

Cloud Threat Modeling Guidance

**March 2021**

***Authors:***

* *Login to your Google account to access full editing permission.*
* *Change from Editing to Suggesting in the upper right of the Google doc for tracking each author’s edits.*

*Please contact research@cloudsecurityalliance.org to request full access to author this document.*

***Reviewers/Visitors:***

* *If you have a Google Account, please login before commenting. Otherwise, please note your name and affiliation in the comment you leave.*
* *Use the Comments or Suggesting features on Google docs to leave your feedback on the document. Suggestions will be written in and identified by your Google Account. To use the comments feature, highlight the phrase you would like to comment on, right click and select “Comment“ (or Ctrl+Alt+M). Or, highlight the phrase, select “Insert” from the top menu, and select “Comment.” All suggestions and comments will be reviewed by the editing committee.*

*For more information about Google's Comments feature, please refer to**<http://support.google.com/docs/bin/answer.py?hl=en&answer=1216772&ctx=cb&src=cb&cbid=-rx63b0fx4x0v&cbrank=1>*

# Table of Contents

[**Table of Contents**](#_jy4w1q8c7c60) **2**

[**Acknowledgements**](#_3cn3vyqelajt) **3**

[**Introduction**](#_not8hqwpwy51) **4**

[**Purpose**](#_7waoi0brkl08) **6**

[**Target Audience**](#_l8yliw40bqgu) **6**

[**Key Takeaways**](#_d4lxfrlro1w3) **6**

[**Threat Modeling**](#_gcm9kmheiiwg) **7**

[**Cloud Threat Modeling**](#_jwe7x41g5yfu) **10**

[**A Cloud Threat Modeling in Practice**](#_5wyvm8bzq5u5) **15**

[Using a Cloud Threat Model](#_njx2g9t1fvkb) 15

[**Conclusions**](#_nosx3k7qnjyd) **16**

[**Case Study Threat modeling -**](#_8it5aflt8gay) **17**

[**References**](#_70flbrxeytma) **18**

[**Appendix**](#_ke8gauo82kl1) **19**

[**CAPEC**](#_o4rs1u21rg0r) **24**

[ABC](#_8g7lzyjo4fvf) 28

[Measuring Risk](#_iatbpc78vdmr) 28

[Key Performance Indicators (KPIs)](#_m4ffvv3xwysm) 28

[Research and Standardization](#_gfg7xowoahwc) 31

[My references:](#_7p9jqoec5oed) 31

[PREVIOUS NOTES](#_3oghcgs2t52) 31

[**OUT OF BOUNDS - DO NOT INCLUDE THIS IS THE DOCUMENT**](#_p30it5rezqt6) **32**

# 

# Acknowledgements

## Lead Authors

Definition: Writer with more than XX words/paragraphs/pages.

Abc, name, name, name

Contributors

Definition: Writer with less than XX words. Reviewer w/ “significant” number of comments (5/10/20)

Name, name

CSA Staff

Sean Heide,

John Yeoh

# Introduction

Businesses look to technology as an enabler, with a goal of creating financial opportunity through automated cost reduction or cost avoidance. One of the areas we worry about surrounds vendor lock-in. This is not just through product choices between Cloud Service Provider A or B, but skills gaps and technical differences necessary in supporting those vendors. Each CSP implements controls differently, accounting for threats with equal effectiveness, but inconsistent methodology. We expect a potential where cloud threat modeling may cover these differences.

Imagine a scenario where a portfolio solution implements the appropriate threat mitigations based on a chosen Cloud Service Provider’s threat profile. Application developers or solution architects will look for the CSP service or product best fitting the need in their product. The security team provides a threat assessment and after modeling the various vendors creates a control profile for each CSP option, potentially through a corresponding Cloud Security Posture Management (CSPM) capability. Without regard for the

Create financial opportunity, enabling the business, swapping between service providers

Looking forward, the potential from dynamism associated with continuous cloud threat modeling creates new financial opportunities. Imagine a situation where a portfolio solution implements the appropriate threat mitigations based on a chosen xxxxx. xxxxx The security team provides a threat assessment and after modeling the various vendors creates a control profile for each CSP option, potentially through a Cloud Security Posture Management (CSPM). without regard for the

We know that cloud X are being targeted, this is not a debate about whether the cloud is secure enough but rather a resource on a practice that can help secure, enable, foster trust

Threat modeling describes techniques of outlying and identifying a comprehensive picture of threats and preventive measures for a planned or an existing system or application. It is a crucial practice in secure development, design, decision making and prioritization of security efforts.

Threat modeling is a cornerstone process in software and secure development lifecycles, penetration testing, application and systems security. It is well defined, adopted and prescribed by leading institutions such as NIST, non for-profits such OWASP and industry makers (and adopters) such as Microsoft.

There is guidance on threat modeling for web applications, native systems, virtualization, and even for microservice and orchestrated workloads. So far, this was not true for cloud systems, services and environments. A lot of confusion, term definitional standardization

# 

# Purpose

**The purpose of this document is** **to** enable and encourage cloud and security practitioners to apply threat modelling for cloud applications, services and security decisions. To that end, this resource provides crucial guidance to identify threat modeling security objectives, set the scope of assessments, decompose systems/application, Identify and rate threats, identify vulnerabilities in the system design, design and prioritize mitigations and controls, communicate/report & call to action.

# Target Audience

The target audience of this document are security practitioners that need to analyze threats and assess system preparedness or design cloud systems and services. However, there also are executive takeaways and insights provided for CIOs, CISOs and Senior Management as context on what cloud threat modelling is, its unique role, how it’s different to standard threat modelling, its objectives and how it fits within a cybersecurity strategy. Developers and Architects will find this document useful when designing secure cloud systems as will auditors and regulators when assessing an entity's threat modeling activities.

# Key Takeaways

Because of the difference of the cloud threat modeling considerations such as threats, unique expertise, training and experience are necessary. Threat modeling skills do not translate to cloud scope as is.

Abc

abc

# 

# Threat Modeling

Threat modeling describes techniques of outlying and identifying a comprehensive picture of threats and preventive measures for a planned or an existing system or application. Before we discuss *cloud* threat modelling, we will describe below key threat modelling qualities and processes taken from various standards and best practices, ones which best serve, to our opinion, as foundation to *cloud* threat modelling.

**The purpose of threat modeling**

* Making a reasonable effort considering security in a given scope
* Identifying, analyzing and rating [security](https://en.wikipedia.org/wiki/Computer_security) [threats](https://en.wikipedia.org/wiki/Threat_(computer))
* Produce prioritized mitigations

We’ve analyzed STRIDE, MITRE ATTACK, OWASP Threat modeling, PASTA, etc and consider the core process steps of threat modeling to be as follows

**Core Threat Modeling Activities**

1. **Identify threat modeling security objectives** for the threat modeling exercise focused on key aspects such as confidentiality,integrity,availability, privacy . e.g. a) Protect the company's databases containing customer or regulated information from external attackers. b) Ensure high availability for your e-commerce web application.
2. **Set the scope of the assessment** with respect to the systems under consideration by providing an overview of the system or application under review. This would typically cover areas such as the technology stack used,existing security controls, deployment scenario, type of users, any specific security requirement which needs to be addressed in the threat modeling
3. **System/application decomposition:** This typically covers breaking down the system into subsystems and examines the interaction among the various smaller components. The key activities done in this phase are -

a. **Understand trust boundaries** (external & internal facing, privileged, unauthenticated, etc)

b. **Identify entry and exit points** to the system (input and output) and format

c. **Map the data flows** in the system

1. **Identify and rate the threats**: ldentify the threats, type of attacks and how the given system or its functionalities can be misused by a malicious user. Some of the common threats are related to unauthorized access , denial of service, information disclosure etc. The severity of the threat can be rated by using a framework such as DREAD.
2. **Identify weaknesses and gaps in the system design and components** to aid the security decisions and define the scope and nature of security testing.
3. **Design and prioritize mitigations and controls** applicable to the predetermined threats, reflect how those controls would reduce the threat or risk level
4. **Communicate & call to action:** Communicate the identified threats, their potential impact & severity as well as the applicable and proposed controls. Make the modelling data & insights available and call to the action of threat medication by design or in effect.

**Furthermore (but not necessarily a part of threat modeling), the following steps can and often should be undertaken -**

* Assessment of existing controls can be conducted and taken into account (if the systems is in existence, rather than in design or development)
* Security testing of the system in scope (like penetration testing, security requirements testing)
* Measurement of metrics and assessment of key performance indicators for controls
* The identified threats can be categorized based on well known models such as Microsoft's STRIDE model
* Model the Attack: Creating visual representations of the threat or attack surface
* Devisement of a threat modelling and/or security concept reports that touch on scope, threat modelling considerations, provide further guidance on the mitigation plan and threats. See appendix for more.
* Devisement of a mitigation plan, or a more comprehensive risk analysis and treatment plan
* Threat actor analysis (motivations, means, methods, techniques, sophistications, industry threat actor matching, etc)

Threat modeling is often considered necessary for penetration testing, it allows a focus on key testing objectives and therefore a better return on investment for the testing. Testing post implementation of the conceived controls in threat modeling can also be conducted after they have been implemented, to assess for effectiveness and establish assurance and trust.

A paragraph on threat modelling in SDLC?

A summary statement of our take on threat modelling, the way we envision it most useful as a base for cloud threat modelling?

# 

# 

# Cloud Threat Modeling

Cloud threat modelling expands on good and standard threat modelling practices to account for unique cloud services, applications and considerations. Observations are made below on how cloud threat modelling would differ from non-cloud threat modelling, it is suggested that security and cloud practitioners consider these insights and suggestions to use threat modelling more effectively, and frequently for their advantage.

We approach the act of providing guidance for cloud threat modelling by first analyzing how a specific threat modelling consideration is different, if at all, once cloud comes into scope.

## Is the Purpose of Cloud Threat Modelling Different?

* The purpose is *not* different, but is of higher impact and importance.

The purpose of cloud threat modeling (threat modeling of cloud systems and services, ones such in cloud environments) is similar to threat modelling in other cases at its core - identify prioritized mitigations, make an assessment of security considerations and identify threats.

Yet, it is unique in the way that it is MORE important to conduct than if ‘cloud’ was not in scope.

### First, cloud threat modeling enables and drives secure cloud adoption -

From the onset of cloud technology, more so than with other technologies or changes, security was preventive to adoption. Although most security related barriers, technology, regulation or risk related, have been lifted, decision makers still ask ‘Can I trust cloud services and infrastructure with company X, in a multi tenant fashion?’, ‘Is it safe to move key business and financial processes to SaaS from our premise?’ and ‘Can the cloud offer sufficient privacy and confidentiality controls for sensitive and regulated data?’.

Although real answers would be more complicated, Cloud Threat modeling would be a first, critical and enabling step. It would bring understanding of threats, of assets, of controls and therefore - confidence.

### Second, cloud threat modeling will help with selection of the proper consumption, service and multi-tenancy models -

When selecting service models (SaaS, PaaS, IaaS), deployment model (private, public, hybrid, community) and multi-tenancy, the primary considerations are security threats, regulation and savings. Cloud threat modeling will inform on what threats are inherent to a selection of a certain model or design, and what controls are available (and therefore what security efforts would be implied as well).

**Are the Model Components of Cloud Threat Modelling Different?**

* The model components are the same but would describe or include cloud unique entrees.

A cloud threat modelling exercise would still consider threats**,** assets, controls in place, vulnerabilities, applicable controls, rating etc.

**Scope** normally a single system is in the scope of a threat modeling. In cloud threat modeling, more of the identity management, cloud service and even underlying cloud account is given consideration.

**Assets** some of the same assets remain the chief concern of (cloud) threat modeling - data, key system components, funds, identities. But, new assets are introduced as well such as cloud accounts, SaaS subscriptions and services.

**Threats** to cloud systems, applications and environments are very much unique. Different technologies

such as instance metadata service and cross account IAM access federation come into play. Different technology and consumption models describe cloud systems. Therefore, different attacks are viable against them, and to different impacts and impact gravity than otherwise.

**Controls in place** some controls that previously would be implemented or proposed, are now controls in place - thanks to the provisions of the cloud service provider. New, unique cloud controls & technologies can be in place as well (such as metadata service protections or cloud Detection and Response (CDR), CSPM[[1]](#footnote-0) and such).

**Rating** of the risks’ severities remains standard whether cloud is in scope or not, the same concerns

apply; how vulnerable the system is to that threat, what asset would be impacted and to what extent. That said, some threats are more severely ranked (such as administrative account compromise) and others - less (such as infrastructure/protocol denial of service) due to inherent cloud qualities.

**Proposed mitigations** would be different for cloud systems and applications, as different threats are applicable. Furthermore, some controls are only available or applicable to cloud systems and accounts as they were developed and designed for them, e.g. - Service Control Policies for AWS accounts.

**Are the Threats Considered in Cloud Threat Modelling Different?**

* Cloud threats are different, unique and diverse, though many of the same still do apply.

Threats to cloud systems, applications and environments are very much unique. Different technologies

such as instance metadata service and cross account IAM access federation come into play. Different technology and consumption models describe cloud systems. Therefore, different attacks are viable against them, and to different impacts and impact gravity than otherwise.

Much of the work of this research group is aimed at learning about cloud threats and we determine that while the risk or impact may seem similar to non cloud scope (such as Data Breach, Egregious Eleven #1), the threats are unique (like AWS EC2 instance metadata account hijacking, Imperva breach, 2018).

**Is the Product of Cloud Threat Modelling Different?**

* The product and outputs are cloud threat modelling are alike to standard threat modelling.

However, threat modelling for cloud applications and services strongly impacts unique cloud related decisions.

The products or output of threat modeling are (1) the threat model, usually presented in an excel sheet or via a visual model such as tree-type mapping. (2) Prioritized mitigative controls, ranked, and (3) security and design decisions or a more conclusive and detailed call to action.

The assessment data and it’s visualization, the model, would be unique for every application, cloud or not, thus there is no unique cloud distinction to be found on those terms. So are the prioritized mitigative controls, unique for every scope, cloud or not.

Finally, there is distinction in the outputs of design decisions (or a more conclusive and detailed call to action). As described in cloud threat modelling purpose(page 8), the unique and highly impactful insights around cloud security helps decide whether cloud adoption is an option, and what the best cloud model is right. While other security activities and architectural assessments do yield design decisions around technological components, threat modelling for cloud applications and services strongly impacts unique cloud related decisions.

#### 

#### 

**Risk Management**

**Threat modeling is a component of risk management. Risk is defined as a combination of severity (impact to assets) and likelihood (how likely a threat occurs). Additional component of risk are often added to the greater equation of risk management necessarily including correlation to the “crown jewels” or most valuable assets of a company, providing a greater level of prioritization to protect such assets. Other variables may also be introduced into risk management, such as level of effort, cost, and other risks such as third party considerations. The Cloud Security Alliance recommends the following foundational cloud threat modeling process upon which organizations may customize as needed for individual priorities within their own risk management:**

**Qualify and quantify risk with four core variables for an organization:**

1. **Threat Rating**
   1. **How severe is a threat to an organization. This includes but is not limited to threats of any type including physical threats (earthquake or terrorism), malware, insider attacks, vulnerabilities, and other threats identified by an organization.**
2. **Likelihood Rating**
   1. **How likely is it that the threat will occur.**
3. **Business Impact Rating**
   1. **What is the impact upon a business if the threat occurs? Elements of preparation, time of recovery, loss of reputation and clients, and similar variables must be identified in a formal fashion to best identify this rating for an organization.**
4. **Defensive Controls**
   1. **What defensive controls exist to proactively protect, detect, and mitigate the threat? If an organization is weak against a specific threat, or more often has several layers of weakness within the killchain of an attack, this impacts this rating. Correlating threats to the MITRE ATT&CK Framework is recommended in developing this score.**

**Organizations may combine the four aforementioned ratings in an additive fashion or weighted, based upon priorities of an organization. Simple levels for scoring are** recommended **for success, such as a five point scale for each variable with one (1) for low and five (5) for a high score, with 20 points being the maximum risk possible without any weighting applied.**

**For example, the following use case reveals how to best identify RISK with the four variables for Ryuk Ransomware, the most common threat in the wild at the time of authoring this document.**

**Threat Rating 5 Provides remote command and control over an entire**

**network including a Ryuk ransomware and/or exfiltration**

**threat.**

**Likelihood Rating 5 The most common threat in the wild. Likely to impact**

**production given how it spreads via email.**

**Business Impact Rating 3 This organization is largely manufacturing with segmented**

**networks and controls from production laptops and email.**

**Impact upon production is less likely.**

**Defensive Controls 4 The production system is weak against phishing attacks**

**with no user awareness training and limited email filtering**

**and blocking of Emotet and Ryuk ransomware. This is**

**prioritized for budget spend but not in place yet to a more**

**mature state.**

**Total Risk Score 17 This is a HIGH level threat against production.**

**The above example helps business managers to align upwards, downwards, and laterally within an organization when attempting to achieve unified risk management for an organization. It can easily be customized and weighted for variables prioritized by an organization. CSA recommends developing both orchestration playbooks and runbooks for specific threats to ensure readiness. For example, a playbook for dealing with a malware event is required to go beyond incident response towards how an entire organization responds to an incident. A runbook, such as ensuring readiness for how an Emotet and Ryuk ransomware threat occurs, is critical in readiness against this specific threat.**

**Organizations that take the time to map their defensive infrastructure against specific runbooks and threats, correlated to the MITRE ATT&CK Framework, can quickly prioritize areas of weakness when compared against defensive controls to strategically mature security. For example, several runbooks may reveal that the endpoint is particularly weak, if a threat makes it past initial email gateway controls. After review an organization may decide that plans for upgrading endpoint security may be the best return on investment to best mitigate current high risk threats with other needs prioritized at a later date.**

#### 

#### Cloud Threat Modeling Process

#### **Is the Process of Cloud Threat Modelling Different**

#### The process is not different, but merges several different procedures, methodology and needs such as a holistic review of the cloud infrastructure (cloud stack) as, focus on the configuration stage, detection of the root cause as an approach to handle the risk.

#### 

#### **Core Threat Modelling Activities**

#### 

#### **Identify threat modeling security objectives**

Complementary to standard goals setting for a threat modeling exercise (identifying most impactful controls or most pressing threats, protecting confidentiality, etc), set cloud threat modelling security objectives such as identifying the most risk averse cloud service and deployment models (IaaS, PaaS, SaaS). Or determine whether ‘cloud’ or cloud architecture (such as PaaS and multi-tenancy) are permissible.

1. **Set the scope of the assessment** with respect to the systems under consideration by providing an overview of the system or application under review. In addition to typical scope definitions (systems, users, controls, etc), consider the cloud stack - is the PaaS control plane in scope? Is the cloud account? It is advisable to make an inclusive scoping.

#### **System / application decomposition:** This typically covers breaking down the system into subsystems and examines the interaction among the various smaller components.

#### a. **Understand trust boundaries** (external facing, internal facing, privileged, unauthenticated, etc). Understand *cloud* trust boundaries like trust in and segregation controls against the *CSP[[2]](#footnote-1),* cross service and account trust and multi-tenancy segregation controls.

b. **Identify entry and exit points** to the system (input and output) and format. Consider cloud unique entry points such as cloud management API, managed API gateways and integrations. Furthermore, map cross cloud service relationships.

c. **Map the data flows** in the system. Consider cloud unique data flows and stores such cloud *EMR[[3]](#footnote-2)* and ETL services*,* blob storage and account log trails.

1. **Identify and rate the threats**: ldentify the threats, type of attacks and how the given system or its functionalities can be misused by an external attacker or malicious user. Identify cloud unique threats using industry resources such as the CSA Top Threats. Do not neglect to assess threats to availability even though many controls to that end would be baked in the CSA platform and infrastructure. Give special consideration to human error insider threat, misconfigurations and poor design.

#### **Identify weaknesses and gaps in the system design and components** to aid the security decisions and define the scope and nature of security testing. Consider common and impactful cloud design and implementation weaknesses, account for defence in depth design/controls -

#### **E**gregious **E**leven**[[4]](#footnote-3) #2 -** Misconfiguration and Inadequate Change Control

#### **EE #3** - Lack of Cloud Security Architecture and Strategy

* + **EE #4** - Insufficient Identity, Credential, Access and Key Management
  + **EE #7 -** Insecure Interfaces and APIs

#### **Design and prioritize mitigations and controls** applicable to the predetermined threats, reflect how those controls would reduce the threat or risk level. Leverage cloud security controls (matrix)[[5]](#footnote-4). Focus on controls that disrupt cloud threats and attack kill chains, even when some cloud and application misconfigurations and weaknesses are in place.

#### **Communicate & call to action:** Communicate the identified threats, their potential impact & severity as well as the applicable and proposed controls. Make the modelling data & insights available and call to the action of threat medication by design or in effect. Communicate your cloud design decisions and core enabling cloud controls.

#### 

#### 

#### **THIS IS WHERE DESCRIBE WORKSHEET & CARDS**

#### 

#### 

# Creating a Cloud Threat Model

The key outcome we would like to see is more threat modeling applied to cloud systems and services in design or as part of assessments. We encourage you to create a cloud threat model today, and leverage this resource.

**How to start from scratch?**

You don’t need to be an experienced security expert or proficient at threat modeling to start, if you are, feel free to act by your own methods and preferred good threat modeling practices and consider this resource complementary, specifically discussing cloud threat modeling considerations.

If you are **starting from scratch**, then start small, start with what you are familiar with and start now -

1. Pick up one our cloud threat modelling cards from [Appendix 2](#_p30it5rezqt6), threat, vulnerability or control or another. One which you’re most concerned or familiar with.
2. Determine whether any of the other cards related to yours, align or visually place them together by the following suggest order: Threats, Vulnerabilities, Controls, Assets
3. Identify more Threats, Vulnerabilities, Controls and Assets that relate to your developing model, introduce them into your ‘mix’, into your visual or analysis. Consider referring to the latest [CSA Cloud Top Threats Egregious Eleven](https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/) for references.
   * Repeat until you have at least one of each
4. Ensure you address every threat and vulnerability with at least 1 or 2 applicable, specific controls.
5. You are done, congratulations!

Alternatively, if you feel you need a more detailed and comprehensive approach, please consider going through the steps described in [Cloud Threat Modeling Process](#_lupp0gfp0amm).

Once the modeling part is done, you’ve made a security analysis and determined actionable steps to take - take them. **Act on your identified controls and mitigate your vulnerabilities (or establish assurance of their lack, thereof).**

Your end result should look like a basic threat model, with cloud specific considerations, like ours, in the next section - ‘A Cloud Threat Model Reference’.

#### 

**A Cloud Threat Model Reference**

Find below a basic cloud threat model reference we’ve created by the very steps described in prior sections

Referring to the [CSA Cloud Top Threats Deep Dives Egregious Eleven](https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/) resource, we recall the key 2019 Dow Jones

**Actor**: An authorized 3rd party vendor for Dow Jones failed to password protect an AWS-hosted Elasticsearch database belonging to Dow Jones.

**Attack**: With no password protection, the database was available to anyone without restriction and could be found with commonly available IoT search engines. The misconfigured database was discovered in 2019 by a security researcher who reported it to Dow Jones.

**Vulnerabilities**: The Dow Jones database was not password protected by one of their authorized and presumably trusted security vendors.

A basic threat model composed of just the cloud threat modelling cards provided in [Appendix 2](#_p30it5rezqt6)



However, this model is far from complete, our cloud threat modeling cards are a good place to start, from hereon, dig deeper, expand on applicable vulnerabilities and controls -



# Conclusions

Abc

# 

# References

* <https://en.wikipedia.org/wiki/Threat_model>
* <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling> V
* <https://www.microsoft.com/en-us/securityengineering/sdl/practices>
* <https://www.microsoft.com/en-gb/download/details.aspx?id=20303>
* <https://drive.google.com/file/d/1n_uMBckp8UMBA1oq1kcKTjvXX6Ea_tLF/view?usp=sharing>   
  Model vs methodology
* CSA Cloud Top Threats Egregious Eleven
* CSA Cloud Top Threats Deep Dives Egregious Eleven
* CSA CCM Matrix
* [PASTA](https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf) (Process for Attack Simulation and Threat Analysis)
* VAST (Visual, Agile, and Simple Threat modeling)
* OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
* DREAD risk assessment model

# 

# Appendix 1: Threat Modelling Reporting detailed guidance

Devise a security concept reportwhich will be mapped to threat modeling report and will include technical level explanation of each security control that is presented in chapter 6, with detailed requirements and references to relevant risks. The document will be constructed from the following chapters:

* + Executive Summary - General explanation of the project, main goals, and cloud architecture snapshot.
  + Attack Vectors Mapping - Explanation of the top five detected risks in the architecture including the explanations, cloud architecture snapshot with detected risks’ icons on it, total security risk score and summary chapter.
  + Mitigation Plan - This chapter will include a list of the required implementation of the security controls ordered by priority. Each security control will includes the following fields:
    1. Security Control Name (e.g. SC1 - Implementation of Authentication SSO Mechanism)
    2. Priority - In this field required to define the priority of the implementation, can be Critical/High/Medium/Low
    3. Risks - Reference to the relevant risks in the threat modeling report (e.g. R1, R2, R5)
    4. Requirements - List of technical level requirements which relevant for this security control. Each requirement starting with the words: must, must not, should, and should not. For example: “The system must implement OAuth 2.0 standard using JSON Web Token (JWT) format.”

# Appendix 2: Cloud Threat Modeling Cards



1. CSPM - Cloud Security Posture Management (CSPM), monitor for, find and remediate cloud misconfigurations. [↑](#footnote-ref-0)
2. CSP- Cloud Service Provider [↑](#footnote-ref-1)
3. EMR- Elastic Map Reduce, cloud EMR [↑](#footnote-ref-2)
4. Egregious Eleven cloud security concern, more in the CSA Top Cloud Threats Research work group publication ‘[Top Threats to Cloud Computing: Egregious Eleven](https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/)’ [↑](#footnote-ref-3)
5. The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing that maps and categorizes applicable cloud controls. [↑](#footnote-ref-4)