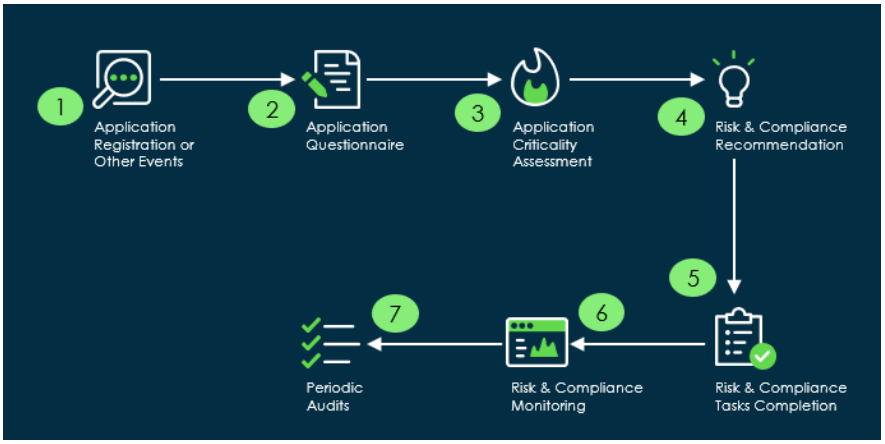
Reduce unplanned work and unpleasant compliance surprises

84% of teams don't collaborate consistently on risk reporting, according to Gartner's Top 5 enterprise risk management priorities.

Your organization is using hundreds or even thousands of applications. Managing the risk, compliance, and audit needs for each new application, throughout its lifecycle, is a massive undertaking if risk and compliance management is not embedded into the application lifecycle process. From the very beginning, where an application in registered and on-boarded through Application Portfolio Management to track licenses, maintenance, and usage – the risk the application and associated data may pose to the organization should be considered. Ultimately, applications must be continuously monitored to quickly identify vulnerabilities, if an application must be shut down it can affect the entire organization – imagine going without Teams, Email, or Salesforce? From a privacy and compliance standpoint, applications that access, store, or process personally identifiable information must be closely tracked – regulations are very clear on steps to take if there is a breach and penalties are high. If application development is in-house DevOps policies must be followed and compliance audited. The list goes on.

The integration of ServiceNow APM and IRM helps Risk Managers, application owners, application development teams (DevOps), and compliance teams work seamlessly together. It allows the traditionally silo-ed teams to continue to collaborate throughout the application lifespan without adding friction.

Realize the benefits of IRM plus APM



This diagram illustrates how IRM and APM work together to protect you from application risks

Align your application portfolio to strategic business needs- Use APM to register new applications to better manage the application lifecycle starting with on-boarding. Registering the application in the ServiceNow platform with APM allows application managers to add "Information Attributes details", "stakeholders" and other basic information about the application. For every new application created in APM, an application questionnaire gets automatically generated and assigned to an application owner for an inherent risk assessment. This increases communication and collaboration between business owners , Risk, and IT teams

Innovative features make IRM and APM work for you

Business lifecycle management

APM tracks value, risk, and cost in addition to the risk posed by outdated technology.

Advanced risk assessments

Use responses that are pulled directly from the platform to keep assessments and risk scores current.

Privacy assessments

Identify sensitive data that applications request, process, transfer, and store to ensure you at mitigating potential privacy risks and penalties.

Recommendations and automation

Let IRM recommend risks, citations, and policies then automatically generate controls to reduce effort and costs, while driving greater efficiencies.

Continuous Monitoring

Real-time visibility into application risk and compliance is essential to quickly responding to threats and vulnerabilities.

Dashboards

Provide oversight for stakeholders at all levels.

Operational Resilience

Gain insights into critical services, plus use scenario and continuity planning to prepare for adverse operational events.

Optimize application architectures to business processes- Application questions are designed to be used by frontline employees. These questionnaires provide details to perform impact assessments and generate reporting metrics to identify how the application will be used in an organization, if it will touch PII or sensitive data, and how PII will be accessed by users, processed, stored, and retired. A better understanding of how sensitive application data is used can help reduce exposure to threats.

A risk identification record against the application will automatically be created. Once the perceived risks are documented risk managers can perform inherent risks assessments with the click of a button. If the applications are associated with a vendor a third-party risk assessment can be generated tying your enterprise and third-party risk processes together.

Lower costs and increase efficiency– Risk assessments are designed for the risk team to assess application criticality (confidentiality, Integrity, and Availability). The responses can be setup to be manually entered or automated. Automated responses pull data directly from the platform and are updated as the values change, keeping the risk assessment and risk score current. The inherent risk assessment will now go to the business owner for approval.

Tracking licenses in APM and automating processes lowers license and operational costs. The various automated features such as pulling data from the platform, generating the risk score, making recommendations, and generating controls combined with sharing data across a common platform increases efficiency.

Reduce manual effort – IRM will automatically recommend risks, citations, and policies based on the defined information objects (such as name, ID, etc.) to make the selection and implementation easier. This results in risks, citations, and policies being tagged to the risk identification record. Based on the policies and citation tagged, controls can be automatically generated by clicking a single button.

Relocate valuable resources– Risk and compliance tasks, such as taking a control assessment and providing an attestation are made readily available for application owners. Making work easier frees up people to work on higher value tasks.

Avoid regulatory compliance penalties– Continuously monitor controls to identify compliance violations, risks, and vulnerabilities associated with critical applications. Real-time visibility is essential for quickly addressing changes in risk or threats. Siloed visibility and governance makes complying with evolving regulations difficult and identifying risk challenging. The Security Operations Vulnerability Response product is valuable in identifying vulnerabilities to help mitigate risk.

Reduce investment in legacy apps (technical debt) – Use dashboards, technology lifecycle plans, periodic audits, and processes to regularly certify applications, track maintenance and usage. These can help identify applications that can be retired (are no longer or under used) or pose a risk because of outdated technology. Dashboards are particularly helpful for executive stakeholders to gain an overall view of application risk and compliance posture across the organization.

Enable successful implementations

There are many opportunities to learn not just the product but also implementation strategies for IRM. Now Learning Success Packs help deliver successful outcomes to projects. ServiceNow Expert Services can not only assist in the implementation of IRM or APM but also can recommend implementation methodologies. There are several implementation partners that offer deep technical expertise, services including quick starts for a faster time to value, and domain expertise in the solution you're deploying, ServiceNow Assure is a collaboration between ServiceNow and your selected Professional Services provider. And finally, you can take advantage of live and on-demand implementation and product training.

servicenow.