



BEST PRACTICES

A Collection of Best Practices for:

Risk Management

Includes Detailed Best Practices for:

- Compliance
- Corporate Governance
- Ethics
- Internal Audit
- Risk Assessment
- Risk Reporting



Table of Contents

Risk Management Best Practices

Risk Management Best Practices

- Compliance 2**
- Corporate Governance 5**
- Ethics 9**
- Internal Audit 12**
- Risk Assessment 15**
- Risk Reporting 18**

This content may not be copied, distributed, republished, uploaded, posted or transmitted in any way without the prior written consent of OpsDog, Inc.



Risk Assessment

Risk Management

Compliance

Corporate Governance

Ethics

Internal Audit

Risk Assessment

Risk Reporting

— — — — The Risk Assessment Group is tasked with researching and determining both current and future risks that may become hazardous to the company's business operations. The Risk Assessment Group's responsibilities range anywhere from identifying new competitors, data security issues, reputational or Public Relations (PR) risk, financial or liquidity risk, product recalls or even weather or natural disaster risks, among other things. The Risk Assessment Group works closely with the Corporate Governance function, who will implement corporate policies based on the findings of the Risk Assessment function.

Risk Assessment


Risk Management Best Practices

Best Practice 1-A

Develop and Clearly Document Risk Assessment Policies to Improve Future Understanding

Develop and clearly document a risk assessment policy that defines how often such assessments are performed, how risk is to be defined and how identified risks should be addressed and mitigated. Document clearly the how and why of a risk rating as well as the risk assessment process as a whole to allow management, regulators and future risk management employees to fully understand the assessment.

Typical Practice (the Status Quo): Allow risk assessment employees to use their “gut” when determining how often risk assessments are to be performed, the how and why of a risk rating, and how risks should be addressed and mitigated. It is the responsibility of employees within the Risk Assessment function to properly perform risk assessments on time and to ensure that any and all questions concerning the risk assessment (whether the questions are made by management, a new risk manager, etc.) is addressed.

 **Benefits of this Best Practice:** Developing and clearly documenting a risk assessment policy (typically details how often risk assessments are performed, how risk is to be defined and how identified risks should be addressed and mitigated) not only ensures quick understanding by anyone who reads developed risk assessment reports, but also reduces the number of questions risk assessment employees will have to field because of ambiguous language or an overwhelming amount of unstructured data. This then frees risk assessment employees to work on other tasks. Furthermore, when a new risk manager or compliance officer takes over the risk assessment program, the tools, data and methodology of past risk assessments will allow them to start their new duties immediately. Such detailed risk assessment policies also allows examiners to see evidence that the company is reviewing and updating the risk assessment throughout the year, which is especially important when a change is made on the rating of a risk, an asset, or the company’s compliance control.

Related KPIs: Composite Risk Index, Mean Time to Incident Detection, Number of Accounts Determined to Have Unintended Access to Sensitive Data Within Last 30 Days.

Risk Assessment

Risk Management Best Practices

Best Practice 1-B

Periodically Revisit Risk Assessments to Keep Them Up To Date

Revisit documented risk assessments on a periodic basis to evaluate the assessment's effectiveness and to identify areas where enhancements might be needed. Periodic updates to the company's risk assessment, furthermore, allows the Risk Management Group to continuously focus on the assets and compliance controls that are considered to be critical to the company.

Typical Practice (the Status Quo): Revisit documented risk assessments only in preparation for examination by an appropriate regulatory body (typically done on an annual basis) and/or whenever an area of risk the business faces is observed or predicted to increase (e.g., expansion into other countries or lines of business, acquisition of another company, etc.) so as to keep risk

**To download the full document,
add this product to your shopping cart
and complete the purchase process.**

