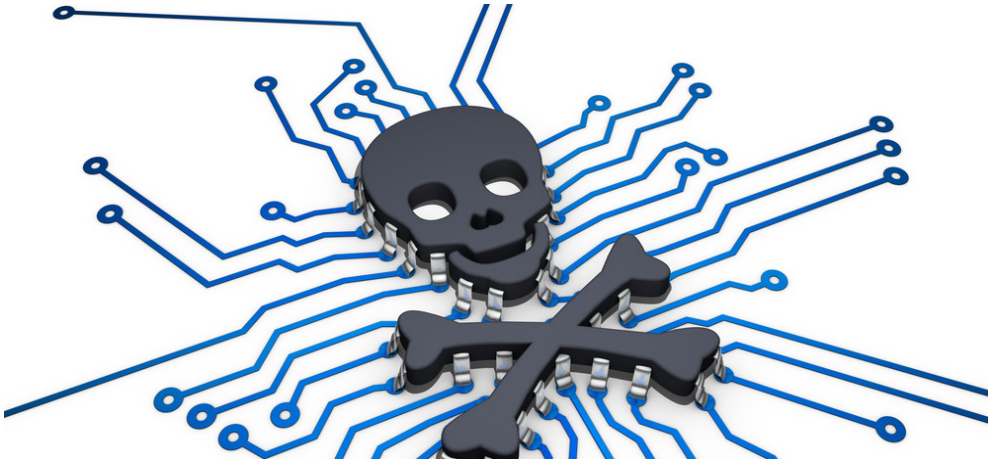
IT Risk Management – What's the catch, what to watch

abstract

Today, Information Technology (IT) is not only considered as a business enabler but also as a tool for market leadership and competitive advantage. Modern global businesses rely on IT to provide direction and insights. We have witnessed the growth of global organizations that have leveraged IT to connect and empower employees, customers and partners across the globe. Organizations that build online social media, mobile applications, chat and voice calling services etc, have made enough gains to make the point very vivid. In line with the latest IT trends, application and data center are being leveraged from cloud services, remote management services are very popular, organizations data is contained in data marts across the globe, Bring Your Own Device (BYOD) is gaining acceptance as employees prefer the popular hand held consumer devices over mundane corporate allocations. Clearly, riding on the wings of technological advancements enterprise IT is rapidly changing and becoming highly complex. This on one hand, if has empowered businesses, but on other side, by its very nature has brought in new risks to be assessed and managed. Organizations must identify measure and manage these risks to ensure smooth business operations.

This white paper intends to put together a broad definition of IT risk, highlight IT risk management strategies and apprise readers about a few pitfalls that must be avoided while formulating ITRM strategies.

IT risks and impact



As per the ISO definition of IT Risk – "It is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence."

Risk (R) = Probability of IT incident occurring (P) × Consequence to the organization due to the incident (C)

For most organizations, IT services are closely associated to their corresponding business services. Similarly, most IT risks have an associated implied business risk within the organization. Thus, the Impact of IT risks must be assessed across both technical and business factors.

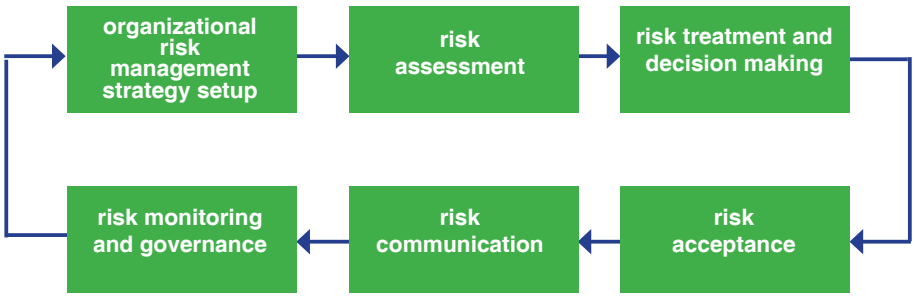
Technical impact can be measured across traditional factors like availability – service not available and its criticality, confidentiality - data disclosures and its sensitivities, integrity – data corruption, loss or damage, and accountability – traceability and associated actions. The objective is to estimate the magnitude of the impact on the system if the incident were to be exploited.

Business impact originates from the technical impact and requires a thorough understanding of what is important to the organization. The businesses risks to a large extend are used to justify investment in fixing IT risk incidents. Traditional business factors include financial damage, reputation damage, non-compliance and privacy violation.

IT risk management

IT Risk Management (ITRM) provides the overall risk and control framework that enables the most important control objectives for IT: effectiveness, efficiency, compliance, confidentiality, integrity, and availability.

An effective ITRM strategy would contain the following critical phases:



Critical phases of ITRM Strategy

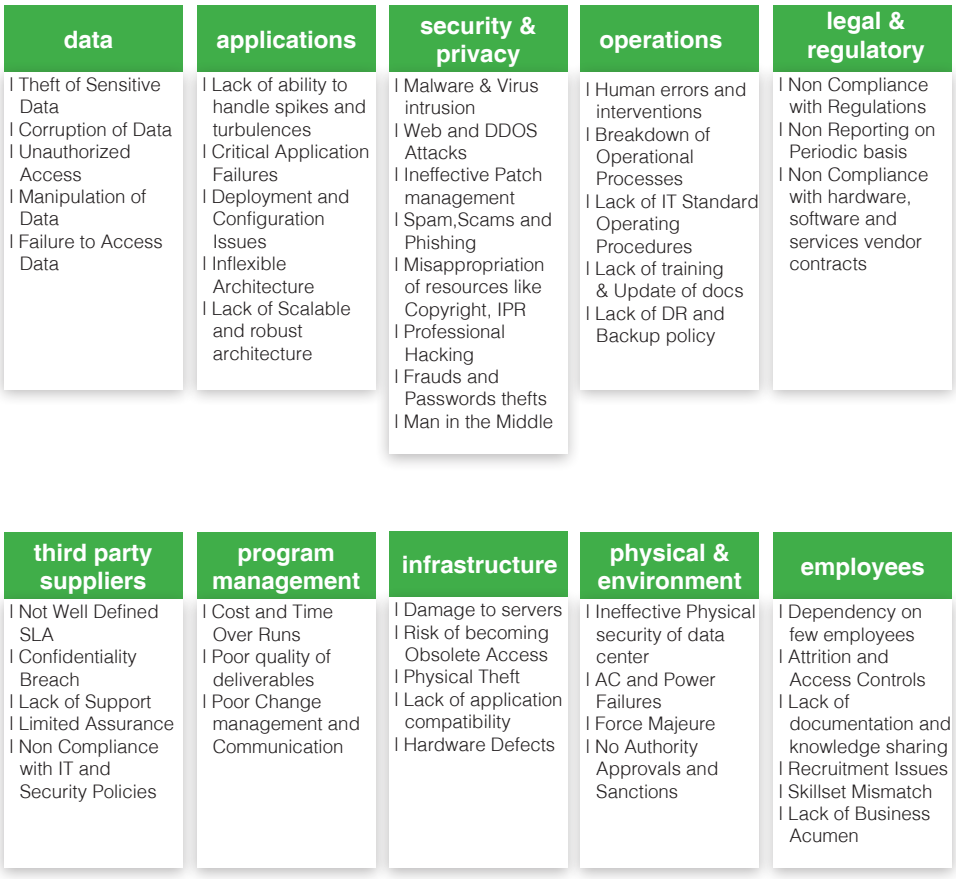


Figure 2: IT Risk Landscape

1. Organizational Risk Management Strategy Setup: This is one of the most important phases of ITRM strategy for an organization. All relevant stakeholders should determine the basic criteria, purpose, scope and boundaries of risk management activities along with clearly define roles and responsibilities.

2. Risk Assessment: Risk assessment is executed at specific time points and provides a view of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures etc. The results of IT risk assessments are used by managers to define the mitigation strategies. It is also essential that we understand the IT Risk Landscape for the modern day organizations. The figure below highlights major risk landscape for organization with relevant details.

3. Risk Treatment and Decision Making: Once the risk is identified, it is important to control and treat the vulnerabilities. The controls used to manage risks must strike a balance between cost, productivity, effectiveness and the value of the informational asset being protected.

The risk control and treatment process aims at selecting security measures to:

- *Reduce Risks* - By implementing controls that minimize the adverse impact of the threat
- *Retain Risks* – When the risk is not significant enough and/or where the possibility of remedy is either not possible or very expensive
- *Avoid Risks* – By eliminating the risk cause and/or consequence
- *Transfer Risks* – By transferring risks to third party or outsourcing where the risk could have a very high impact and is not easy to reduce significantly by means of security controls.

4. Risk Acceptance: All the risk assessments and treatments must result in a risk dashboard that must be acceptable to the senior management of an organization. In the risk dashboard, there must be a clear categorization of risks and there mitigation strategies. All known residual risks must also be shared with the management for their approvals.

5. Risk Communication: The purpose of risk communication is to establish a common understanding of all aspect of IT risk amongst the entire stakeholder in the organization. This is important to bring all stakeholders to a common understanding and highlight any concerns. Communication also influences decision making.

6. **Risk Monitoring and Governance:** ITRM is an on-going and iterative process and must be repeated continuously as new threats and vulnerability emerge every day. Moreover, business requirements, vulnerabilities and threats can change over the time. Thus continuous governance is a must.

what to look from ITRM

1. **ITRM should be understood and supported in the boardroom:** Boards of directors and decision makers should clearly understand the significance of ITRM. They should empower organization leaders to define an approach to understand and actively govern the enterprise IT operations and risk management. This requires a mindset change, as until recently, IT was not an area of focus for most boards of directors.

2. **ITRM should be tracked as a business metric:** Traditionally, IT risk was seen as the sole responsibility of the IT department. It was not considered a strategic business risk that required an enterprise wide focus. However, with ever increasing dependency on IT tools and technology, it is essential that organizations include ITRM within their overall enterprise wide risk management approach.

3. **ITRM should have multiple lines of defense:** IT risks must be mitigated along several lines of defense with the entire enterprise IT setup. It is extremely difficult for any one single control, function, or organizational layer to tackle today's complicated IT risks. Several business support functions like legal, regulatory, finance, tax, operations, revenue assurance, fraud, HR must work together along with the IT teams, the internal / external governance and audit teams to effectively combat IT risks.

what to watch in ITRM

While it is essential that all organizations clearly define their ITRM strategies, and measure and monitor them effectively, it is essential that prevalent pitfalls are avoided. Below are some common mistakes that lead to an ineffective or/and incomplete ITRM strategy.

1. **ITRM Strategy without Context:**
   It is essential that the core group of people who are defining, measuring and reporting IT risk should have business, regulatory and market context to the initiative. Without correct and complete context, it becomes difficult to identify and provide remedy to IT risk.

2. **Excluding external ecosystem services in the ITRM strategy:**
   Today, most large and mid-sized organizations have a host of external third party vendors, suppliers and service providers. All these entities should be part of the ITRM strategy as they continuously access the organizations IT and business systems.

3. **Not making ITRM comprehensive and inclusive:**
   Most large organizations overlook key assets and indicators in their risk assessments, forget physical security as a key component of the strategy, may not include a cross functional team to be part of the initiative and ignore human intervention risks. ITRM must also complement the business dynamics of the organization.

4. **Over dependence on ITRM tools:**
   There seems to be a more than necessary reliance on ITRM tools and its recommendations. Many tools, when not setup with the correct details due to limited context, can provide incorrect insights which could lead to unnecessary, even damaging, recommendations.

5. **Taking ITRM as a routine and mundane activity:**
   When executing IT risk assessment becomes a repetitive activity that is outsourced to third parties, it often ends up becoming a mere a check in the box activity. From being a proactive initiative it turns into a reactive afterthought, which defeats the whole purpose.

6. **Not updating the ITRM strategy periodically:**
   As the world is facing newer market dynamics and forces, there is continuous enhancement in technology and there is competition thriving, it is essential that ITRM strategy is aligned with the latest in the industry and the changing threat landscape.

About ARCON

about ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.