Diligent

TIP SHEET

Key Risk Indicators for IT Risk Management

Choosing which key risk indicators to implement isn't always easy — especially when it comes to IT risk management.

Each business or organization has a number of different factors—like objectives, culture, products, processes and other activities—that will define which key risk indicators (KRIs) should be monitored. For IT risk, 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.

Also, KRIs are not 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. But we've gathered 15 example KRIs to get you started.

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 that business comes to a full stop.	☐
Loss of data	Number of system backup failures due to software failure	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	Overspending in IT can mean critical or new tools go unfunded. Underspending 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 that could cause business interruptions.	☐

Reputational Damage

ASSOCIATED RISK	MEASURABLE KRI	NATURE	WHY YOU SHOULD TRACK THIS	APPLICABLE
Terminated employees accessing systems	Average time between employee termination and deletion 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 imply 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 mean that, 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 are issued for organizations that 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 access.	☐
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 employees who require additional security training.	☐
Employees unaware of what defines confidential information	Pass/fail results for employee information security training initiatives	Leading	Employees who fail or don't complete security training on a regular basis increase the risk of customer information being shared.	☐
Hackers access systems via password cracking	Number of users whose passwords are past expiry/ change dates	Leading	Employees who don't update passwords on a regular basis can expose the organization to increased breach risks.	☐