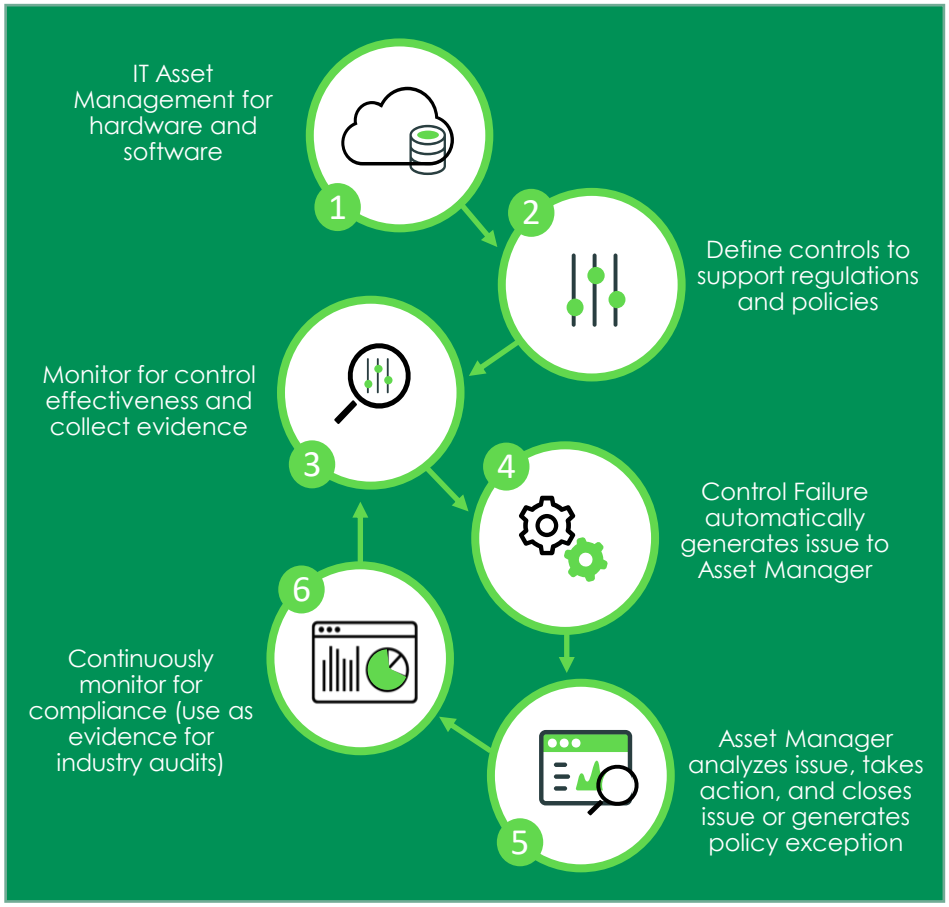
The more you know the lower the risk

A governance paradox

According to Gartner, "84% of teams do not collaborate consistently on risk reporting[1]". You can put governance in place with as many policies as you want, but unless you know what you have, how it's being used, and the way it impacts your business, you'll still lack control over your environment. It's critical to manage the lifecycle of hardware, software, and cloud resources. Equally important is to have good overarching governance in place to help ensure compliance to regulatory requirements (SOX, GDPR, NIST, DORA, ESG, etc.) and processes the business has put in place. To do that, you need consistent collaboration across teams. You also need comprehensive IT asset management (ITAM) for software and hardware assets and a flexible and scalable risk and compliance solution that utilizes a common platform to share data and build response workflows across the enterprise (IT, Finance, and Risk).



The combination of ITAM and Integrated Risk Management (IRM) can help reduce unplanned work and unpleasant compliance surprises.

Tech Tip: From the ServiceNow Store, to quickly put controls in place, use the Sarbanes-Oxley (SOX) Content Pack for financial processes; for your most critical IT assets use the Cybersecurity Controls Accelerator and Technical Controls Accelerator, then begin continuously monitoring for compliance & risk.

Achieve peace of mind

- Approach regulatory audits with the peace of mind that you have the data and evidence to prove compliance across whatever required time period.

Save time and money

- Take back the time spent snapping screenshots, filling out spreadsheets, and running reports provided to auditors.

Gain a level of governance and oversight for critical processes

- Mistakes in some processes can cost the business millions of dollars. Having an additional safety net in place to ensure compliance is an investment well spent.

Improve decision making

- Prioritize risks holistically across the enterprise to address the risks that will have the most impact on the business.

Enable quick response and effective communication across teams

- With a single platform, built-in CMDB, automated cross-functional workflows, and AI-driven smart issue management, data can be easily shared to identify and prioritize risks based on the impact to the business. Issues can be automatically generated and routed quickly to the correct owner to speed remediation. And team members at all levels have the necessary visibility to more effectively perform their jobs.

1. Gartner Webinars: The Top Enterprise Risk Management Priorities for 2021

Only ServiceNow connects IRM and ITAM teams with workflow to mitigate enterprise risk

There are numerous ways ServiceNow IT asset management works with ServiceNow risk and compliance to save significant time and money.

Industry compliance: Provide evidence for industry audits

ITAM provides point in time data needed when it comes to industry audits. However, you need compliance evidence over the last 3, 6, or 12 months, depending on the regulation. Collecting evidence takes you away from day-to-day activities, but penalties for failing an audit can be steep. IRM can automatically collect the necessary evidence over time, saving you time and providing peace of mind.

Asset end-of-life: Help ensure the proper disposal of hardware assets

Hardware assets have strict disposal processes, especially for data protection and environmental (ESG) issues. If the process is not followed, it can result in millions of dollars in fines. ITAM performs hardware audits to track devices and provide a current status. IRM can identify any device over time that is no longer active or marked as "disposed of", which often indicates the device was not properly retired.

Security operations: Maintain proper security best practices

Patching servers is critical to maintaining a strong security posture. ITAM and ServiceNow Vulnerability Response help identify devices without up-to-date patches, then work with IT operations – modernizing a manual and error prone process. With a single platform and data model, IRM can easily identify servers left unpatched longer than policy dictates and generate an issue for IT operations to address – closing the door to attackers.

Asset refresh: Keep hardware and software under support and in warranty

ITAM helps you track warranty periods and support contracts, so you can keep your business running smoothly – you don't want to be running critical systems on servers that are out of warranty. Example: You currently have two devices with operating systems that will be out of support in four months and one that will be out of support in two months. The current policy mandates you address support issues three months prior to the end of support date. You either need to get the operating system updated now or go into extended support (and pay more). IRM has flagged the compliance violation and created an issue for you and the risk team to resolve, but you know you can't update the operating system for another month. For regulatory audit purposes, you must submit a policy exception to show the risk created by the delay has been analyzed. You'll get another notification when the exception expires, if the violation is still present. The extra oversight acts as another check and provides transparency across the enterprise.

Cloud resources: Keeping costs in check for cloud instances

Cloud Insights, which is another component of IT asset management, can tell you if an instance is still active without any activity. Unused instances can be costly. IRM can provide added protection if an instance meets a policy threshold after a set time or exceeds a dollar value, and automatically generate an issue for the violation. If it is a failover instance, a policy exception can be submitted or IRM can be configured to no longer flag the instance in the future.

> "Without compliance automation, it takes an Internal Audit team 2-3 months to do an asset management audit"
>
> – Now on Now: Hassan Javed from NOW Internal Audit

Conclusion

Having ITAM and IRM on one platform provides significant benefits to the business. IRM uses ITAM data to manage risk and compliance across the enterprise while ITAM uses IRM to provide governance and oversight for asset management and sustainability processes. No other vendor can provide a single platform solution and shared data model, to support cross-functional automated workflows and reduce manual processes. Point solutions only provide a subset of capabilities without significant integration and customization. With ITAM and IRM you get the necessary visibility, governance, and consistent processes to reduce the risk to your business, in addition to increased efficiency and productivity.

Learn more at
www.servicenow.com/risk
www.servicenow.com/itam

servicenow

© 2023 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
SN-itam-irm-solution-brief-08092023