Once an organization starts its cloud journey and gets the basics in place from a security standpoint, the next questions are typically, “What does the cloud security journey look like?” and, “How can I organize my cloud security program?” Most organizations today are already in the cloud, but the transition is often reactive to support business needs, and security doesn’t always have the time to design and map out a complete program. The Cloud Security Maturity Model (CSMM) was built to help organizations understand what their cloud security journey looks like and, more importantly, be able to consciously determine how mature they want to be in each category.

The first version of the CSMM focused on defining the domains and categories of a cloud security program and the maturity levels. Based on feedback and hands-on projects with clients, we realized the CSMM was far more useful and started serving as a high-level cloud security framework that helped organizations structure and manage their programs. Version 2.0 of the CSMM recognizes this wider usage and has been updated and expanded with extensive new content to meet these needs, including a comprehensive set of cloud security control objectives that function as key performance indicators (KPIs) to assess and guide your program.

The CSMM 2.0 includes four major components:

- Twelve categories in three domains that cover the major areas of cloud security activities that should be in any program. These align with the structure of the upcoming Cloud Security Alliance (CSA) Security Guidance version 5.0.
- Five maturity levels, based directly on the standard Capabilities Maturity Model (CMM) levels.
- Cloud security control objectives for each category and maturity level. The control objectives serve as sample KPIs and were carefully designed to reflect expected maturity and support automated assessment, to the greatest degree possible. These are actively being aligned with the CSA Critical Controls Matrix (CCM) in future revisions.
- Sample cloud security control specifications for the three largest cloud providers. These are complete for AWS in the current version but are still under development for Microsoft Azure and Google Cloud Platform. IANS and Securosis, who co-developed the CSMM in partnership with the CSA, encourage readers and users of the CSMM to submit their suggestions for additional controls.

In addition, IANS offers a free, online diagnostic survey tool to assess your CSMM status and readiness. IANS has also partnered with FireMon on the release of a technical assessment platform that integrates with your cloud deployments for real-time CSMM assessments.

CSMM 2.0 Structure

The Domains

The Cloud Security Maturity Model is broken up into 12 categories across three domains. Domains represent the logical grouping of security capabilities. There are also two “meta-domains” that span the model. Here is a brief description of each domain:

- **Foundational domain:** Core, critical domains to ensure availability of a secure baseline. This is where you want to start when building your program and these capabilities will span your deployments.
- **Structural domain:** Domains to protect the building blocks of your cloud environment. While there will be some shared capabilities here, you will find that these will vary more to meet the needs of different deployments and environments. These capabilities will require more collaboration with deployment/application teams to meet their individual needs.
- **Procedural domain:** Domains to highlight the processes needed to protect your cloud (and keep it protected) over time. These process-oriented capabilities are required for long-term sustainment and stability and are usually implemented after covering the basics of the foundational and structural domains.

The two meta-domains are key overlays that span most, if not all, of the categories. These are not measured in this version of the model but are included to align with other frameworks and to emphasize that you will see activities in these areas throughout the model:

- **Threat management:** This includes the spectrum of threat intelligence, assessment and remediation.
- **DevSecOps:** Alignment with DevOps and implementation of automation in security operations.

The Categories

Categories are areas of security capabilities. This list isn't meant to cover all possible aspects of security, which are better managed using NIST Cybersecurity Framework (CSF) and other comprehensive frameworks. The CSMM categories were selected to focus efforts on cloud-related activities and skip over areas like HR, endpoint and BYOD that are already covered with other models.

The Foundational Domain Categories

This is where you start. Creating the foundation for a strong cloud security program. These are the things that (hopefully) you do before implementing cloud. Of course, it's not always like that, so, at times, you need to retrofit existing processes and, optimally, these categories are addressed across the entire organization.

- **Governance:** Overall governance of cloud providers, deployments, applications and general usage.
- **Organization Management:** Core cloud deployment security and multi-deployment/-provider architectures to control blast radius and ensure baseline security.
- **IAM:** Managing users, authentication and authorization through the cloud provider and resources within the cloud. Also refers to managing IAM within the provider.
- **Security Monitoring:** Monitoring and logging of both cloud administrative activity (the management plane) and assets within the cloud (networks, workloads, applications, data).

The Structural Domain Categories

The Structural Domain represents what would be considered traditional security—looking at the infrastructure, data and applications and ensuring the security of the resources at every level of the computing stack. Of course, the base concepts of securing resources in the cloud are vaguely familiar to experienced security professionals, but how the underlying technology works and how those resources are secured can be very different. This domain is about understanding those differences and using both automation and orchestration to enable all of the requisite controls to work in an agile, adaptive manner—keeping pace with the speed of cloud and DevOps.

- **Network Security:** Security of the virtual networks in the cloud, as well as the connections to/from the cloud.
- **Workload Security:** Securing the environment where code runs, including virtual machines/instances, containers and function as a service (FaaS or serverless).
- **Application Security:** Full-stack application security, which includes testing and protection of pipelines, workloads, architectures, etc.
- **Data Security:** Encryption and access control of cloud data.

The Procedural Domain Categories

The Procedural Domain represents critical processes needed to secure your cloud and keep it secure. Where the Foundational categories should be the focus at the start, the Procedural categories cover the capabilities required for a sustainable security program.

- **Risk Assessment and Provider Management:** There are three aspects of risk assessment:

1. provider selection (choosing providers);
2. ongoing provider reassessment and management; and
3. risk assessment of specific projects and programs.

- **Resilience:** Ensuring resilient use of cloud that meets an organization's business requirements for availability and recovery.
- **Compliance and Audit:** Meeting regulatory compliance requirements and mandates.
- **Incident Response:** Cloud-specific incident response processes, including compromise of the cloud console/management plane.

Cloud Security Control Objectives

The CSMM 2.0 includes separate tabs for each category. On each tab are between one and three representative control objectives for each maturity level, starting at Level 2. These control objectives are KPIs that are representative, not exhaustive. They are based on industry and subject matter expert consensus and were open to public review through the CSA before being finalized.

If you meet the requirements of the control objective, it means you are likely to be at or around that maturity level, not *definitively* at that maturity level. The individual control objectives should not become your sole operational targets and a more-comprehensive approach like the CSA CCM is more appropriate for that case. Each control objective includes the following:

- **Control ID** for reference, assessments and alignments with other frameworks.
- **Maturity Level** of that control objective.
- **Control Objective Name**
- **Control Objective Description** with the expected outcome or state when the control objective is implemented.
- **Automated or Manual** for the assessment state of the objective. "AUTOMATED" means the control objective can and should be automatically assessed. "MANUAL" means it is unlikely the control objective can be accurately assessed using automation. "EITHER" means the control objective can probably be automatically assessed, but you may be implementing it using a technique that requires a manual assessment. These are typically controls implemented using third-party tools that don't integrate with your cloud assessment tooling (e.g., an external endpoint protection agent).
- **CSP Control Specification Examples:** These describe the implementation of a control objective. There are columns for the three largest cloud providers and (generic) cloud security posture management (CSPM) tools. CSPM tools are included because they are one of the most common ways of assessing cloud security controls. *[**Note:** At this time, control specifications are only complete for AWS; IANS, Securosis and the CSA will continue to build these out and revise the CSMM, and external contributions are encouraged.]*

An important note on using the control specification examples

Any given control objective may map to multiple control specifications for implementation. Control specifications are the technical mechanism for meeting a control objective. For example, if your requirement is that all users must log in with MFA, you might have specifications for MFA on your SSO portal, a policy blocking API calls without MFA, monitoring to identify logins without MFA and more.

Controls specifications in the CSMM 2.0 are examples to show just one of multiple methods of meeting a control objective. The ones included in the model are selected for maximum ability to automate the assessment, but many organizations will have other means of meeting those requirements.

Using the Model

The CSMM 2.0 was architected to assist organizations with designing, building and maintaining their cloud security program. It incorporates many lessons learned in using the first version of the model with multiple organizations.

- **CSMM as a security framework:** CSMM 2.0 includes domains and categories that are compatible with, and meant to work in parallel with, existing high-level security frameworks like NIST CSF. The CSMM is the cloud lens for organizing your security activities. It can and should help focus the cloud capabilities of your security program. Using the CSMM as a structural framework allows you to focus on the areas that matter most for cloud and, likely, need a cloud-native approach.

- **CSMM as a maturity model:** The maturity levels of the CSMM describe the cloud security journey for organizations just getting started to the most mature and fully automated "cloud unicorns." As we've stated before, the levels represent what we commonly see and are meant as qualitative, not quantitative, guidance. It's also important to understand that, in most organizations, different business units and initiatives will be at different maturity levels. It's far easier for your born-in-the-cloud application team to operate with high maturity compared to the lift and shift of a 30-year-old legacy application.

  You should *not* attempt to achieve Level 5 across the board. This is likely too expensive and inappropriate for all your initiatives. It is absolutely acceptable to target a Level 3–4, or even Level 2 if your program is just getting started.

- **CSMM for KPI-based assessments:** The cloud security control objectives can serve as KPIs to measure the maturity of your program and individual deployments. You can and should modify these KPIs to align with your way of doing things, as long as you can reasonably defend that your alternative is of the same maturity level. The control specification examples are included to show you how to automatically assess a given KPI on a given cloud provider.

Recommended Process

1. Review the CSMM 2.0.

2. Take the IANS diagnostic survey at https://www.iansresearch.com/cloud-maturity-diagnostic. This survey will generate a report based on your answers to provide a quick qualitative assessment of your current maturity level.

3. Review the results and determine your goals. Goals should be "S.M.A.R.T." (Specific, Measurable, Achievable, Realistic and Time-based). An example would be to achieve CSMM Level 4 for monitoring in 12 months and Level 3 for network security in nine months, as measured using the CSMM control objectives.

4. Assess your cloud deployments. You can do this by hand or using the free service from FireMon at https://defense.firemon.cloud/csmm/.

5. Build the plan. Start by prioritizing your deployments (e.g., production vs. development), and then work with the appropriate teams to identify a roadmap for implementing required controls. Remember, the CSMM 2.0 includes only the general descriptions and KPIs; you will need to use tools like the CSA CSM and security guidance for full implementation.

A key point: The model is a set of guidelines—not all of which will work for every organization. So, organizations should use the model as a starting point and a means to make decisions about how much investment makes sense for their environment. The difference between Level 3 and Level 5 can be significant (depending on the category), and it may not reduce enough risk to warrant the time and investment.

To be clear, there is no right or wrong level of cloud security maturity. Over time, organizations should be improving their cloud security and ensuring critical data moved to the cloud is protected. But not every organization needs to be Level 5 across the board. As long as the cloud security team makes educated choices about how mature the organization should be, then the model is serving its purpose.