THE NATIONAL CYBERSECURITY SOCIETY

# Continuous Monitoring

## What is Continuous Monitoring?

Continuous monitoring is the process used to detect compliance and risk issues associated with an organization's financial and operational environment. In 2010, the Office of Management and Budget issued a directive to all federal agencies to implement a continuous monitoring program for their IT systems and infrastructure rather than conducting an assessment once a year. This approach has now been adopted as an industry best practice.

The NCSS recommends that when your company is selecting a managed security service provider (MSSP) -- ensure they provide a continuous monitoring program.

## FACT 1: ASSESSMENT PARAMETERS

In the event your company might be interested in establishing your own continuous monitoring program or you would be interested in evaluating a vendor to provide the service, here are the program parameters:

- Establish your company's risk tolerance;
- Develop a method to detect changes in your infrastructure;
- Update and keep current an asset inventory (hardware, software, policies)
- Monitor security controls and assess on a regular basis;
- Establish an assessment frequency (determine daily, weekly, monthly) based upon cost and risk tolerance;
- Establish a program that has the ability to ingest and adapt to changing threat actors/events;
- Verify software is patched on a regular basis;
- Establish a methodology that reports findings of the assessment and the means to take corrective action;
- Sustain a program that has the ability to either - mitigating the technical, management, and operational vulnerabilities identified; accept the risk; or transfer it to another authority;

## Did you know?

- √ Continuous monitoring started from a directive from OMB to federal agencies
- √ Most cloud service providers include continuous monitoring in the suite of offerings
- √ Continuous monitoring will help your company respond and recover more quickly
- √ Continuous monitoring is required for Cloud Service Providers who provide services to the federal government.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.



## JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

# Continuous Monitoring continued....

- Review and update the program, revising the strategy, metrics or risk tolerance as business events change.

## FACT 2: FEDRAMP and CLOUD SERVICE PROVIDERS

FedRAMP is a program that provides a standardized approach to the assessment, authorization, and continuous monitoring of cloud services for the federal government. FedRAMP security baselines are based upon the NIST Cybersecurity Framework, and align to the federal information impact levels of low, moderate and high.

FedRAMP authorization is generally required for all Cloud Service Providers (CSPs) providing cloud services for the U.S. government. If your company is bidding on a government contract, and you plan to store data as part of the service - in all likelihood the contract will require you to store that data in a FedRAMP certified provider. If you would like to become a FedRAMP provider the authorization process is defined at: https://www.fedramp.gov/cloud-service-providers/

If you would like to purchase services, listed below is the current list of approved FedRAMP vendors: https://marketplace.fedramp.gov/#/products?sort=productName

## FACT 3: BENEFITS

Timely identification of problems and quick corrective action can help reduce the cost of any required periodic financial, regulatory, and operational review. Ongoing assessments are more cost effective than a yearly cybersecurity compliance audit and puts your company in a much better position to defend your company in the event of a data breach.

Moreover, continuous monitoring can examine 100% of transactions and data processed in different applications and databases. This methodology can test for inconsistencies, duplication, errors, policy violations, missing approvals, incomplete data, dollar or volume limit errors, or other possible breakdowns in internal controls. Testing can be done for processes like payroll, sales, order processing, purchasing, account receivables, travel and entertainment expenses, purchase cards, and inventory transactions.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

# Continuous Monitoring continued....

Lastly, cybersecurity compliance in the U.S. means private and public organizations that do business with the federal government or receive funds from the federal government must institute the FISMA standards as defined by the NIST Cybersecurity Framework. Agencies and organizations must be able to show specific documentation, policies, procedures and defined processes. Selecting a FedFAMP provider and/or establishing a continuous monitoring program is a must have if you plan to work with federal government.

## FACT 4: CONTINUOUS MONITORING VS CONTINUOUS AUDITING

Continuous monitoring and continuous auditing are not the same, but often used interchangeably. While continuous monitoring enables management to continually review business processes for adherence to and deviations from their intended performance and effectiveness, continuous audits enables the internal audit team to continually gather information from processes to support its auditing functions.

The current environment of GDPR and increasing number of states instituting compliance requirements for data breach notifications, implementing both approaches might be worth considering. For a full understanding of the requirements of both programs, see the Deloitte document under our resource section - "*Continuous Monitoring and Continuous Auditing, from Idea to Implementation",* Deloitte LLC.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.