Assessing and Managing IT Operational and Service Delivery Risk

Service resilience has gained a lot of importance in recent years. A resilient service is one that is capable of withstanding major and minor disruptions caused by natural and man-made sources. Service resiliency is best ensured before any change is put live in the service. Hence, the assessment and management of IT operations and service delivery risk during the project life cycle assumes a great deal of importance. Designing and implementing an IT operations and service delivery risk assessment process can be embedded in the systems delivery life cycle (SDLC).

IT risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It is categorised into:

1. IT benefit/value enablement risk
2. IT programme and project delivery risk
3. IT operations and service delivery risk

The third category of risk is focused on here. IT operations and service delivery risk is the risk associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to an enterprise. An example of such risk is a critical service that is live without adequate disaster recovery (DR) provisions. For day-to-day IT operations, the assessment and management of this category of risk is vital, as this category of risk has the most visible impact on the end user.

IT operations and service delivery risk could be understood as a stack comprised of three layers:

1. **Existing IT operations and service delivery risk**—This is existing risk in the live environment. It could also include residual risk already accepted by the enterprise. Most organisations have remedial programmes in place to handle this layer.

2. **IT operations and service delivery risk caused by environmental changes**—This layer of risk includes the risk introduced due to changes in environmental/external factors. For example, if a vendor declares a particular version of an operating system out of support, new risk is introduced to the existing risk profile of the services that have unsupported versions of the operating system.

3. **IT operations and service delivery risk introduced by the projects**—Projects continuously change existing solutions, or add new solutions to the existing services or create new services. New risk is introduced through the projects/programmes going live with unmanaged or misunderstood risk.

In large, complex IT organisations, understanding the risk and impact of individual IT projects can add real value to decision makers and strategic IT thinkers. IT operations are constantly in a state of change and a simple error or an aggregated thematic issue from IT projects can destabilise critical systems and applications. Some recommendations based on experiences in a global and complex IT environment serving one of the world’s largest financial institutions are described here.

**KEY RISK CATEGORIES TO BE MANAGED**

While the risk process employed for managing the IT operational and service delivery risk is the focus here, a brief summary of the key risk categories assessed through the risk process gives context to the risk process:

- Failure of infrastructure and application resulting in disruptions and nonavailability of IT systems
- Inadequate business continuity planning (BCP) and DR, resulting in the inability to support business and operations and, ultimately, resulting in losses
- Failure to follow defined change incident or problem management processes, for example, resulting in service disruptions and nonavailability
- Failure to engage with service management and put service documents in place, resulting in no or inadequate support for users
• Unresolved security issues introduced into the production environment, resulting in compromised security
• Failure to apply standard logical access management controls, resulting in unauthorised access and losses

This is not an exhaustive list. The controls to be validated with an IT operational risk assessment process should be derived from the organisation’s risk and control framework. Sample control questions that relate to the risk of inadequate BCP and DR resulting in the inability to support business and operations and, ultimately, resulting in losses are illustrated in figure 1.

A generic risk and control questionnaire is seldom found to be useful for such assessment. Thus, the organisation should prepare its own IT operational checklist, which should be derived from its risk and control framework.

KEY SUCCESS FACTORS

Based on the experience of running a similar process in a very large and complex financial institution, the following essential ingredients of an effective and efficient IT operational risk assessment process have been identified. At the end of each success factor, a practical tip is provided that can help put each idea into practice. The tips are summarised in figure 2.

**Align a Project Risk Process With the Needs of the Business**

Aligning the size and scope of the IT operation with the risk appetite of its leadership is a vital first step. Establishing those appetites through effective stakeholder management creates a baseline for a project risk process to be built. In a complex IT operation impacted by more than 1,000 projects per year, an assessment model run and driven by the IT risk and security

---

**Figure 1—Sample Control Questions**

<table>
<thead>
<tr>
<th>No.</th>
<th>Control Question</th>
<th>Control Response (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Will the proposed solution to be implemented by the project automate a new business process or introduce a new service?</td>
<td>In case of a no answer, please prepare an action plan.</td>
</tr>
<tr>
<td>2</td>
<td>If yes to question 1, has the business sponsor conducted a business impact analysis (BIA) and provided the criticality rating to the project?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>If the project is implementing a high or medium criticality rating business process/service, has the project provided a DR environment?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Does the DR environment exactly replicate the production environment in all respects? Does the DR environment exactly replicate 100 percent of the production environment in terms of capacity and performance?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Has the DR environment been secured with the same level of security as the production environment?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Has the DR environment been certified as fit-for-use by the security team?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Has the project prepared a DR plan or updated an existing DR plan?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Does the DR plan cover all processes and procedures required to activate the DR site?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Has the DR solution been tested successfully by the project?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Has the project been able to demonstrate successful achievement of recovery time objectives (RTOs) and recovery point objectives (RPOs) during the DR test?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Have the business process owners and operational team participated in DR testing and approved the results?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Have the DR environment, DR plan and DR test results been handed over to the central DR team for continued maintenance?</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Has the business sponsor updated the business continuity plan to reflect the changes in the business process introduced by the automation/project?</td>
<td></td>
</tr>
</tbody>
</table>

Source: Copley and Parekh. Reprinted with permission.
function will not sustain itself. In this type of situation, a self-assessment method should be employed, but with clear process ownership (IT risk and security) aligned to process execution accountability and risk ownership (project and programme leads handing in to the IT operations functions).

Idea in practice: The IT operational risk assessment should be a self-assessment undertaken by the project manager. Any unmitigated risk, in line with the risk appetite set by the business head, should be accepted by the service managers responsible for live service.

Make Assessing Risk Part of a Standardised and Mandated SDLC

A stand-alone operational risk assessment for IT projects runs into compliance and ownership issues if it is not part of a standard SDLC. An IT risk function can spend valuable time attempting to influence a huge project and operations community to be good corporate citizens, rather than establishing a developmental standard via a mandated SDLC from the very beginning. Embedding a project risk assessment within a standardised SLDC framework means the IT risk function can put more effort into supporting the quality of input and output, rather than persuading projects to be compliant.

Idea in practice: The completion of an IT operational and service delivery risk self-assessment process should be checked as a part of the stage-gate process in the SDLC. Remember, adherence to a self-assessment process would be as strong as the organisation’s SDLC compliance.

Use Standard Risk Questions Combined With a Scoping Mechanism

An early issue when implementing an IT project risk assessment is that project leads do not understand how to complete the assessment and become concerned that the scope of the assessment does not take into account the particulars of their development. To combat this, the creation of a set of standard control-related questions aligned to the IT operations risk and control framework can be employed. A scoping mechanism that expands and contracts the size of assessments depending on development activity can also be developed to create a process that helps understanding and creates specific assessments.

Idea in practice: It would be a good idea to use a standard questionnaire for the self-assessment. Any questionnaire should be reviewed by the sample stakeholders, including the service managers and project managers. Piloting new questionnaires on select projects can help sharpen the focus.

Figure 2—IT Operational Risk Process Recommendations

- Embed the process within the enterprise SDLC.
- Use a self-assessment process.
- Use an enterprise-wide tool set.
- Devise a robust exception-handling process.
- Keep it simple and easy.
- Base the risk area to be assessed on the nature of the project.

Source: Copley and Parekh. Reprinted with permission.

Build Trust Relationships and Establish Specific Roles

In a complex, global IT operation, a self-assessment process will work more effectively if all stakeholders and actors know their role. Projects having accountability to perform assessments and present their final risk profile to their operations counterparts for approval being a key element. In an IT SDLC, it is also beneficial for the owners of individual processes (e.g., enterprise design, architects, designers, testing teams, the IT risk and security functions) to understand how their processes and methods overlap. This understanding leads to opportunities for streamlining, which, in turn, leads to life being made easier for a project team.

Idea in practice: A Responsible, Accountable, Consulted and Informed (RACI) matrix embedded in the SDLC is handy to crystallise roles and responsibilities. Training and communication are keys to driving the sense of ownership among the project managers and service managers.

Employ Enterprise Tool Sets

If an IT project risk assessment is placed in an enterprise-wide tool set and used consistently across the technology estate, governance and compliance becomes simple and, in some cases, automatic. If an IT operation deploys a central SDLC governance reporting framework that scans the enterprise tool sets within the SDLC, business rules can be constructed that indicate when assessments are completed, submitted, approved or finalised. Compliance to SDLC processes and, in this case, the IT project risk assessment then becomes simple and almost binary in nature.

The other advantage of a consistent enterprise-wide tool set for IT project risk is that the mechanism can incorporate approvals and sign-offs that allow a project to be guided through the assessment.
Idea in practice: Microsoft Excel can jump-start any new initiative. As the process matures, standard risk assessment tools may be used for administering the entire process.

Make It Easy
IT control assessments can, by their very nature, be complex. In an agile project moving at full speed, complex control assessments will not fit easily. In this situation, an assessment will either not be completed regardless of consequence or the quality will be compromised. To avoid this and to build an assessment mechanism that can be used regardless of development methodology, it is crucial to use simple scoping mechanisms combined with easy-to-understand questions.

Idea in practice: Deploying a very early, simple assessment question set can be used to determine the need for further assessment. If questions are weighted with impact, scoring a result can be presented and a project then completes or continues the assessment task. For projects moving to a wider risk assessment, the project can still scope out the size of the assessment. For example, if a project has no impact on current supplier arrangements or is not bringing in new suppliers, it should not be made to spend time on assessing supplier-related risk.

Have Consequences
While scoping, automating and easy question sets are favourable, there must always be a consequence to not completing or following the assessment process. For example, when a project gets to a final go/no-go decision and cannot evidence its final risk profile, what confidence does the change approval board have that the changes will be available, secure and operationally stable? It is recommended that a lack of evidenced risk assessment and sign-offs should be a hard stop to a release slot.

Idea in practice: Tightening the controls around compliance to the process should be gradual. It helps to address resistance to change.

Report and Monitor Effectively
Finally, while the previously described recommendations can establish an effective IT operational and service delivery risk assessment across the IT organisation, the IT risk function must analyse inputs and outputs. Providing monthly, weekly or even daily monitoring of project risk profiles should be considered a standard offering of an IT risk function. Risk analysis through trending of common themes is very useful as projects can highlight issues with operational processes that could be slowing delivery or creating control gaps and weaknesses.

Idea in practice: Monitoring compliance to this process in conjunction with an SDLC governance function allows the IT risk function to pinpoint issues with process understanding or examples of poor behaviours.

CONCLUSION
IT projects introduce different operational and service delivery risk to live services. It is essential that such risk should be assessed and managed before the project goes live. This can be achieved only if there is a robust and sound IT operational and service delivery risk assessment process designed and implemented by the organisation. While the operational risk areas to be assessed by the process depend upon the IT risk and control framework of the organisation, there are certain essential ingredients to the process. A robust self-assessment process embedded within an SDLC process that includes effective adherence monitoring, supported by an enterprise-wide tool set, has proven successful in meeting the end objectives.

ENDNOTES
1 ISACA, COBIT® 5, USA, 2012, www.isaca.org/cobit