OPERATIONAL RISK MANAGEMENT TOOL 01

A GUIDE FOR FINANCIAL SERVICE PROVIDERS

Detailed Risk and Control Assessment (DRACA)

ACCION

UPDATED JANUARY 2024

Contents

1 What is the DRACA tool?

- **The Detailed Risk and Controls Assessment (DRACA) tool is an analysis tool for understanding operational risks faced by an institution.** This tool follows a systematic framework to identify the inherent risks in a process, and evaluate the controls put in place by the institution to address these risks.
- The detailed analysis is visually presented in an easy-to-interpret 'DRACA Dashboard,' which clearly identifies processes where risks have not been mitigated sufficiently.
- The tool is designed for identifying critical processes that, when not tightly controlled, may lead to large negative consequences for the institution from a strategic, financial, reputational, legal or business continuity perspective. A unique aspect of the DRACA tool is its ability to evaluate risks in a process according to the likelihood and extent to which they might impact the entire institution.
- The DRACA tool is flexible and can be applied to rigorously study a single process, several processes in a department, or even multiple departments. The tool assigns numeric scores to capture the extent of residual risk in a process (defined below), which is useful in comparing the risks in processes across the institution.
- Since the tool evaluates risks based on the impact they would have at an institutional level, the tool outputs are helpful for senior managers who wish to optimally allocate resources to tackle priority problems faced by their institution.

2 Tool terms

Process: For the purpose of the DRACA tool, a process is a set of activities that together produce an important outcome for the institution. Each department of an institution is responsible for a specific set of processes. For example, the commercial department is responsible for the promotion, loan evaluation, loan approval, and loan disbursement processes.

Activity: An activity is a purposeful set of tasks performed by people and systems. Each process is comprised of a number of activities. For example, the promotion process consists of activities such as “planning and preparing for sales activity,” “identifying potential customers,” “delivering sales pitch,” “handing over sales material,” and “answering questions”.

Risk Event: A risk event is an event that occurs while performing an activity that poses a risk to the institution. For example, when performing the ‘loan evaluation’ activity, it may happen that the client provides an expired identification document or shows a fake residence address – each of these is a risk event.

Inherent Risk Score: The inherent risk score (also known as gross risk) is calculated for a risk event based on the likelihood of the risk occurring, and impact on the institution when the risk occurs, assuming that there are no controls in place. The impact of a risk event is calculated considering severity of consequences for the institution from a strategic, financial, reputational, legal and business continuity perspective.

Residual Risk Score: The residual risk score (also known as net risk) is calculated as the risk score of an event after control(s) have been put in place. If the controls are effective in reducing risk of an event, then the residual risk score should be less than the inherent risk score.department, or even multiple departments. The tool assigns numeric scores to capture the extent of residual risk in a process (defined below), which is useful in comparing the risks in processes across the institution.

3 Using the tool

Why use the DRACA tool?

Obtain a big-picture overview of where the institution is exposed to operational risks.

Identify processes that require an action plan to manage residual risk and strengthen existing controls.

Build a risk awareness culture within the institution, since implementation of the tool requires that staff of each department take responsibility for identifying risks and implementing controls in their own department's processes and activities.

Who can use the DRACA tool?

Senior management and/or the Board of Directors can use the tool to identify processes and activities across functional areas that increase the institution's risk exposure, and to hold specific departments accountable for risks originating in their departments.

Department heads can use the tool to prioritize process improvements such as to introduce additional controls to mitigate risk.

Risk managers can use the tool to aggregate residual risk at an organizational or functional level, and see it evolve over time. Additionally, they can track the gap between inherent risk scores and residual risk scores over time as a proxy for effectiveness of controls, and effectiveness in managing risk.

3 Using the tool

What is required to use the DRACA tool?

- **Process maps and manuals** of the institution's policies and processes are recommended tool inputs to ensure that the DRACA has systematically documented all the processes and activities.
- **Availability of experienced staff** who can collaborate with a trained risk expert to identify risk events that have occurred (or may occur) during the performance of activities and processes, quantify the likelihood and impact of risks, and evaluate the effectiveness of controls.
- **A trained risk expert** to collaborate with the departmental staff to ensure risk scores are consistently applied, and to compile and report on the findings of the DRACA tool.

4 Tool results

The DRACA Dashboard is a heat map that shows inherent risk and residual risk for processes across departments.

For each department, every process is assigned a color code based on the inherent and residual risk scores calculated for that process. This provides a visual overview of risk arising from processes across departments and allows management to focus on problem areas.

When risk controls are in place, the residual risk colors indicate similar or lower risks than those for inherent risk in the processes. In the example to the right, the DRACA tool identified two activities with high inherent risks that were reduced due to effective controls put in place by the institution.

Usually, managers are interested in the residual risk dashboard since it shows the “current” risk situation (i.e. the risk remaining after controls have partially mitigated the risk). It is also possible to view inherent risk and residual risk side-by-side to visualize the effectiveness of controls for each activity. In the example to the right, the DRACA tool reveals that the risk controls implemented in the HR department are effective.

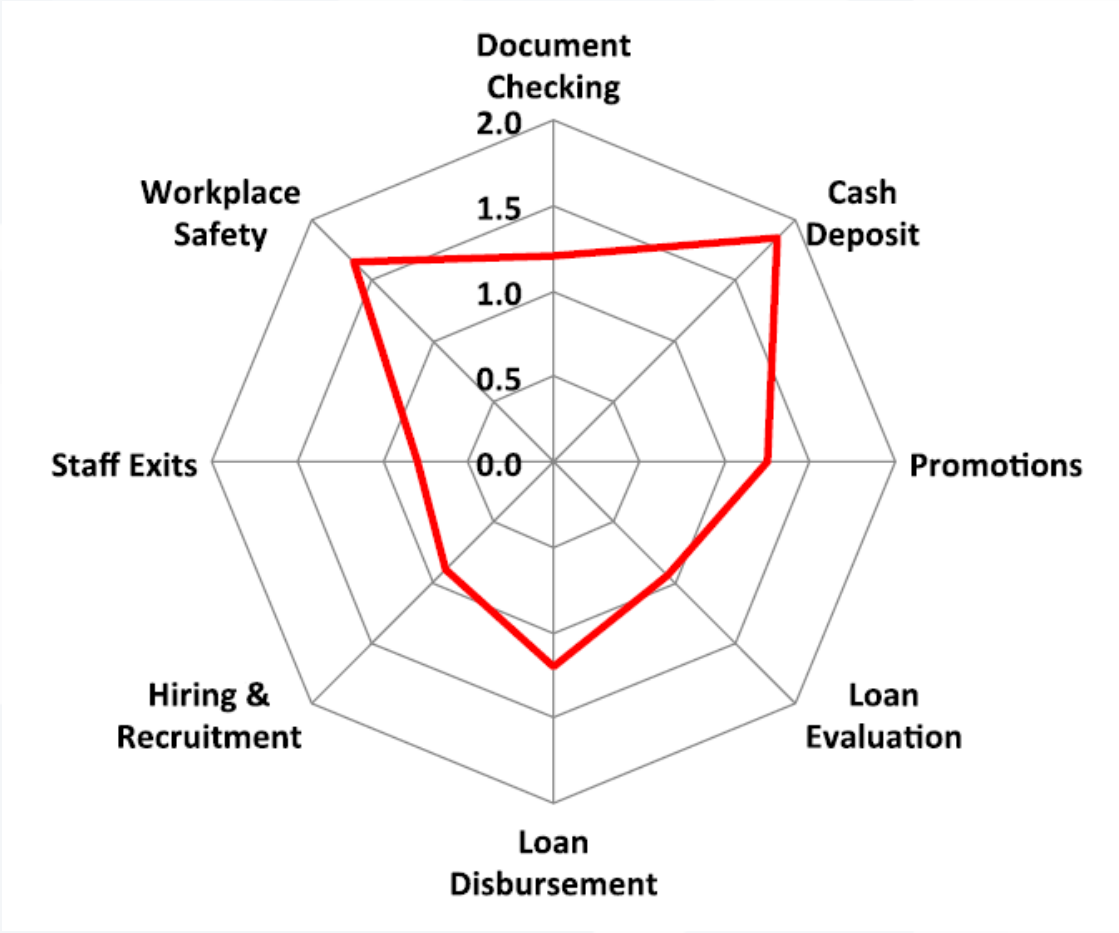
4 Tool results

A Radar Chart shows the residual risk score assigned to key processes by the DRACA tool.

The score typically ranges between 0 to 10 but may vary depending on the ranges used by the institution for measuring the likelihood and impact of a risk event. In the radar chart, each process occupies a spoke, and its risk score is marked along the radial length of the spoke.

Processes may be arranged in order of lowest to highest score or sorted by department. Connecting risk scores across the spokes helps to quickly identify the outliers, i.e. the processes with very high and very low risk scores.

Moreover, this radar chart is very useful to show two or more iterations of the DRACA tool, where each iteration uses a unique colored line. Such a chart helps to visualize the improvements or changes in risk scores over multiple runs of the DRACA tool.



5 Key considerations

Key metrics

The DRACA tool assigns a numeric risk score to each process within a department, which represents the residual risk in that process.

The outcomes of the residual risk assessment can be used to create an information dashboard for management to visualize trends in risk scores.

A dashboard may include:

- Average risk rating of the top ten riskiest processes at an institutional level and top five on a functional/specific department level.
- Number of processes where the risk rating increased and decreased over the quarter, or since the last run of the DRACA tool.

Tool variations

The residual risk scores of activities can be aggregated to calculate a residual risk score for each process or department. This provides useful insights for management to understand how the overall risk exposure of the institution is attributed to departments. Note however that such aggregation is only meaningful if the DRACA tool has been implemented across all key departments and processes.

Complementary tools

The Branch Risk Transaction Reports can be used as inputs into the DRACA tool. Managers collate the Branch Risk Transaction Reports based on risk events that have occurred at the branch level in the past. This information can serve as a useful input when identifying the risk events in the DRACA tool. See the Branch Risk Transaction Reports Guide for more details.

5 Case study

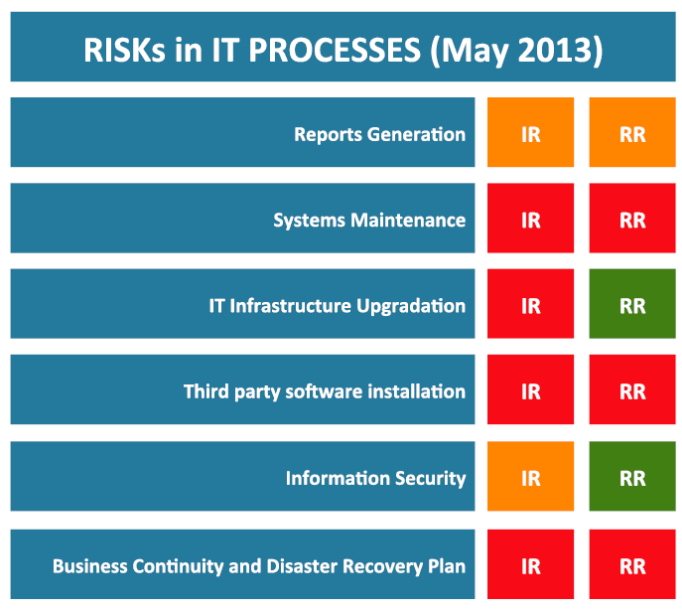
Institution	CCB Bank is a mid-sized bank offering microfinance products in Africa. After operating for five years, it achieved a loan portfolio size of $40 million with 25,000 active clients. It offers two loan products and three savings products supported by nearly 500 employees. CCB's main product is a working capital loan for small to mid-sized businesses.
The problem	CCB Bank recently faced significant challenges such as delays in closing of accounts by end of day, delays in management reports by up to two weeks, and errors in reported portfolio size and status. CCB recently rolled out a new core banking system to support its future growth plans. This new system integration had not gone smoothly and caused disruptions in several related processes. Recognizing the need for a better understanding of the operational risks facing the bank, and to encourage the relevant departments to take responsibility for operational risks arising in their areas, the senior management of CCB decided to deploy the DRACA tool.
How the DRACA tool was used to diagnose the problem	The DRACA tool was run twice in CCB during the year, in May and again in October. The two outputs of the DRACA tool are shown in Figure 1. The first run of the DRACA tool showed high residual risk in three key processes within the IT department: "Systems Maintenance", "Third Party Software Installation" and "Business Continuity & Disaster Recovery Plan." The contributing risk events were (1) The new core banking system had not undergone test runs after changes were made in the system; (2) Feedback from the User Acceptance Testing was not documented and implemented; and (3) Scheduled tests on the disaster recovery centers were skipped in the past year. The DRACA tool also reinforced findings from the Audit department that had highlighted several deviations from established policies within the processes of the IT department.

5 Case study

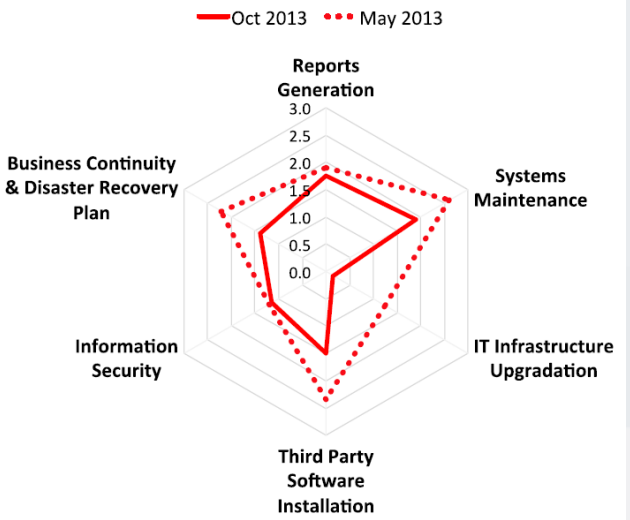
Figure 1

The DRACA dashboard only shows IT processes. The columns on far right show risk scores for inherent risk and residual risk for each process

DRACA Dashboard



Radar Chart



Insights and solutions

- An in-depth investigation into the causes of these IT-related issues revealed that attrition at key levels in the IT department had caused many of these risk events to go unnoticed for several months.
- As a result of the DRACA findings, CCB's senior management identified the most critical positions that had to be filled in the IT department. They then worked out a plan to address the most critical IT issues that had affected operational continuity. Within five months, many of the IT-related processes had shown improvement as illustrated in the radar chart for the DRACA run in October.

The DRACA tool guide is one of a four-part series including guides on Branch Transaction Risk Reports, Credit Scoring, and Portfolio Quality Analysis (PQA).

Learn how to implement these tools and how we can help manage operational risks.

Contact us

Andrés Calderón
Vice President, Risk Management
accion.org | acalderon@accion.org

Accion is a global nonprofit on a mission to create a fair and inclusive economy for the nearly two billion people who are failed by the global financial system. We develop and scale responsible digital financial solutions for small business owners, smallholder farmers, and women, so they can make informed decisions and improve their lives. Through targeted investment strategies, advisory, and expert thought leadership, we work with local partners to develop and scale cheaper, more accessible, and customer-friendly financial solutions. Since 1961, Accion has helped build more than 230 financial service providers serving low-income clients in 75 countries, reaching more than 350 million people. More at accion.org.

Accion Advisory combines decades of on-the-ground experience with insights into new technologies to help institutions overcome the strategic and operational challenges they face in driving change. With a presence in North America, Latin America, Asia, and Africa, our experienced global team delivers advisory support through integrated service offerings and products — all focused on deepening the impact of providers on underserved clients. Learn more here.

First published 2016 with support from JPMorgan Chase Foundation.