technology, insights and connections they need to drive greater impact and accountability – to lead with purpose.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com