Process Mapping Synergy Gains From BCP and DR

Understanding how processes work and where controls are needed is crucial for organizations to improve their efficiency. Process mapping is a common place to start. Process mapping is the graphical representation of business processes in swim lanes using a diagram mapping application such as Microsoft Visio. It depicts business processes from start to finish as they flow from one business unit or application to another. Process mapping was developed to identify and manage the white space[1] between departments and eliminate the silo effect between departments and bottlenecks to bring products to market sooner, lower costs and, ultimately, improve profitability. Process mapping can also enhance audit and control functions. It can be used to determine if existing controls are working as intended. It can also uncover gaps that have previously gone unnoticed or unreported or have recently emerged due to external threats or other changes over time.

Process mapping can also be used for training and, more important, can lead to a widespread understanding of how processes work rather than dependency on a single employee who could leave the organization and risk leaving a knowledge gap resulting from their absence. Process mapping can be used throughout the organization and for multiple purposes; however, to better respond to the ever-increasing velocity of change to the threat landscape, the scope of process mapping should expand to include two key concepts of business continuity planning (BCP) and disaster recovery (DR). This is a necessary change—a paradigm shift—in how organizations must view and treat risk.

Process Mapping

Traditional swim lane-based process maps depict the current state of a process and may identify related controls, but they can also be used to depict the future target state of a process and help plan the implementation of a new control. A well-thought-out process map should also identify new risk that requires new controls to protect the organization. It should clearly identify if the process is subject to regulations such as the US Sarbanes Oxley Act of 2002 (SOX)[2] or the US Gramm-Leach-Bliley Act (GLBA).[3] The relevant policies that govern the process should be included in the map. In addition, the applications, servers, databases and other systems that drive the process should be included. Process maps help identify ways to improve processes as they move from one department to another.

Including BCP/DR Concepts

Expanding process mapping efforts to capture key BCP and DR concepts is especially important for processes that enable an organization to recover from a disaster. BCP/DR concepts such as single points of failure (SPOF), recovery time objective (RTO), recovery time capability (RTC), recovery point objective (RPO), recovery point capability (RPC), estimated recovery time capability (eRTC)

ALONZO LONGSHORE | CISA, CRISC

Is a senior IT segment risk specialist and assistant vice president at a US Midwest regional banking institution. He has experience in cybersecurity and infrastructure control uplift process mapping, business continuity planning (BCP) and technical third-party risk management. He can be reached at DiamondPhox@outlook.com.

"In the case of a SPOF in the form of personnel, the map should clearly state whether there is a trained backup employee who can perform the same duties."

and composite estimated recovery time capability should be considered and incorporated into process maps in the form of a matrix (**figure 1**). Incorporating these concepts does not add significant effort or time, but it will result in a more holistic view of a process, including the controls, potential process improvements and BCP/DR insights.

SPOF

A SPOF can be defined as "A resource whose loss will result in the loss of service or production."[4] This resource may be a colleague, application, server or other type of asset. At a minimum, known SPOFs should be identified and listed in every critical process map. If there is an interim workaround or mitigation approach, this should be noted as well. In the case of SPOF in the form of personnel, the map should clearly state whether there is a trained backup employee who can perform the same duties. The key risk concept here is availability. If and when a disaster occurs, it is critical to an institution's survival to restore vital operations as soon as possible. All SPOFs should be known, listed and updated on a regular basis (i.e., at least annually or when there is a change in a process).

Recovery Objectives

RTOs and RPOs establish expectations for recovery timelines for operations, applications, systems and data, and acceptable data loss. RTOs should be verified and documented in disaster recovery testing. The applications that are critical to the process should be listed in the matrix, especially if they are critical to ongoing operations or the protection or gathering of data. For example, if an application is used to track capacity usage or for identity and access management, it should be listed in the matrix. Depending on the complexity of the process it may also be listed in a swim lane that describes its role in the matrix. The matrix is intended to be used as an at-a-glance summary of a process.

RTOs and RPOs should be reviewed on a regular basis. Organizations should know the time it takes for an application to recover and the data loss tolerance. Another key question to ask is whether the organization depends on other applications or systems to recover before the primary application can fully recover (e.g., database server first, database application second, data third, application layers fourth, integration and communication fifth). This is where the BCP/DR concept of RTC comes into play. RTC is defined as:

> *The demonstrated amount of time in which systems, applications and/or functions have been recovered during an exercise or actual event, at the designated recovery/alternate location (physical or virtual). As with RTO, RTC includes assessment, execution, and verification activities. RTC and RTO are compared during gap analysis.*[5]

If an organization needs a process or service to recover in four hours, but the application or system on which they are dependent requires eight hours to recover, then a gap exists. The enterprise may need to develop a workaround, purchase a solution that meets the requirements or raise the RTO so that it is in line with existing capabilities. If no workaround exists, then one must be developed. If the cost of the

Figure 1
Matrix Prototype

Line of Business	Process Map Name	Individual Process Maps	Is This Process Related to SOX, GLBA, Crown Jewels or N/A?	Policy Number	Dependent Applications	Line of Business RTO	Application RTO	Line of Business RPO	Recovery Point Capability	System eRTC	Composite eRTC	Does This Process Involve a SPOF?	If Yes, Is There a Workaround?	Does Risk Acceptance Exist?	Are all Apps Related to the Process Being Used Listed in the Configuration Management Database (CMDB)?	For Apps Not Listed in the CMDB, What Is the Scheduled End Use or Addition to the CMDB?	Finding/ Action Plan Number(s)
		Process 1			Application 1												
		Process 2			Application 2												
		Process 3															
		Process 4															

fix is prohibitive, then the risk of that gap should be acknowledged and accepted or further analysis of the RTO must occur. The same exercise should be conducted for the RPO and RPC, which is "the point in time to which data was restored and/or systems were recovered (at the designated recovery/alternate location) after an outage or during a disaster recovery exercise."[6] Again, these data elements should be readily available and can easily be added to the matrix (**figure 1**).

Application Status

The final BCP/DR element of the matrix is application status, and it is used to determine the status of all applications in use. It is possible for organizations to have test applications that are not entered into the central database management system, but they could be in the test stage for extended periods of time. Therefore, they should be included in the matrix because they then can be accounted for should there be an unforeseen disaster. This is especially important for applications used for processes considered to be high risk. Their impacts on strategic planning can be known and contingency plans developed if the applications contain bugs or gaps that are being addressed in the test phase. This should include all applications designated as Software-as-a-Service (SaaS).

Conclusion

The addition of the BCP/DR matrix to process mapping can benefit internal audit, second-line and first-line functions; domain and executive leadership; and the BCP/DR office. This document can be used to perform at least five functions:

1. Verify control design and understand execution
2. Provide context for changes to processes and controls
3. Determine gaps and opportunities for improvement
4. Review the impact of BCP/DR threats
5. Assist in the business impact analysis phase of BCP

Because the matrix is concise and concentrated, it can serve as a reference for those making executive/strategic decisions. The lines of business—audit, executive leadership, and the BCP and DR teams—can use it as a one-stop view of the impact of individual processes across the organization. Expanding process mapping to include BCP/DR provides a more holistic, enterprisewide view of a process's impact on risk and potential process improvements and assists with disaster preparedness and the business impact analysis phase of BCP. It is a low-cost way to foster a paradigm shift that can identify and mitigate risk across the organization.

"Expanding process mapping to include BCP/DR provides a more holistic, enterprisewide view of a process's impact on risk…"

Endnotes

1 Rummler, G.; A. Brache; "Managing the White Space," Training, January 1991, *www.tlog.lth.se/fileadmin/tlog/Utbildning/Kurser/Logistik_i_foersoerjningskedjor/Artiklar/Rummler_and_Brache.pdf*

2 US Sarbanes-Oxley Act of 2002, P. L. 107-204, 30 July 2002, 116 STAT 745, *https://www.congress.gov/bill/107th-congress/house-bill/3763/text*

3 US Gramm-Leach-Bliley Act, P. L. 106-102, 12 November 1999, 113 STAT 1338, *https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf*

4 ISACA®, Glossary, *https://www.isaca.org/resources/glossary*

5 Staff, "Recovery Time Capability: Concept and Context," *Disaster Recovery Journal*, 11 October 2011, *https://drj.com/journal_main/recovery-time-capability-concept-and-context/#:~:text=Recovery%20time%20capability%20is%3A%20%E2%80%9CThe,assessment%2C%20execution%20and%20verification%20activities*

6 Staff, "Recovery Point Capability (RPC)," *Disaster Recovery Journal*, 23 July 2019, *https://drj.com/bc_glossary/recovery-point-capability-rpc/#:~:text=by%20DRJ%20Editorial%20Team%20%7C%20July,during%20a%20disaster%20recovery%20exercise*