Many security regulations for various industries today promote or require mandatory security risk assessments. For instance, in healthcare industry, cyber security risk management is not only required for compliance to Health Insurance Portability and Accountability Act (HIPAA), but also helps the IT team and business leaders in identifying and improving the vulnerable and high-risk areas of the organization. Similarly, Payment Card Industry Data Security Standard (PCI DSS) ensures that all companies dealing with cardholder data comply with [card](http://www.cardzgroup.com/SmartTokenBands.html) and customer security regulations.

The ultimate goal of cyber security risk management is to be able to better manage all IT related risks that cover the whole organization, applications, vendors, and customers in most cases. Careful risk assessment and management leads to lesser probability of risk-associated mishaps.

## NIST Risk Management Framework

According to various publications by National Institute of Standards and Technology (NIST), including [800-30](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf), 800-39, 800-37, and 800-53, organizations get guidance to conduct risk assessment and to carry out three steps of risk assessment including assessment preparation, conducting the assessment, and maintaining the assessment.

Based upon these, below are key guidelines on how to effectively plan and conduct risk management process of your organization.

### Prepare for Risk Assessment

Your risk management strategy should essentially include the preparation of risk assessments. The following key tasks are required to perform thorough risk assessments:

* Identify assessment purpose
* Identify assessment scope
* Identify constraints and scope of the assessment
* Identify the inputs and sources of information of the assessment
* Identify analytic approaches and risk model (i.e., analysis and assessment approaches) used during the assessment

### Prepare the Scope

For effective cyber security risk management, it is best to include your entire organization in the scope. This can help assess the exact areas of risk and vulnerabilities, whether those are internal or customer-related. Your scope must be prepared in terms of supported time frame, organizational applicability, and technological/architectural considerations.

### Identify the Assumptions and Constraints

Next, you need to identify the assumptions and constraints under which you will have to conduct the risk management process. This includes identifying threats and assumptions related to the process of identifying these threats. Also determine the type of threats that should be considered during risk management and the level of details that will be required to describe those events.

### Implement a Process that Evolves

Risk management is not a one-time process. It is an ongoing process that needs to monitor risks regularly as they arise. The risk management process of an organization should be reviewed regularly since new technologies keep getting introduced. These new technologies can change where and how sensitive information is stored. When more tools get integrated into your organization’s systems, the risk of data to go into wrong hands increases.

As IT systems get updated, software applications get replaced with latest versions, and the cyber criminals become more sophisticated, it is important to train new as well as old personnel about evolving security practices. New risks keep surfacing and those that were mitigated previously can also return in the form of new vulnerabilities. Overall, the risk management process must be ongoing and should evolve to deal with existing and newly identified risks and threats.

### Share Information with Stakeholders

The [800-30](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf) NIST publication states that, “ the risk assessment process entails ongoing communications and information sharing between those personnel performing assessment activities, subject matter experts, and key organizational stakeholders (e.g., mission/business owners, risk executive [function], chief information security officers, information system owners/program managers).”

By sharing the risk assessment information, you can ensure that all inputs going into the risk assessment are credible and accurate. It also ensures that all intermediate results can be utilized to support assessments in all other organizational areas, bringing about meaningful results.

## Conclusion

It is important to prioritize risk mitigation decision based upon real data by using the organization’s risk profile. This helps identify new mitigation opportunities providing higher return on investment for a specific organization.