IBM and Cybersecurity Maturity Model Certification

The Department of Defense released the Cybersecurity Maturity Model Certification (CMMC) to proactively protect both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC was designed to provide assurance to DoD that its contractors can protect CUI. At IBM Security we believe cybersecurity should not be bolted on after the fact, it needs to be integrated into all aspects of your business in order to solve today's challenges and remain ahead of those that will come tomorrow. It's time to drive security into the fabric of your organization with IBM's commitment to educating customers on changing challenges and requirements. IBM Security is not certifying a CMMC solution; instead the intention, right now, is to provide a resource for DoD contractors to navigate newly combined standards relevant to the cybersecurity certification board. The CMMC encompasses 1-5 levels ranging from 'Basic Cybersecurity Hygiene' to 'Advanced' and combines control standards into one unified cybersecurity standard and some additional best practices.

To access whether contractors have met a CMMC level, the DoD will deploy certified third-party assessor organizations (C3PAO's) to conduct audits. The initial round of audits will be conducted between June-September 2020 and certification will be necessary from a C3PAO by October 2020 and beyond.

IBM Security recognizes Federal System Integrators, agencies, and businesses of all sizes struggle with the implementation and usability of fragmented, disconnected security tools and the specialized skills and costs required to integrate and operate them. As a result, many organizations lack a complete view of their data security and compliance landscape, which can diminish their ability to effectively assess, prioritize and respond to threats and issues.

Our core solution to address protecting CUI combines strength, security and compliance. Guardium's suite offers capabilities for protecting and controlling access to databases, files and containers. It can help protect assets residing in cloud, virtual, big data and physical environments. This set of scalable data security solutions helps enable you to address pressing requirements and helps prepare your organization to respond when the next security challenge or compliance requirement arises.

Guardium's comprehensive capabilities are helpful in implementing a range of security and privacy requirements, including some of those outlined in the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and regional data protection and privacy laws. Guardium equips organizations with powerful tools to help combat external threats, guard against insider abuse and establish persistent controls, even when data is stored in the cloud or an external provider's infrastructure.

IBM Security Guardium is comprised of several different integrated products, which provide specific capabilities based on user needs, that are accessed via a common management server known as the Data Security Manager (DSM).

Key features:

- Multi-tenancy support
- Proven scale to 10,000 + agents
- Toolkit and programmatic interface
- Easy integration with existing authentication infrastructure
- RESTful API support
- Container Encryption / Cloud Vendor Storage

Additionally, business may be under increased pressure to move their data and infrastructure to the cloud in order to achieve greater business agility, responsiveness, and to save costs. They may also face external and internal pressures to support data privacy and compliance requirements – which might become more complicated in the cloud. These types of organizations might be struggling to understand how to leverage their existing on-prem data security investments, while forging into the hybrid multi-cloud world.

IBM Security is a security vendor that is also part of a cloud company. Only IBM Security has the industry's broadest and most complete security portfolio to help transform your security program.

- Our Strategy and Risk solutions are not only delivered by our consultants out in the field, but also through our Security Command Centers so that you can build a proactive and pervasive security culture that is prepared to respond to potential threats.

- IBM's Threat Management solutions combine top orchestration capabilities from our Security Operation Centers, Security Analytics Platforms, and Response and Threat Hunting solutions — all enabling you to find and eliminate threats.

- And our expansive Digital Trust solutions deliver data protection, identity and fraud management, cloud and endpoint management solutions needed so security professionals can keep up with digital transformation.

The guide below maps back CMMC controls to potential software tools to satisfy the requirement. If you have any questions reach out to your IBM Federal Security Account Representative. If you are unsure who that is send a note to justin.taylor.miller@ibm.com and an introduction will be facilitated.

IBM Security
Federal Market

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security Guardium