**Application Risk Management**

Day by day, companies feel the need to put more software applications in use. As the number of software applications in a company’s application inventory increases, so are the risks of malfunctions and security issues. Application Risk Management is the framework to assess applications and identify potential threats before they even surface. This way, Application Risk Management saves time and effort along with ensuring a cost-efficient and flawlessly running the company as it points out the risks for business, providing time to prevent them.

Some examples of potential risks could be human error, unrealistic scheduling or budgeting, unidentified vulnerabilities in applications, and inadequacy to meet user or customer needs. Around ninety percent of system malfunctions, security breaches, and IT infrastructure inadequacy are, in fact, a result of dispersed application storage, inefficient architectural structure, and a complete lack of application management. See how Application Portfolio Management (APM) could be the methodical approach missing for a company’s success [here](https://loggle.io/blog/5-reasons-your-company-needs-application-portfolio-management).

Several reasons enhance the risks for applications:

1. Business systems getting more complex: Businesses need more applications to keep level with the growth of their sector today. So, business processes grow more and more complex, requiring a number of new applications to be added to the application inventory. For this reason, the risk of malfunctions and security threats rise.
2. Multi-sourcing: Multi-sourcing is quite similar to outsourcing, but it happens in the IT structure. With multi-sourcing, the IT department of a company has contracts with multiple vendors that provide each provide software applications, hardware, servers, or anything related to IT. This process may create an overall risk if poorly managed.
3. Rapid development practices: Rushing the development of applications might result in more risks for it to malfunction or fall prey to hacking. Developing an application fast is a good thing, but only if it doesn’t hinder the overall capabilities and security of the application.
4. Allocating little time for testing and insufficient resources: Similar to the fourth reason, skipping past testing or rushing would also mean drastic enhancement for threats. Methodologies like Agile or Shift-Left came into play to further optimize testing and development processes in general. So, it would be wise to modernize the processes of developing and testing so as to reduce the risks once the application is put on the marketplaces.
5. Shadow IT: Shadow IT refers to purchases without the consent of the IT department. These unbeknown purchases might result in extra threats as they are not controlled by the IT department and required cybersecurity measures.

**What are the Steps of Application Risk Management?**

Steps of Application Risk Management have not been strictly defined and they may differ from sector to sector, from company to company, or even from department to department in a business. Yet, the framework to evaluate and prevent the risks are quite similar when generalized a bit.

They could basically be as follows:

1. Identify the risk: The first step of risk management is actually noticing that there is a risk. Identifying the risk would set the necessary channels for coping with risks in motion. So, a company should form an IT landscape that makes it possible to detect risks. This could be realized with the help of an Application Portfolio Management software as APM methodology deals with monitoring applications and detecting noteworthy issues like low-efficiency or chronic malfunctions. Read more about how Application Management works for today’s enterprises [here](https://loggle.io/blog/application-management-for-todays-enterprises).
2. Evaluate the risk: Having detected the risks, assessing them is the second stage. Analyzing the size of a risk is important are to decide how much of the resources to be allocated to cope with the issue. This stage is mostly automatized.
3. Triage the risk: Evaluating the risks leads to prioritization of the risks. This way, allocating defense or repair mechanisms is optimized.
4. Treat or prevent the risk: Then, cybersecurity or repair sessions start depending on the type of the risk. Resolving the issue depends on the quality of these teams.
5. Post-monitor the risk: Having resolved the risk, timely check-ups would ensure that the same problem does not reproduce.

**How to Perform Application Risk Management?**

The basic scope of Application Risk Management has been covered. It’s practically comprised of identifying, assessing, and coping with the potential issues. In order to employ efficiently running Application Risk Management, a comprehensive and systematic approach towards applications might be beneficial. This leads to ITAM (IT Asset Management) and APM (Application Portfolio Management) which is a sub-genre of ITAM.

APM provides overall monitoring for all the applications used by a company. Some APM software may rather work as a suite and have a built-in Application Risk Management tool. If that be the case, integrated management towards both application inventories and risks can be realized. A systematic accord between APM and Application Risk Management may provide some features with high business value. They could be as follows.

1. Creating an inventory of applications in use and constant monitoring of them
2. Identifying the risks by evaluating how these applications are running
3. Scanning if an application has similar malfunctions in its history
4. Pointing out compliance issues