White Paper

Infor Risk and Compliance for Cybersecurity

Cyber-attacks are on the rise

Over the past decade, technology has greatly improved access to governmental services, giving the masses access to vast amounts of information that was previously only accessible by a few. It has also changed how we work and live, with more people accessing information today from Internet sources. This is further compounded by troubling instances of insider threats.

Cybersecurity incidents are inevitable, so agencies must plan for them, according to White House Cyber Czar Michael Daniel, who is far from alone in that opinion. The threat is becoming broader and more diverse, as more devices are connected to the Internet, an emerging phenomenon usually called the "Internet of Things." Yet, as access to information and data continues to increase, it has also increased the complexity of cybersecurity and the ability to prevent unwanted and unwarranted access to government networks. In fact, according to IBM Security Services, there were 1.5 million cyber-attacks in the United States in 2013, with nearly 40% of those attacks motivated by industrial espionage, terrorism, financial crimes, data theft, or dissatisfaction with employers.[1]

To combat cybersecurity threats, the Continuous Diagnostics and Mitigation (CDM) Program was created to provide a dynamic approach to fortifying the cybersecurity of government networks and systems. This program provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis.[2] This represents a significant shift from past policies, and moves toward combating threats on a real-time basis. According to the US General Services Administration, "The CDM Program will help transform the way federal and other government entities manage their cyber networks through strategically sourced tools and services, and enhance the ability of government entities to strengthen the posture of their cyber networks. The [CDM Program] brings an enterprise approach to continuous diagnostics, and allows [for] consistent application of best practices."[3]

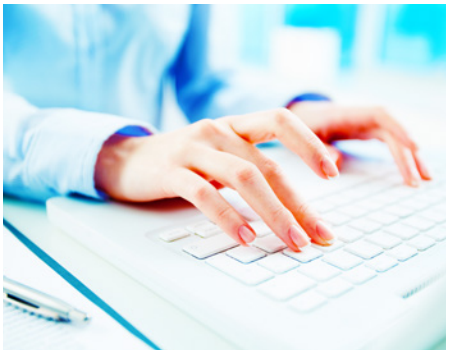


Table of Contents

1 IBM Security Services: Cyber Security Index, http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html
2 US Department of Homeland Security. June 24, 2014. www.dhs.gov/cdm.
3 US General Services Administration. http://www.gsa.gov/portal/content/176671

Continuous Diagnostics and Mitigation Program—A phased approach

The U.S. Department of Homeland Security outlines six key steps, to be implemented in three phases, for agencies to expand their continuous diagnostic capability. These steps include:

1. Agencies install sensors to perform automated searches looking for known security flaws.
2. Searches are conducted to detect network and security flaws.
3. Results are fed into a dashboard from various departments and agencies.
4. Results are analyzed to determine priorities.
5. Resources are efficiently allocated to address and fix threats.
6. Progress is reported and shared among networks to further enhance security.

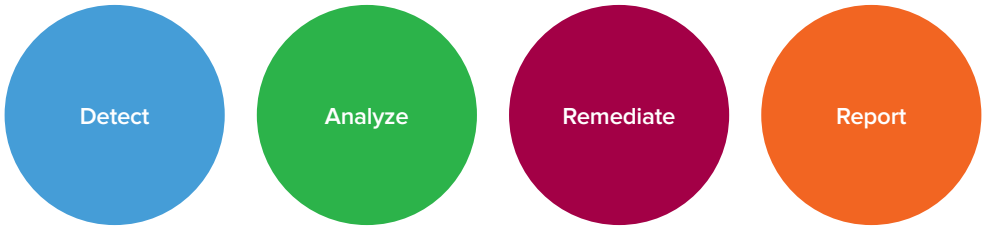
Phase 1, which is already complete according to the Department of Homeland Security, focused on hardware, software, and vulnerability asset management, along with configuration management. Phase 2, which is currently underway, shifts the focus from managing identity and access to more complex issues, such as network and information system integrity. Finally, Phase 3, which is expected to begin approximately mid-way through GFY 2015, will focus on preparing for contingencies, incident response, and managing operations security.

The CDM Program is expected to drive real, enhanced cybersecurity improvements for federal, state, local, regional, and tribal government entities through the prioritization of risks based upon potential impacts, while enabling cybersecurity personnel to mitigate the most significant problems first. To achieve these ends, it is imperative that cybersecurity professionals deploy sophisticated solutions designed to monitor external and internal threats that allow for the mitigation and management of security threats based on risk in real-time.

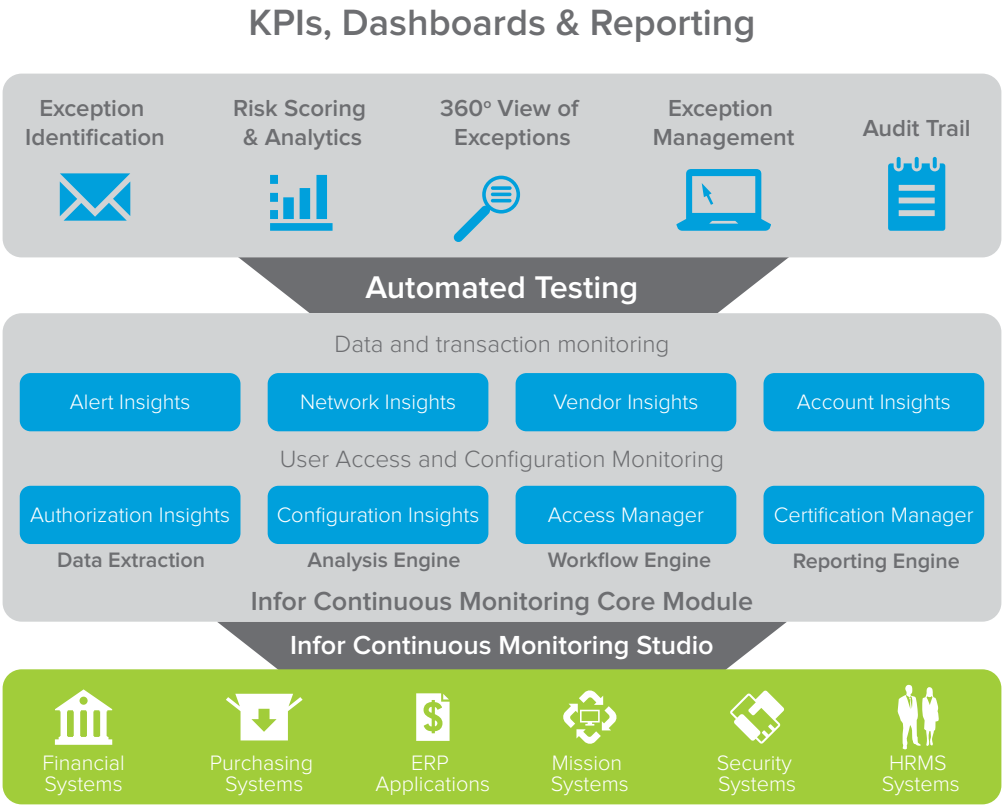
Infor Risk and Compliance for Cybersecurity

As network security continues to increase in complexity, it is important to deploy a solution that serves as a “monitor of monitors.” This system can provide escalation and prioritization of alerts and incidents for mitigation. Infor® Risk and Compliance for Cybersecurity, serves as that solution, automatically finding and reporting cybersecurity issues by identifying exceptions and security breakdowns within and across networks. It enables cybersecurity professionals to flag exceptions, drilldown into emerging threats, collaborate with other stakeholders, and resolve issues as they happen.

By finding and correcting security issues immediately, organizations are better able to reduce risk and take proactive corrective actions—a cornerstone of the CDM Program. Infor Risk and Compliance for Cybersecurity is unique in that it can monitor systems across the organization, including financial systems, purchasing systems, ERP applications, mission-critical systems, security systems, and HRIS systems. This distinctive ability allows for a 360-degree view of the organization—people, data, applications, and infrastructure—a critical feature considering security threats are often present within and outside of government agencies. Ultimately, Infor Risk and Compliance for Cybersecurity enables federal, state, and local government agencies to improve cybersecurity by prioritizing threats and enabling continuous mitigation and monitoring programs.



How Infor Continuous Monitoring for Cybersecurity works



Solution highlights

- Automated monitoring of user access controls
- Detect, remediate, and prevent segregation of duties conflicts and inappropriate access
- Out-of-the-box analytics to track KPIs and automate reporting
- Track user activity within and across systems
- Intuitive all-in-one interface
- Conduct “what if” analyses to prevent new issues from getting introduced
- Built-in collaboration tools
- Risk scoring analytics to quickly understand impact and risk of exceptions
- Automatically identify security exceptions as they occur
- Manage security exceptions, assign them, and follow up via dashboards
- Compliant user provisioning to ensure segregation of duties
- End-to-end process for reviewing and approving user access rights across applications

641 Avenue of the Americas
New York, NY 10011
800-260-2640
infor.com

About Infor

Infor is fundamentally changing the way information is published and consumed in the enterprise, helping 73,000 customers in more than 200 countries and territories improve operations, drive growth, and quickly adapt to changes in business demands. To learn more about Infor, please visit www.infor.com.

Disclaimer

This document reflects the direction Infor may take with regard to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. This document is not a commitment to you in any way and you should not rely on this document or any of its content in making any decision. Infor is not committing to develop or deliver any specified enhancement, upgrade, product or functionality, even if such is described in this document.

INFDTP1450531-EN-US-0615-2