ermetic | Whitepaper

Cloud Security Maturity Model:

Vision, Path, Execution

Executive Summary

Securing a cloud environment is an incredibly difficult task to perform and doing so is becoming more and more vital as much of modern infrastructure is either natively deployed on cloud platforms or is migrating to cloud infrastructure. As cloud environments are dynamic, very complex and scale quickly, security officers may find it difficult to set up a viable strategy to move their organization forward in the context of cloud security. There are so many different variables to consider when designing and implementing such a strategy and so many people and moving parts to coordinate. The massive industry shift to the cloud also makes it difficult to locate experienced talent makes things even more difficult.

Best practices and compliance standards are a good first step and can provide a nice abstraction of the domains to focus on. Some offer best practices for securing the cloud environment.

However, some compliance standards are written abstractly, which requires content poured in (which really leaves you with doing most of the work), and some best practices are extremely specific, leaving many bases uncovered. We reviewed this situation in our recent compliance webinar.

So, while these standards are a good resource to use along the way - to lead an organization through the stormy waters of securing cloud infrastructure, you need a viable map to guide the way. For this reason, we've created a lightweight framework to help you easily assess the current level of your organization's maturity in each of the crucial domains of cloud security. The framework enables you to set clear, practical and achievable goals to advance to the next level.

We call it the Ermetic Cloud Security Maturity Model.

About the framework

We developed the Ermetic Cloud Security Maturity Model based on our engagement with hundreds of organizations and our expertise providing service in the cloud security space.

It defines the key guidelines for a comprehensive cloud security strategy, which you should apply in stages. This is due to the fact that one of the biggest challenges when securing a cloud environment is maturing the entire organization and its infrastructure - and this CAN'T be done in a single bound.

Maturity Model: Organization

	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
PEOPLE				
Roles and responsibilities	No dedicated personnel for cloud infrastructure security	Some knowledge and responsibility within the security team Executive sponsor for cloud security program, early form of CCOE	Dedicated person / team with relevant training and expertise Established CCOE	Additional expert delegates within R&D team
Training	No dedicated training / expertise in cloud security	Some members of security team undergo cloud security training	Cloud security team undergoes formal cloud security training and certification	Cloud security awareness training program for R&D
PROCESSES				
Remediation process	Best effort with no structured process	Security team owns and prioritizes security findings	Prioritized findings automatically shared with stakeholders	Full ownership of R&D teams for resolution of issues
Integration to CI/CD pipeline	Infrastructure is not managed as part of CI/CD pipeline	Proper process for governing change management	Managing Infrastructure as Code	Embedding infrastructure security in the CI/CD pipeline
Compliance	Meeting no defined standard	Mandatory compliance standards are met	External best practice(s) implemented and audited Governance principles documented and tracked Screen reader support enabled	Custom compliance rules enforced
Access governance	Rudimentary access review is done based on best effort, if it all	Groups / labels / organizational-structure based level access review Consistent access and governance Screen reader support enabled	Risk-based access review for sensitive resources and privileged identities	Risk-based access review for all resources and identities
Incident response	No defined playbook for incidents Immature incident response plan for cloud	Well defined manual playbook for responding to incidents	Organization wide incident response program in place and tested periodically	Automation of playbook based on previous experience

Maturity Model: Technology

	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
VISIBILITY				
Inventory management	Manually or with cloud console	Using a script or in-house solution	Automatically, centralizing from all cloud platforms	Inventory is filterable and searchable
Contextualization	Basic information only	Mapping relationships between resources	Classifying inventory manually	Automatic classification of inventory
PREVENTION				
Identities	Best effort identity governance	Implementing basic best practices	Retire the use of static credentials	Governing unused identities and credentials
Entitlements	Best effort governance of human / service entitlements	Visibility into what identity can access what resource	Classifying privileged Identities	High resolution least privilege
Data	Data security best practices	Public data exposure governance	Governing segregation to critical environments	Governing sensitive data segregation on the resource level
Computing	No governance and visibility of compute security posture	Conducting Host (OS / Containers) patch management	Implementing Host (OS / Containers) configuration best practices	Vulnerability management for software packages
Network access	Ungoverned network access	Public access is governed and remediated	Network access to sensitive resources is restricted	Microsegmentation of network resources
DETECTION				
Log collection	Distributed /cloud vendor default	Centralized logs	Indexed and queryable logs	Normalized and enriched information
Log analysis	None / Manual review of logs	Detection of specific suspicious events	Detection of IoCs from native monitoring tools	Comprehensive detection of anomalous behaviour

The model separates organizations into four different maturity levels:

- **Level 1 - Ad Hoc -** At this level, cloud security is basically done as an afterthought, only really addressing it when there are fires to put out (usually the worst time) and not done in any structured way.

- **Level 2 - Opportunistic -** This is when the enterprise actually starts addressing cloud security in a structured way, with some kind of strategy which is also incorporated into the roadmap.

- **Level 3 - Repeatable -** To reach this level, the enterprise should be able to easily execute its cloud security strategy when needed (e.g. when there's a new set of requirements from the resources in the environment due to business constraints, or new resources that have to be provisioned), a major addition of resources (e.g. due to an M&A) or any other significant change.

- **Level 4 - Automated and Integrated -** This is the highest level of maturity for an enterprise. At this level, the most significant components of the cloud security strategy are applied automatically within the infrastructure.

The framework isn't simply a long and exhaustive checklist of attributes to accomplish; it defines key abilities to keep in mind when advancing from one level to the next. Through our experience with hundreds of enterprises, we were able to zero in on the abilities and attributes that really set organizations apart from one another. We call these abilities or attributes "Indicators of Matriculation."

To achieve these goals effectively, you may run into challenges and tasks to complete; however, since the indicators of matriculation are simple to articulate, it will be easier for you to set an achievable goal for the organization. With a goal, stakeholders will get on board, and together, you can motivate the entire organization to strive toward the next level, or improve the current one.

The framework is NOT an archive of knowledge and it's completely cloud/service provider neutral. It's not meant to provide technical instructions on how to do things, specific advice on what services to turn on / off or an outline of what specific configurations to use. It does, however, provide clear goals to help you locate relevant materials and tools to implement.

The practice of advancing an organization in a synchronized manner through the various parameters has important benefits:

- Some parameters are codependent, meaning that they benefit from and rely on each other - so trying to advance in one without doing proper work on another might be difficult,less effective and maybe even impossible.

- Organizations are made up of people, and when it comes to security, they

usually need time to mature their practices, habits and standards. For this reason, building a security program under these milestones and syncing it across various parameters allows you to softly integrate it into the corporate culture.

- The plan helps you define reachable and practical goals between levels, and get clarity for the security team and other stakeholders in the organization, thus making it easier to get them on board.

- Moving toward the goal of becoming cloud mature in an holistic manner allows you to present a step-by-step process of advancement to the organization's leadership.

What this is not

The Cloud Security Maturity Model serves many purposes, but there are several things it is not.

The silver bullet - Practitioners tend to expect frameworks like these to be a guaranteed solution to solve all cybersecurity problems. Unfortunately, a silver bullet does not exist in the form of a framework or even as a set of technologies. Nothing will ever fully replace common sense and vigilance - specifically in such a dynamic domain as cloud infrastructure cybersecurity. Even if your organization optimally meets every requirement in this framework, it will not prevent your organization from being vulnerable.

A step-by-step guide - As mentioned, this framework won't provide any specific instructions. There are no tutorials, as this is not meant to serve as an extensive body of knowledge or a technological archive. This is due to the fact that compiling such an archive is 1. borderline impossible, and 2. unnecessary, as the answers to many of the questions and challenges raised by this framework will always be easily available in vendor documentation, online forums, expert corporate websites, etc. This framework helps you and other decision makers understand what questions to ask, at what point and of whom.

Vendor and security technology recommendation(s) - We do not discuss any specific technologies or vendors. Again, this framework will help your team prepare questions to ask - the answers are usually abundant, and assessing tools and finding implementation guides is usually not the most pressing challenge. So even if it may seem implied - this framework does not provide recommendations or refer to specific technologies or vendors.

How to use the framework

Implementing this framework is quite simple and is made up of the following stages:

- **Qualify** - First, assess where your organization currently stands. This may sound simple to do, but the assessment process must be done rigorously because its success depends greatly on how thoroughly each stage is applied. It's ok to provide immediate high level answers to questions qualifying your organization to a certain level of the framework; however, as with everything of this form, the principle of "garbage in garbage out" applies. The better informed the team is about the topic being assessed, the more certainty there will be when qualifying at the current level and the more confidence there will be moving to the next level.

- **Set milestones** - The second stage is to determine how to move your organization forward. The main benefit of this framework is being able to pinpoint the main criteria that will advance the organization forward. This can be done either by fortifying the status at the current level by asking more rigorous questions and demanding more at the current indicators of matriculation - or those at the next level. It's possible, of course, to advance to different levels at different domains based on specific needs and abilities; however, we recommend to initially advance in sync between the various domains as possible.

- **Execute** - Set milestones for a predetermined amount of time, and get all relevant stakeholders on board to incorporate them into their roadmap and execute to the best of their ability. Encourage measurable goals aligned with the indicators of matriculation, which may require you to implement prerequisites. This is not only expected, but is part of the organizational maturity process. This is actually one of the main benefits of the model: set a very clear and significant security goal (i.e. the indicator of matriculation), and by getting stakeholders on board to accomplish it, other tasks that mature the organization along the way may be performed.

- **Repeat** - After executing the roadmap, repeat the process by first qualifying the results of the execution stage. Determine the frequency of performing this process based on your organization's needs and abilities, and preferably also aligning with other roadmap planning and assessment processes. We recommend, however, that you perform it at least once each quarter. Regardless, if this strategy isn't employed on a regular basis, one of its most important benefits will be missed: not only maturing the organization, but keeping it mature and always moving forward. Remember - a maturity level is not a certification, it's a commitment!

As with almost everything - it's imperative to apply common sense and practical thought as your organization's specific needs may change. Even once cloud maturity is achieved, remember that maintaining it is a constant process and the work is never done.

Maturity Model categories

The parameters are separated into two main categories:

- **Organization:** personnel and procedures that are required to maintain a more secure environment
- **Technology:** technical controls and configurations

In the following sections, we will outline the different parameters and requirements for matriculation between levels.

Part 1: Organization

People

This category addresses the following questions:

- Who is responsible for securing the cloud environment?
- What is their level of expertise?
- Do the people responsible for implementation have enough resources to complete the work?

The parameters in this category align well with one another, as responsibility and training usually go hand and hand.

Roles and responsibilities

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
No dedicated personnel for cloud infrastructure security	Some knowledge and responsibility within the security team Executive sponsor for cloud security program, early form of CCOE	Dedicated person / team with relevant training and expertise Established CCOE	Additional expert delegates within R&D team

Training

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
No dedicated training / expertise in cloud security	Some members of security team undergo cloud security training	Cloud security team undergoes formal cloud security training and certification	Cloud security awareness training program for R&D

At the **Ad Hoc** level, the entire practice of cloud infrastructure security is done as an afterthought of the general security program, and there is no bandwidth or training allocated to it as a practice.

At the **Opportunistic** level, the practice of cloud infrastructure security starts getting proper attention. The organization acknowledges that it is, in fact, a separate practice from on-prem security and assigns the responsibility and the task of skill acquisition to specific people. In addition, at this stage there's usually executive sponsorship of a cloud security program and an early form of a Cloud Center of Excellence (CCOE).

At the **Repeatable** stage, there is a person or team focused on cloud infrastructure security, and they acquire formal cloud security training and certification. At this point there's also an established CCOE.

The indicator of matriculation to the **Automated and Integrated** level is the effective delegation of responsibility to personnel on the R&D team, who will both acknowledge their responsibility and cooperate with the process of being trained to perform tasks around securing the cloud infrastructure.

Processes

The following parameters revolve around the definition and performance of certain processes and procedures within the organization.

Remediation process

The process of remediating findings of security gaps / misconfigurations in the cloud environment leads one to ask who owns the process of responding to findings arising from governance, and how is it done?

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Best effort with no structured process	Security team owns and prioritizes security findings	Prioritized findings automatically shared with stakeholders	Full ownership of R&D teams for resolution of issues

At the **Ad Hoc** stage, there is no structured process to locate, acknowledge and respond to such findings in the cloud infrastructure.

At the **Opportunistic** stage, when such a process is put in place, it's usually the security team that simply prioritizes the findings and handles them. At this stage, normally automated detection of such findings occurs (see the Prevention category in the Technology section), followed by manual review of the issues and assignment to relevant stakeholders within the organization.

At the **Repeatable** stage, differentiation is usually an automated process of assigning the findings to the relevant stakeholders based on predefined definitions, with overview from the security team and adjustments as necessary.

At the **Automated and Integrated** stage, R&D teams are not only automatically notified with relevant findings, but they are also responsible for remediating issues with the security team experts.

Integration to CI/CD pipeline

This parameter examines the level of integration of cloud infrastructure security into the CI/CD pipeline. The first condition for such integration is, of course, having the infrastructure itself as part of the CI/CD pipeline.

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Infrastructure is not managed as part of CI/CD pipeline	Proper process for governing change management	Managing Infrastructure as Code	Embedding infrastructure security in the CI/CD pipeline

At the **Ad Hoc** stage, organizations simply don't have infrastructure as part of the CI/CD pipeline, and don't have it defined as code (i.e. leveraging Infrastructure as Code or IaC).

At the **Opportunistic** stage, organizations incorporate a procedure for change management of the infrastructure. This means there are clear standards of what kind of changes should be made, how resources are provisioned and who in the organization approves them based on which criteria.

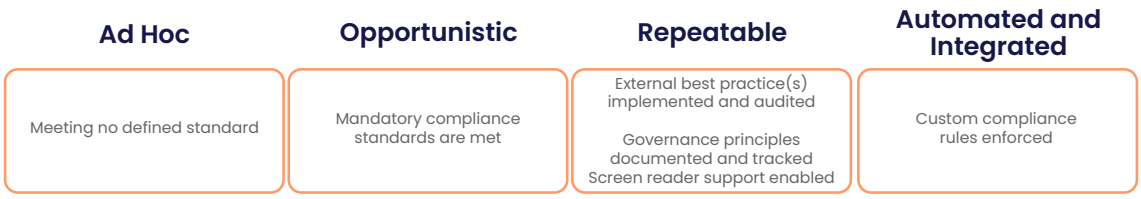
At the **Repeatable** stage, organizations take a giant leap forward by properly maintaining their infrastructure as code. This is a major indicator that the organization's infrastructure management approach has grown and that it has become much more mature. Among its other benefits, managing infrastructure this way is an incredible platform for carrying out any kind of security strategy. For example, change management can be done by reviewing and approving a pull request to the repository where the infrastructure-as-code is maintained.

At the **Automated and Integrated** stage, not only is infrastructure managed by code and controlled properly, but security controls and policies are monitored and enforced as part of the CI/CD pipeline at the build stage or earlier - before being deployed. By doing so, the organization's security "shifts left" and issues are automatically detected and enforced before the infrastructure is staged. This may include security posture issues and rules of access management, network compartmentalization configurations, and more.

Compliance

The best practices and compliance standards an organization adheres to offers a certain indication of its maturity level, since doing so means the organization effectively and periodically audits itself (or submits to external auditing), and complies with certain requirements.

The main question is - which standards and/or best practices?



At the **Ad Hoc** stage, the organization typically does not meet any defined standard.

At the **Opportunistic** stage, the organization meets the compliance standards required by law or by its basic business requirements.

At the **Repeatable stage**, the organization meets at least one commonly known

best practice in addition to its required compliance standards. In addition, senior officials of the organization carefully document and track the compliance and auditing practices for the inherent security value, not just to "check the boxes."

At the **Automated and Integrated** stage, the organization can define custom compliance requirements designed to effectively meet specific security needs. This is usually very difficult to do because defining custom-made enforceable cloud security requirements means very deep and intimate knowledge of the technology and the specific infrastructure, as well as the business requirements and threats to protect against. This also requires constant governance of custom requirements and the ability to adjust them as necessary.

Access governance

An important part of maturing an organization is determining what type of governance processes are implemented to ensure that only business-relevant access is granted to identities.

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Rudimentary access review is done based on best effort, if it all	Groups / labels / organizational-structure based level access review Consistent access and governance Screen reader support enabled	Risk-based access review for sensitive resources and privileged identities	Risk-based access review for all resources and identities

At the **Ad Hoc** stage, access review is best effort - if done at all.

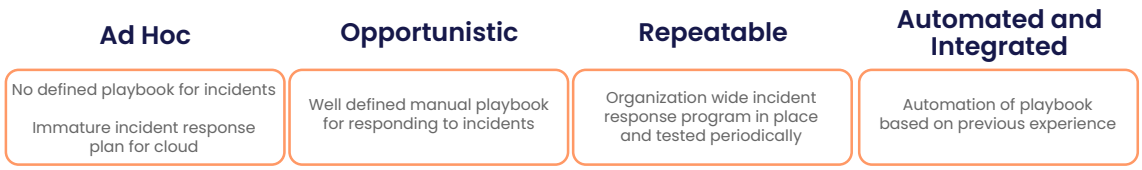
At the **Opportunistic** stage, a periodic review reveals which identities have access to which resources, but the review is done simply based on attribution by measures such as labels and group memberships. This means that the review only ensures each identity is affiliated correctly, but doesn't ensure that only proper permissions are granted because the permissions granted due to the affiliation aren't inspected. It should be noted that at this level, the organization takes a big step forward by adopting the practice of routinely reviewing access.

At the **Repeatable** stage, there is risk-based access review, where the actual permissions granted to identities are assessed based on the permissions they are supposed to have. This is only done for sensitive resources and identities like admins, mission critical resources and sensitive data. This highly correlates with the entitlements parameter of the prevention domain in the technology section.

At the **Automated and Integrated** stage, a risk-based review is done for all identities and resources.

Incident response

The preparation level and response procedures of an organization to security incidents in the cloud is paramount to its maturity.



At the **Ad Hoc** stage, there's usually no defined playbook for incidents. There may be some sort of response for the incidents detected, but any response will be ad-hoc and not very well defined.

To matriculate to the **Opportunistic** level, the first indicator is to go define an incident response playbook based on prior experience of ad-hoc response to incidents or theoretically preparing for them. This process will bring a lot to the awareness of various stakeholders in the organization, not to mention, it will prepare them for the day when an incident actually occurs.

At the **Repeatable** stage, the playbook becomes an organization-wide program that is not only acknowledged officially within the organization, but also periodically tested and modeled to ensure that the technology is in place and that the various stakeholders are trained and aware of their roles.

An organization reaches the **Automated and Integrated** stage of maturity when these playbooks are automated based on prior experience and/or the detailed and tested definitions. This doesn't mean that all incidents are automatically responded to, but the organization learns to convert a well-thought out and tested playbook to an automated process that is triggered by an incident.

Part 2: Technology

Resource visibility

The basic assumption is that you can't secure or protect your organization from what you can't see. There are two parameters for defining this ability:

- How to manage and store inventory results in what kind of usability it has
- What type of contextualization information to add to enrich inventory data and make it more useful as the foundation for the security strategy

Management

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Manually or with cloud console	Using a script or in-house solution	Automatically, centralizing from all cloud platforms	Inventory is filterable and searchable

Contextualization

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Basic information only	Mapping relationships between resources	Classifying inventory manually	Automatic classification of inventory

At the **Ad Hoc** stage, the organization consumes inventory using basic consoles provided by cloud vendors. This may include some manual exporting and gathering of data regarding the inventory. Only the information provided is used. For each resource, very basic information (e.g. id, name, type) can be accessed through the vendor console or an API query. While very basic, this information still provides a good foundation to get familiar with the console and everything the cloud vendor provides for each resource.

At the **Opportunistic** level, the organization collects information using an automated script. At this stage, the organization leverages vendor APIs via a homebrew script or an open source solution to curate inventory to be used later. The adoption process of such technology compels the organization to get better acquainted with the data collected for each of the different resources.

When it comes to contextualization, the next step is to add information regarding relationships between different resources. A map like this would include relationships such as network components (e.g. subnets, ip addresses, networks, load balancers), their configurations and the resources using them (e.g. computing resources, data storage), data volumes and the computing resources they are attached to, encryption assets and the data resources protected by them, logical collections of computing resources (i.e. used for scaling) and the resources on them, and more. The process of creating, maintaining and working with such a map is important for the growth of the organization and support of the stakeholders, but the data itself can be useful when managing incidents or understanding which of the resources in the environment are significant.

At the **Repeatable** level, inventory is automatically updated and centrally managed across cloud deployments, vendors, regions, accounts, etc.

Context-wise, inventory is manually labeled based on business logic. Usually only resources that are mission critical and/or hold sensitive information are labeled.

At the **Automated and Integrated** stage, the organization stores and indexes inventory in a way that makes it easy to query specific resources. Various professionals across the organization should be well-versed in making such queries and should be able to do so when needed.

Resources are automatically classified based on predetermined logic. This applies to all relevant resources, not only mission critical resources or those holding sensitive data, but also segmenting projects allowing for better data compartmentalization, understanding blast radius, managing access, prioritization of security findings, remediation, etc.

Prevention

Breach prevention is split into 5 different parameters: identities, entitlements, data, computing and network access. An organization's maturity is measured by examining the configurations and controls meant to prevent breaches from occurring due to poor security posture.

Identities

What controls are in place to prevent identities from being compromised?

At the **Ad Hoc** level, the organization does the minimum to manage creation and governance of identities in the environment. This includes acknowledging third party and guest identities, and granting authority to specific people to create and configure new identities. At this level, an organization also aligns identities with organization and business logic.

At the **Opportunistic** level, the organization employs standard best practices for securing identities. This ranges from straightforward configurations like setting password policies (e.g. complexity, preventing reuse), enforcing MFA for all power users, rotating static credentials, and allowing third party access In addition, the organization may enforce more complicated and organization-wide best practices like centralized management of users and employing instance profiles for service identities.

At the **Repeatable** level, the organization retires static credentials, which may sound like a trivial feat; however, it's not that easy to accomplish. To retire static credentials, it's necessary to first find all the ones currently in use, then provide effective replacements, get developers and DevOps engineers to cooperate with replacing them, and actually lead the process. In addition, the organization must ensure that such credentials are not generated and used, except in some very specific exceptions (e.g. break glass users).

At the **Automated and Integrated** stage, identity governance enables the organization to effectively disable unused identities and credentials. Most organizations don't typically have controls enabling them to confidently remove an identity even though it has been inactive for a very long time. To reach that point, the person in charge of securing the identities (refer to the remediation parameter under processes in the organization segment) would have to be extremely close to the development team - perhaps even a developer him- or herself. This is difficult to accomplish, but very easy to define as a goal.

Entitlements

What kind of visibility and enforcement are required for the principle of least privilege?

At the **Ad Hoc** level, the organization only does best effort governance of human and service entitlements, making sure that policies granting permissions actually align with business functions and that the access on the service level makes sense.

At the **Opportunistic** level, the organization gains visibility into the effective permissions each identity has for each resource (i.e. being able to identify what each identity may access and which identities can access which resource).

At the **Repeatable** level, the organization is able to classify all privileged identities. This is composed of two parts:

- Understanding what actions are, in fact, considered privileged in the environment. There are the straightforward answers, such as admin level permissions, control level access to mission critical resources or access to

view and/or manipulate sensitive data. There are also some actions that usually go unnoticed, such as the ability to privilege escalate to admin level permissions or run code on certain resources.

- Finding the identities that are entitled to these permissions, thus understanding which are the privileged identities in the environment, also being able to govern them.

At the **Automated and Integrated** stage, the organization performs very fine grain controls of privileges to enforce high resolution least privilege. The organization enables only the needed permissions based on actual business functions for both human and service identities, automates this process to detect changes, continuously analyzes the environment as it changes, and even grants permissions in a just-in-time manner.

Data

Sensitive data and its posture are extremely important components of any security strategy. This framework helps you understand at what level sensitive data is segregated from other resources.

At the **Ad Hoc** level, the organization only employs the very basic data security best practices, and the segregation of sensitive data is an afterthought. Practices such as encryption (at rest and in transit) and backups are employed; however, there is no separation (at least, no strict separation) between various kinds of data.

At the **Opportunistic** level, a distinction is made between data which is public and data which is not. There's governance of which data is made public as well as management of the process making data public, therefore there is some separation between different types of data.

At the **Repeatable** level, there's governance for the separation of data into critical and non-critical environments, ensuring that sensitive data only resides in dedicated environments for better protection (e.g. between test-staging-production environments, third parties environments, operational environments).

At the **Automated and Integrated** stage, there's granular segregation on the resource level between sensitive data types. This enables the organization to control and govern the existence of different types of data even within the same critical environment.

Computing

Compromised computing resources may be breached as the target of an attacker or used as a vehicle through which additional attacks may be made. Because of this, it's important to assess what governance, security controls and configuration are in place to protect workloads from being compromised.

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
No governance and visibility of compute security posture	Conducting Host (OS / Containers) patch management	Implementing Host (OS / Containers) configuration best practices	Vulnerability management for software packages

At the **Ad Hoc** level, vendor default and best effort configurations are used, but there is no real governance of security posture.

At the **Opportunistic** level, patch management is done on the host level (e.g. for the operating system/container images).

At the **Repeatable** level, host configurations and hardening best practices are done (e.g. CIS bechmarks for the relevant OS), as well as enforcement of endpoint and network security policies on the machines.

At the **Automated and Integrated** stage, vulnerability management is employed on software packages to check third party and proprietary libraries for potential application vulnerabilities that may be exploited.

Network access

What governance is done to compartmentalize network traffic, and in what resolution is it performed?

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Ungoverned network access	Public access is governed and remediated	Network access to sensitive resources is restricted	Microsegmentation of network resources

At the **Ad Hoc** level, there is ungoverned network access.

At the **Opportunistic** level, resources are governed to ensure no unwarranted public access to the internet (e.g. making sure storage and databases are not publicly exposed to be accessed from anywhere).

At the **Repeatable** level, restricting and governing network access to sensitive (e.g. resources holding regulated customer information) and mission critical resources (e.g. computing/data resources required for proper business functionality) are standard.

At the **Automated and Integrated** stage, full micro-segmentation is applied and governed across all network resources, ensuring that only actually required network access is permitted for any resource that resides in the network.

Detection

Collecting and reviewing logs is a key factor in how soon an organization can detect potential incidents, how many of them will be found, and how well the organization will respond to them.

Log collection

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
Distributed /cloud vendor default	Centralized logs	Indexed and queryable logs	Normalized and enriched information

Log analysis

Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
None / Manual review of logs	Detection of specific suspicious events	Detection of IoCs from native monitoring tools	Comprehensive detection of anomalous behaviour

At the **Ad Hoc** level, the organization usually uses the out-of-the-box logging ability provided by the cloud vendor. This means that the organization wouldn't be familiar with accessing and/or effectively reviewing them..

At the **Opportunistic** level, logs are centralized across regions and cloud providers and are usually reviewed automatically with logic that will detect very specific suspicious events like change management, privilege escalation or network configuration management.

At the **Repeatable** level, the logs are indexed and queryable, which also means the organization is experienced at performing relevant queries which can be employed for investigating incidents or detecting indications of compromise. At this stage, the organization will start to employ cloud native monitoring tools using a large set of signatures for detecting indicators of compromise and will also be able to properly process and respond to them.

At the **Automated and Integrated** stage, the data in the logs is not only indexed but is also normalized so identities and resources are identified by exactly the same values in all logs. If the same resource is referred to differently by different event entries, or if the same identity is referred to differently across services or environments - those differences would be resolved and normalized to a single identification. Logs data is enriched by creating references between pieces of information relevant to each entry. If a proxy identity is used by an originating identity, the relevant log entries for the proxy identity would also include the data for the originating identity so it can be easily identified.

At this stage, monitoring for abnormal behavior is done compared to a baseline, thus allowing for a comprehensive detection of potential breaches and known signatures for indicators of compromise.

So... what's next?

When presenting the model, a common question we get asked is: “When is the best time to apply it?” The answer to that, of course, is an enthusiastic: “Right now!”

The process of constantly assessing and moving your organization’s cloud security strategy forward is not a luxury in this day and age, and no matter what the current level of your organization’s maturity is, you have to at least recognize it; this framework will help you do so. It’s flexible and doesn’t require a huge commitment to begin, so it can be that first step you take in launching an iterative cloud security program to propel your organization towards becoming mature in this very important - and hard to tackle - domain.

If you have any questions, or want to learn about how our technology can help you promote your cloud infrastructure security faster - feel free to contact us.