Risk Management Policy and Procedure

Tesla Inc.

Date: Apr 25, 2025

Cole Debardelaben, Rahne Hartman, Chen Lin, Eunice Olasoko, Devan Rajendran

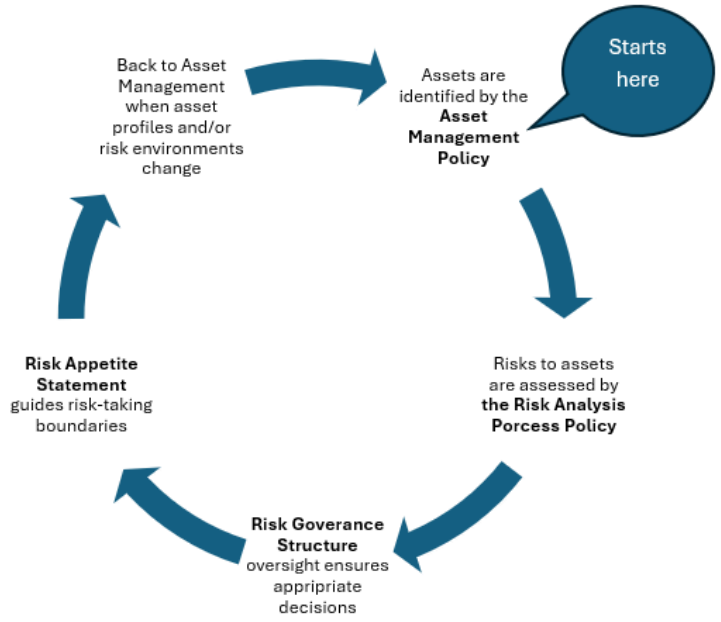
Table of Contents

Executive Summary

Tesla Inc. has developed a comprehensive Risk Management Policy and Procedure framework designed to safeguard its operations, assets, and achieve its mission to “accelerate the world’s transition to sustainable energy.” (Tesla Inc., 2025) This framework is composed of four key components: **Asset Management Policy, Risk Analysis Process Policy, Risk Governance Structure,** and **Risk Appetite Statement.** These components enable a consistent and proactive approach to identifying, managing, and responding to risks across the enterprise, while ensuring alignment with corporate strategy.

1. Introduction

Tesla's Risk Management Policy and Procedure designed as an comprehensive framework, where each component supports each other in a continuous cycle of managing risks:



The **Asset Management Policy** serves as the starting point, which defines what Tesla considers an "asset". Proper asset identification, classification, and valuation are crucial, as risks cannot be assessed or managed without first understanding what is at stake. Once assets are understood, the **Risk Analysis Process Policy** provides the structured methodology for evaluating risk to those assets using the OCTAVE Allegro framework. It defines how to identify, assess, and prioritize risks. The **Risk Governance Structure** defines who is responsible for making decisions for risk-related processes. Accountability and escalation processes are established. The **Risk Appetite Statement** sets the limits and thresholds for risk acceptance across various domains. Decision-making across all levels of governance and operational planning will be formed in a consistent manner. Each of the four components in this document was prepared in the same sequence: *what* the policy is, *why* this policy is required, and the procedure on *how* to apply the policy. Discussions of the Acceptable Response Plans, Risk Ownership and working with Tesla's corporate strategy are included in the Other Considerations section at the end.

2. Asset Management Policy

2.1 What Asset Management Policy Is

This document contains the Asset Management Policy for Tesla Inc. developed as part of the risk management program. For the purposes of this document, assets subject to the procedures outlined within are defined as all company assets including but not limited to: all employees, all data both print and digital produced by or contained within the company, all physical products and machinery, all warehouses, offices, and production facilities, and all services provided by third parties. This policy will be maintained by the chief risk officer and the procedures within will be carried out by the risk management team, with bi-annual assessments of the efficacy of the policy. The procedures of this policy are cyclical in nature as new assets are acquired, values change, or assets leave Tesla.

2.2 Why Asset Management Policy Is Required

The purpose of the Asset Management Policy is to ensure consistent handling of all company assets within Tesla Inc. throughout the asset's lifecycle with regards to maintaining confidentiality, integrity, and availability, as well as clear asset classification and asset ownership. Effective asset management will also assist Tesla Inc. with risk and threat management by enabling easier identification of weak links in services and processes. Implementing a systematic asset management approach at Tesla provides measurable cost savings, risk reduction, and long-term operational efficiency. The benefits can be categorized as follows.

2.2.1 Operating and Maintenance Cost Savings

Optimizing asset utilization reduces maintenance costs and prevents unexpected failures. A structured asset management strategy enables Tesla to minimize downtime in Gigafactories and optimize the efficiency of production equipment, leading to increased productivity and lower operational expenses. Network Rail saved £178 million by adopting a systematic approach to Asset Management (Justin, 2011).

2.2.2 Extending and Preserving Asset Life

Proactive maintenance extends asset lifespans, reducing the frequency of costly replacements. Timely intervention prevents Tesla's critical infrastructure like battery production lines, supercharger networks, and software platforms from deteriorating prematurely. For example, New York State's Department of Transport found a five to six times difference in cost between repairing "poor" and "very poor" condition highways. This aligns with De Sitter's "Law of Fives" that neglecting maintenance leads to exponentially higher repair and renewal costs (Justin, 2011).

2.2.3 Performance Improvement

Effective asset tracking and predictive analytics enhance Tesla's ability to monitor and improve key performance indicators (KPIs) across production, service, and logistics. With real-time monitoring of manufacturing equipment and vehicle performance, Tesla can optimize resource allocation, enhance production output, and improve customer satisfaction through higher reliability and service quality (Justin, 2011).

2.2.4 Business Risk Reduction

Asset failures pose operational, financial, and reputational risks. A structured asset management approach allows Tesla to identify and mitigate risks proactively, whether related to manufacturing defects, supply chain disruptions, or cybersecurity threats to its digital infrastructure (Justin, 2011).

2.3 How to Apply Asset Management Policy

Three-step procedure will be introduced to apply this policy. It starts with identifying who the stakeholders are to clarify the risk ownership. Then, the Asset Management Process will be introduced with examples in the Appendix 1. Finally, proposed solutions are discussed to address some inevitable

challenges. Assets identified through the procedure become the subjects of the Risk Analysis Process in the next section, which aligns resource awareness with Tesla's strategic priorities.

2.3.1 Identifying Stakeholders for Asset Management

Tesla maintains key stakeholders within and external to the company itself. Each of these groups benefit from Tesla succeeding and maintain individual interests for the company's operations. These groups are as follows.

2.3.1.1 Shareholders

One of the primary purposes of a company is to produce value for the shareholders. Tesla's shareholders can be found both within and outside of the company. Overall, institutional investors hold 47.5% of Tesla's stock, with the remaining split between executives, employees, and individual investors (Nasdaq, 2025).

2.3.1.2 Employees

Tesla's employees are essential to the success of the business. Tesla's employee base is multinational, and represents many fields, due to its nature. Manufacturing, robotics, AI and machine learning, engineering, and software design exist alongside traditional fields such as marketing, sales, finance, and legal (Tesla, 2025).

2.3.1.3 Suppliers and Partners

While many of the components used in Tesla's cars are built inhouse, the materials required to make them are obtained via 3rd party suppliers. Many of Tesla's suppliers are not disclosed, but they work to provide the materials Tesla needs at various stages of production (Maverick, 2024).

2.3.1.4 Customers

Customers represent a significant stakeholder in Tesla's success. Tesla dominates the EV industry, particularly within the domestic market, representing over 50% of the USA's EV sales (Montoya, 2024).

Customers expect high-quality, reliable vehicles, and many bought Teslas due to their climate-related premise and sustainability.

2.3.1.5 Government

As Tesla is an automobile manufacturer, it is subject to regulations. Maintaining legal standing is important to ensuring Tesla's availability. Tesla is also in the spotlight due to Elon Musk's relationship with Donald Trump. For example, President Trump recently showcased multiple Tesla models in front of the White House (Ingram, 2025).

2.3.2 Asset Management Process

This section will provide an outline for the process of asset management at Tesla Inc. For examples of the application of this process in relation to different types of assets, please refer to Appendix 1 where a set of 8 tables are used to demonstrate the asset management process.

2.3.2.1 Plan for Asset Management

The first phase of the asset management process is to develop a plan for asset management. During this phase, Tesla Inc. should also reassess the purpose and objectives, ensure support from management, examine possible risks, assign responsibility for asset management, and ensure that activities remain within the allocated budget (Tucker, 2025, *Module 2_Asset Management_Tucker_Spring_2024,*). Achieving this may necessitate reviewing company plans, contracts, customer communications, and work processes within the company (Tucker, 2025, *Module 2_Asset Management_Tucker_Spring_2024*).

At the end of this phase, asset definitions should be confirmed and the asset management team should have a prioritized list of services with short profiles justifying the reason for prioritization (Tucker, 2025, *Module 2_Asset Management_Tucker_Spring_2024*).

2.3.2.2 Identify Assets

During this phase, the prioritized list of services is taken and then the assets are identified and defined based on their role in supporting these services. Each asset should be linked to the specific service it enables. These assets are then categorized as People, Information, Technology, Facilities, and External assets. This will be a comprehensive list of assets, type, and critical service supported to understand the lifecycle and role of the asset in the organization (Tucker*, 2025, Module 2_Asset Management_Tucker_Spring_2024*). Creating an asset profile for each asset begins to identify risks and unique characteristics that should be considered.

2.3.2.3 Document Assets

Once the assets are identified, an Asset Inventory is created. The asset inventory is made using details gathered during the Identification stage. Asset profiles include, but are not limited to - Type (People, Information, Technology, Facility, External), Categorization by sensitivity, Location of asset and backups, Owners and custodians, Format/form, Asset Security, Dependent services and Value for each asset (Tucker*, 2025, Module 2_Asset Management_Tucker_Spring_2024)*.

This helps link the assets with the services, which can lead to finding any assets that can support multiple services in Tesla and determining the High Value Assets (HVAs) that Tesla owns. Documenting the assets can leave room for repeated revision of the assets to adapt with the requirement changes and thus can provide more comprehensive asset management (Tucker*, 2025, Module 2_Asset Management_Tucker_Spring_2024)*.

2.3.2.4 Manage Assets

Tesla has been a pioneer at many technological advancements in recent years. This means that the services that are provided by Tesla change very frequently. As services change, assets change and resilience requirements and protection strategies change accordingly. Thus it is important to develop a

change criteria consistent with each asset and a combination of asset types which are independent to Tesla. (Tucker, *2025, Module 2_Asset Management_Tucker_Spring_2024)*

2.3.3 Expected Challenges and Proposed Solutions

Operating in a dynamic environment, some challenges outside the standard Asset Management Process discussed above may also be expected by Tesla. Some of these challenges are listed below with proposed solutions.

2.3.3.1 Asset Stocktake

Due to Tesla's rapid expansion in its global presence and diversified operations in many fast-growing industries (Tesla Inc., 2025), it will be a challenge to have a complete and accurate asset stocktake in a timely manner. Some assets may not be included in the asset management process or their information may not be accurate. To address this challenge, a centralized asset register shall be established that is accessible to all relevant staff across Tesla to manage assets. This may reduce the risk of having incomplete and/or inaccurate assets records. In addition, regular asset audits should be conducted to reconcile and validate asset records.

2.3.3.2 Shadow IT

The use of IT hardware or software by individuals without the approval of the organization's IT department may create 'Shadow IT' (CISCO, 2025). Although there is currently no reported evidence about shadow IT practice within Tesla, with the rise of work from home since the COVID-19 pandemic, a significant increase in hardware shadow IT usage has been observed within the broader industry (Chipeta, 2025). To minimise the risk of Shadow IT, at a high level, continuous policy enforcement to mandate approvals for all the IT assets deployed across Tesla should be enacted. On an individual level, Tesla staff should be regularly educated on security awareness. From a technical perspective, tools to identify unauthorized devices and applications need to be utilized (Scarfone, 2022).

2.3.3.3 High Value Assets (HVAs)

As an industry leader, Tesla owns large numbers of HVAs, such as its self-driving and battery technologies, which are prime targets for espionage, insider threats, or data breaches. For example, a data breach that affected Tesla in May 2023 has been officially attributed to “insider wrongdoing” (Powell, 2023). To protect Tesla’s HVAs, a Zero-Trust Architecture with strict identity verification and continuous monitoring is required.

3. Risk Analysis Process Policy

3.1 What Risk Analysis Process Policy Is

The Risk Analysis Process section covers the risk analysis process for Tesla Inc. as part of the risk management program. For the purposes of this document, a risk is realized and must be analyzed when there is a probability of a threat, an event that would harm the company, and when the impact of this threat is determined or estimated. The risk analysis process within this document is applicable to any company assets and follows the steps of OCTAVE Allegro as a guide. Maintaining the standards of Tesla's risk management program, this policy will be maintained by the chief risk officer and the process will be carried out by the risk management team, with bi-annual reviews on the efficacy of the process. This process is cyclical in nature and ongoing as assets move within the company, interests of actors change, and technology continues to evolve, requiring regular consideration of what risks Tesla faces.

3.2 Why Risk Analysis Process Policy Is Required

The purpose of this policy is to ensure that Tesla establishes and maintains a consistent risk analysis process across all company assets. With consistent risk analysis, the company should feel more capable of identifying what risks most urgently need to be addressed to avoid loss of profit, loss of company reputation, data breaches, legal fines, or other potential negative consequences. This purpose serves the interests of multiple stakeholders such as the owners of the company and stockholders who seek to remain profitable, employees who want job security, customers who want a reliable product, and third party providers who do business with Tesla.

3.3 How to Apply Risk Analysis Process Policy

The risk analysis process outlined for Tesla below follows OCTAVE Allegro. For examples of how to apply this process to an information asset, please see Appendix 2.A . For a non-information asset, please see Appendix 2.B. The outputs of this analysis such as the risk levels and recommended actions are communicated to the appropriate governance tier for oversight and decision-making. Each assessed risk is compared to Tesla's defined Appetite Statement to determine whether it is acceptable or requires action.

3.3.1 Establish Risk Measurement Criteria

Successful analysis of risk within Tesla requires the baseline establishment of risk measurement criteria. These criteria define the ranges of high, medium, and low impact that a risk has on the company if the related incident were to occur. These criteria should be consistent throughout Tesla to ensure that risk based decisions can be accurately made when making comparisons. These criteria should be qualitatively defined using impact areas important to Tesla which may include: reputation, financial, productivity, safety and health, legal penalties, and any other user-defined areas, which then should be prioritized with the highest number as the most important and the lowest as the least important (OCTAVE Allegro Student Workbook v1.0, 2012). This step corresponds to the appendix Worksheets A.1-A.7 for a sample of information asset and Worksheets B.1-B.7 for a sample of non-information asset.

3.3.2 Develop an Asset Profile

Developing an asset profile requires an assessment of which assets are of concern to Tesla, particularly assets that could cause harm to the company if they are improperly disclosed, modified, lost, destroyed, or interrupted (OCTAVE Allegro Student Workbook v1.0, 2012). This step draws on information gathered from the asset management process, and it is advised to review that process for this step. Examples of information and non-information asset profiles to use in the risk analysis process are in appendix Worksheet A.8 or Worksheet B.8.

3.3.3 Identify Asset Containers

The vulnerability of assets and their associated risk must be considered both when the asset is at rest or when it is in transit. During an asset's life cycle, it is stored, transported, and processed within a container which could be a true physical container, a technical asset such as hardware or software, or simply a person holding information (OCTAVE Allegro Student Workbook v1.0, 2012). Identifying ways to protect and secure these containers is necessary to determine the extent of the vulnerability or threat a container is subject to, while ensuring that all containers an asset travels through are considered. This step corresponds to appendix Worksheets A.9a-c or Worksheets B.9 a-c.

3.3.4 Identify Areas of Concern

This step begins to assess the threat associated with risk, explained as an area of concern that correlates to potential real world scenarios that could harm a company asset (OCTAVE Allegro Student Workbook v1.0, 2012). This step does not intend to identify all possible areas of concern, but by identifying some specific areas of concern it becomes easier to understand the threats facing Tesla and consider how to respond. For this step, use the worksheets completed in Step 3.3 and consider each container for an area of concern. For each area of concern identified, think of a threat scenario during which an asset could be compromised and work through sections 1-5 of Worksheet A.10 or Worksheet B.10 on a new worksheet (OCTAVE Allegro Student Workbook v1.0, 2012).

3.3.5 Identify Threat Scenarios

For this step, it is important to understand the components of a threat: an asset, an actor, how the actor gains access to the asset, a motive for why the actor wants access, and the outcome of the asset being misused (OCTAVE Allegro Student Workbook v1.0). Each of these components contributes to how a threat should be addressed and understood, and they can be useful in determining if a threat scenario is realistic. In this step, consider if there are any threat scenarios facing the asset of interest that were not

covered by the areas of concern by using Threat Scenario Questionnaires A1.-3 or Questionnaires B.1-3 to review Worksheets A.9a-c or Worksheets B.9a-c accordingly. Any new threat scenarios should receive their own Asset Risk Worksheet (A.10 or B.10) with sections 1-5 completed, and then optionally complete section 6 for all Asset Risk Worksheets if assessing probability is desired (OCTAVE Allegro Student Workbook v1.0). A threat tree may also be useful for this step as demonstrated below using Tesla's Supercharger Network and Tesla's Autopilot Code as examples.

Assets	**Actors**	**Outcomes**
Tesla's Supercharger Network (non-information asset)	Malicious hacker	Unauthorised access and Malware injection
	Employee	Data theft and System sabotage
	Competitor	Supply chain disruptions
		Intellectual Property (IP) theft
	Natural disaster	Charging station downtime
Tesla's Autopilot Code (information asset)	Malicious hacker	Reverse engineering and Malware injection
	Software developer	Insure access and Source code leakage
	Competitor	Intellectual Property (IP) theft

3.3.6 Identify Risks

Now that areas of concern and threat scenarios have been identified, their potential consequences and the impact of those consequences on Tesla must be examined to fully understand the risk the company faces. For this step, go back to each recorded threat scenario and determine what the impact would be if the

scenario occurs, then document the consequence in section 7 of each Asset Risk Worksheet (A.10 or B.10) (OCTAVE Allegro Student Workbook v1.0).

3.3.7 Analyze Risk

With risks now being identified, they must be analyzed to determine which one is the most urgently needed to be addressed and which risks can be deferred or accepted for the time being. Assigning a relative risk score as a qualitative value assists in the prioritization of risks. Return to the worksheets filled out as part of establishing risk measurement criteria and go through the consequences of each Asset Risk Worksheet. Determine if the consequence falls under a low, moderate, or high impact and record this in the Value column of section 8 of the Asset Risk Worksheet. Next, look at the Impact Area Prioritization Worksheet (A.7 or B.7), and multiply those rankings by the impact value, using 1 for low, 2 for moderate, and 3 for high. Record the result in the score column, then add each together. The result is the relative risk score for each identified threat scenario. The higher this score is, the more urgently the risk should be addressed, however, the difference between the scores is not indicative of the extent to which one risk is greater than another (OCTAVE Allegro Student Workbook v1.0).

3.3.8 Select Response Approach

The final step of the risk analysis process is to decide how to respond to identified risks; should they be accepted, mitigated, or deferred? This decision should be made with the understanding that it is impossible to remove all risk, and Tesla must accept some level of risk (OCTAVE Allegro Student Workbook v1.0). When mitigation is chosen, it can be carried out by implementing technical, physical, and administrative controls to make it more difficult for vulnerabilities to be exploited, and/or by implementing changes that will lessen the impact to Tesla (OCTAVE Allegro Student Workbook v1.0). To help determine how to respond, take the risks previously identified and sort them by their relative risk score, then determine how best to group them to match Tesla's needs. If probability is being considered,

risks with high relative risk scores and high probability should be considered first with the ranking decreasing accordingly. Once the risks are sorted, decide if they should be accepted, mitigated or deferred and indicate this decision in section 9 of the Asset Risk Worksheet (A.10 or B.10). Any risks being mitigated must then have a response strategy decided on, which will vary based on the risk itself (OCTAVE Allegro Student Workbook v1.0).

4. Risk Governance Structure

4.1 What Risk Governance Structure Is

Tesla's Governance Structure (RGS) adapts the OCTAVE FORTE three-tier methodology (Tucker, 2020) to Tesla's unique business environment by balancing Tesla's strategic risk oversight (*Tier 1: Executive Board*), operational risk management (*Tier 2: Risk Committee*) and functional technical expertise (*Tier 3: Risk Subcommittees*) to respond to the emerging challenges in the industry. An overview of Tesla's RGS is summarized in the table below.

Tiers	Members	Responsibilities
1. Executive Board	Chief Executive Officer, Chief Financial Officer, Chief Legal Officer, Independent board members	Approves mission related risk strategies; oversees legal, financial, and reputational risks
2. Risk Committee	Chief Risk Officer, Heads of the Automotive, Energy, and AI divisions	Coordinates operational risk management across Tesla
3. Risk Subcommittees	Departmental risk leaders and operational managers	Manages functional risks across Tesla

4.1.1 Tier 1 - Executive Board

There are three tiers in Tesla's RGS and Tesla's Executive Board is the Tier 1 at the highest level and serves as the ultimate authority for enterprise risk management. Comprising the *Chief Executive Officer*, *Chief Financial Officer*, *Chief Legal Officer*, and some independent board members, Tier 1 is responsible for approving the enterprise risk appetite, endorsing major mitigation strategies, and overseeing Tesla's exposure to strategic, financial, regulatory, and reputational risks.

The Executive Board meets quarterly to review risk reports and will serve as the final escalation point for critical risks identified across Tesla's global operations. It aligns risk management initiatives with the company's long-term objectives and obligations to shareholders.

4.1.2 Tier 2 - Risk Committee

Tier 2 acts as the operational leader for Tesla's risk management framework and consists of 5 to 7 senior executives such as the Chief Risk Officer, Heads of the Automotive, Energy, and AI divisions. This tier plays a pivotal role in bridging the strategic guidance of the Executive Board with the operational practice of Tesla's business units to ensure that risks are managed systematically across the organization.

Meeting every two months, the Risk Committee coordinates cross-divisional risk assessments, monitors the consolidated enterprise risk register, allocates resources for mitigation actions, and recommends significant risk actions to the Executive Board (Tier 1).

4.1.3 Tier 3 - Risk Subcommittees

At the functional level of the RGS, Risk Subcommittees are responsible for Tesla's day-to-day risk management within specialized areas. Departmental risk leaders and operational managers are the members of the Risk Subcommittees.These subcommittees will maintain updated risk registers, monitor risk mitigation performance, and contribute to improving Tesla's risk management processes. They meet monthly to identify, assess, and respond to functional risks, escalating significant threats to the Risk Committee (Tier 2).

4.2 Why Risk Governance Structure Is Required

To achieve its mission to 'accelerate the world's transition to sustainable energy' (Tesla Inc., 2025), a RGS must be established by Tesla. As the formal system, RGS defines who is responsible for managing different types of risks in an organization, how risk-related decisions are made, communicated and enforced. It ensures risk owners are assigned and response plans are implemented for specific risks and guides risk decision-making within acceptable boundaries.

4.3 How to Apply Risk Governance Structure

Tesla's risk governance structure depends on its stakeholders at each level of the aforementioned governance structure. Within the tiers of the structure, individuals are tasked with specific risk-related duties, with obligations at each descending tier becoming more granular. Sample charters for Risk Committee and Risk Subcommittee are included in the Appendix 3.1 and Appendix 3.2, respectively.

4.3.1 Executive Team Level

On the executive team, Tesla's CEO shapes the risk environment and is the main factor in setting Tesla's risk appetite. The CFO handles fiscally related risk matters, using metrics and strategizing to align Tesla's financials with the overall organizational goals. The CLO directs both legal and compliance risk management, ensuring Tesla does not run afoul of laws or governmental regulations. Finally, independent board members assist in providing oversight to Tesla's operations, functioning as both a balance and a guide to the executives and their decisions.

4.3.2 Risk Committee Level

Within the risk committee, the CRO takes directives from the executive tier and oversees Tesla's overall risk management framework. They coordinate with each division to understand metrics and other data, assess risk exposure, and provide reports on the risk environment. The heads of each department, such

Automotive, Energy, and AI, are responsible for the identification and monitoring of their respective departments. This includes department-specific assets, operations, safety, and compliance-related matters, amongst their other responsibilities.

4.3.3 Departmental Risk Leaders and Operational Managers Level

Finally, the departmental risk leaders and operational managers in the risk subcommittee are tasked with directly coordinating and reporting to their respective departmental heads. The department-based risk leaders work to identify risks, direct the implementation of risk strategies and oversee departmental compliance with risk-related policies. The operational managers are responsible for day-to-day risk management practices, such as monitoring risk during operations and executing risk management routines, and reporting anything outside normal scope to the risk leader of their department.

5. Risk Appetite Statement

5.1 What Risk Appetite Statement Is

A Risk Appetite Statement (RAS) is a formal document that defines the amount and types of risk an organization is willing to accept in pursuit of its objectives (Tucker 2020). Seven key assumptions are established first to set the tone and focus of the RAS at Tesla. These assumptions are essential to ensure that the RAS is comprehensive, relevant, and aligned with Tesla's strategic priorities. The seven key areas identified for consideration are:

1. Technology
2. Operation
3. Finance
4. Regulatory
5. Cybersecurity
6. Publicity
7. Safety

First of all, innovation requires risk-taking (Giaccone & Magnusson, 2021). As the pioneer in the automotive industry, it is assumed that higher technological risks are accepted by Tesla compared with most traditional vehicle manufacturers. So, a higher tolerance for developmental risks is acknowledged. Second, 'operational efficiency' refers to an organization's capability to perform tasks swiftly and efficiently (Team Mediaocean, 2022). To maintain competitiveness in the marketplace, Tesla needs to maximise its operational efficiency and therefore operational risk must be minimised as a critical factor for Tesla. Third, Tesla has been investing heavily in emerging markets (Zhu, 2020) and must accept the possibility of slow returns as the financial risk since the long-term financial gains outweigh the risks. Therefore, acceptable ranges of deviation from the expected financial outcome are established to account for the inherent uncertainties associated with investment activities. Fourth, as an enterprise spanning globally in various industries such as AI, autonomous driving and battery innovations (Tesla Inc., 2025), Tesla's regulatory risk is high and requires flexible and agile risk posture adjustments in multiple regulatory environments. Fifth, while Tesla is well known for producing cutting-edge self-driving electric vehicles, its innovative use of data collection and application has played a significant role in making it

arguably the most valuable car company in the world (dwang, 2023). In other words, Tesla's dependence on software-driven products such as Autopilot, FSD, energy platforms necessitates extremely low cybersecurity risk tolerance. For the publicity risk, as a high-profile public company, Tesla's stakeholders expect a transparent and disciplined approach to risk management. As a result, stringent reputational safeguards are required for Tesla. Finally, Tesla should consider the safety of its employees and customers to minimize harm to both groups.

The development of Tesla's RAS will be based on the aforementioned seven key risk consideration categories to ensure that the RAS is aligned with Tesla's strategic direction. Stakeholders across Tesla, including executive leadership, business unit managers, engineers, financial officers, legal counsel, and cybersecurity experts, will be engaged annually in September through structured workshops and individualized interviews organised by the Enterprise Risk Management (ERM) Committee. The annual updating cadence of the RAS is in line with the annual financial reporting requirements for Tesla as a public company.

It starts with the reviewing of Tesla's mission statement, which is Tesla's core strategic objective. Tesla's RAS needs to reflect Tesla's emphasis on achieving innovation and technological leadership in the industry; therefore, it must support the assumption that technological risk at Tesla will be inherently high but can still be accepted. Next, a comprehensive assessment of Tesla's internal and external environment will be conducted. This is a reality check to understand Tesla's current operational efficiency, most recent market trends, regulatory landscapes and the dynamics of the global emerging market. Informed by the contextual reviews, Tesla will adjust any existing assumptions about operational efficiency requirements, the financial risks associated with its investment and regulatory compliance to align with environmental realities. For cybersecurity risk, near-zero tolerance for breaches will be strictly enforced at all times, without exception, due to the increased number of cyberattacks around the world (Black Hat Ethical Hacking, 2025). The insights of stakeholders involved in this process will help define realistic and

actionable risk appetite levels in line with the assumption regarding public expectations for transparency and discipline when it comes to managing risks.

A draft of the RAS will be prepared by the ERM Committee with findings from the workshops and interviews. There will be an internal consultation process for the draft afterwards, where feedback is solicited from the stakeholders, and necessary adjustments will be made to balance ambition with practicality to further ground the RAS in Tesla's operational reality. Upon the completion of internal consultation, the RAS will be finalized and endorsed by Tesla's ERM Committee and subsequently presented to the Board of Directors for formal approval, which signifies that the RAS is an authoritative policy for risk-based decision-making across all levels of Tesla. This approved version of the RAS will be integrated into Tesla's corporate governance framework alongside any existing risk escalation protocols, with the goal of aligning these protocols to represent risk response as presented in the RAS. These steps ensure that the risk appetite is monitored, enforced, and adapted through a formal governance process.

5.2 Why Risk Appetite Statement Is Required

It is recognised that risk is inevitable and not all risk can be eliminated. Tesla's Risk Appetite Statement (RAS) establishes clear guidelines to ensure that all strategic, operational and functional decisions support achieving its mission to 'accelerate the world's transition to sustainable energy' (Tesla Inc., 2025). It directs asset-related decisions such as how much risk to tolerate and informs risk analysis thresholds.

5.3 How to Apply Risk Appetite Statement

To apply Risk Appetite Statement, it starts with reviewing the assumptions for the key areas. The table in Appendix 4.1 captures information for each of the seven identified categories with some real-world scenarios (Appendix 4.2) and indicates who should be concerned with the levels of risk. This serves as an example, and may not align with reality after the appropriate stakeholders have been consulted. Consequently, the assumptions made for each category due to these interviews not yet being conducted are notated below. The categories in this table are not ranked in any particular order due to missing information from appropriate stakeholders, but it is recommended to order them in priority order once all possible information has been obtained, considered, and consolidated. Then, the likelihood of Risk Realization needs to be assessed as demonstrated in the table in Appendix 4.3. It provides a designation of the level of attention that should be given to a risk, based on the likelihood that it occurs. If a risk is on the boundary of a range, it should be assessed on an individual basis to determine which level of attention it should receive. Once the category rankings for the previous table have been determined, it may be useful to assist in that designation based on the priority level of the risk.

Another aspect of risk that may be beneficial to consider is the controllability. With this, for each risk consider the number of response options available and the resource demand required to address the risk. Risks that have fewer response options or require the most resources are considered to be less controllable and should be addressed by the executive levels, while cheaper risks could be addressed by the front line (Tucker, Advancing Risk Management Capability Using the OCTAVE FORTE Process, 2020).

A heat risk map can also be useful in indicating prioritization for risks quickly. This heat map in Appendix 4.4 serves as an example of a variety of risks and takes into consideration assumptions made without full information on response capabilities, true likelihood of a risk, true impact of a risk, or true

concerns of the company. For proper usage of a heat map to determine prioritization, these factors should be investigated and considered.

6. Other Considerations

Acceptable Response Plans (ARP) are predefined actions to address a risk when it occurs. For Tesla, each risk identified through the Risk Analysis Process must include an acceptable response plan with available options including avoiding the risk, mitigating the risk through safeguards, transferring the risk by insurance or accepting the risk in accordance with Tesla's Risk Appetite Statement. (Tucker, 2025, Module 3_Asset Management_Tucker_Spring_2024). Frequent review for the ARP must be undertaken to ensure its relevance. For example, if a supply chain disruption occurs in Tesla, the ARP should include options to find an alternative supplier to avoid the risk or stockpiling critical materials to mitigate the risk.

Risk Ownership refers to assigning responsibility for managing risks to individuals or the team within the organization. A risk owner will then be responsible for monitoring and reassessing the risk to implement mitigation strategies to respond based on the ARP (Williams, 2021). For example at Tesla, a plant operations manager is likely to be the risk owner of production-related risks and the Chief Information Security Officer may own data breach risks. Having clarified risk ownership can help ensure continuous improvement of controls across the organization.

When it comes to the alignment with Tesla's corporate strategy, all the policies and procedures discussed above are directly or indirectly tied to Tesla's overarching mission that is to "accelerate the world's transition to sustainable energy." (Tesla Inc., 2025) Incorporating ARP, assigning clear risk ownership, and aligning risk management with Tesla's corporate strategy ensures that risk oversight is not treated in isolation but is embedded within the company's corporate strategic framework.

7. Conclusion

The integrated approach discussed in this document transforms risk management at Tesla into a dynamic, continuous process that reconciles with its objectives and external environment. Each policy component: Asset Management, Risk Analysis, Risk Governance, and Risk Appetite builds upon the others in a cohesive manner to have a comprehensive system for identifying, assessing, mitigating, and monitoring risks. This structure enhances Tesla's ability to safeguard its assets, foster innovation, and maintain operational resilience, which establishes a robust governance framework that supports sustainable growth and the long-term achievement of Tesla's mission.

Appendices

Appendix 1: Use Case: Autopilot/Self-driving System

Appendix 1 contains a set of 8 tables to be used as part of the asset management process. Each table includes a note to describe its purpose and indicate its corresponding step.

Table 1: Service Profile

As part of step one, planning for asset management, the service profile assists with identification of responsibility, prioritization, and a service's related assets.

Service Name	Category	Dependencies	Ownership	Prioritize
Recruiting qualified personals for the autopilot system	Human capitals	Skills and experiences in AI and edge computing	Human Resources Department	High as talented engineers are rare and highly sought after
Writing and development of code supporting the autopilot system	Code development	Autopilot code, coding libraries	Code engineers	High, necessary for functionality of autopilot system

Supercharger Network	Infrastructure service	Power grid & renewable energy sources, Internet & cloud connectivity for monitoring and payment processing	Infrastructure & Energy Division	High, Supercharger availability directly affects customer satisfaction, Tesla's competitive advantage, and revenue generation
FSD Computer Chip	SoC development & implementation	Manufacturing, the supporting autopilot code, Tesla Vision cameras	SoC Engineering team	High, implemented within each Tesla to handle autopilot and related systems
Autopilot Neural Network Model Training	AI/ML development	NVIDIA H100 AI Chips	Tesla's Global Supply Chain Management Team	High, Core service for the use case of Autopilot / FSD

(Tucker, 2025, *Module 2_Asset Management_Tucker_Spring_2024,* p. 22)

Table 2: Asset Profile

For step 2, identifying assets, an asset profile should be constructed for each asset to give an idea of key information for each asset.

Asset	Organizational Risks if Jeopardized	Unique Features & Characteristics	Our Subject Matter Experts
Supercharger Network	Revenue Loss: Tesla generates revenue from Supercharger usage, particularly for non-Tesla EVs that now have access to the network. Downtime or inefficiencies can impact profitability. (Supercharging Other EVs | Tesla Support, 2025)	Fast-Charging Capabilities: Tesla's Superchargers are among the fastest in the industry, allowing most vehicles to charge up to 80% in about 15–30 minutes. (*Supercharger | Tesla*, 2025)	Infrastructure & Energy Engineers: Specialists who design and maintain the Supercharger network, ensuring uptime and optimizing efficiency.

NVIDIA H100 Chips	This chip is used to train the deep neural networks used for Autopilot and self-driving capabilities. When jeopardized, this can lead to falsely trained models. These models can lead to accidents on the road.	The Tesla FSD chip is designed specifically for autonomous driving applications and has 6 billion transistors, 12 CPU cores, and 96 GPU cores. This is the most	ML engineers and lead who design and maintain the Machine learning process at Tesla making the Autopilot system more efficient.
Autopilot code	If the autopilot code is jeopardized, Tesla could face multiple errors impacting vehicles that use the code ranging from failure to start, to steering errors, to failure to recognize pedestrians. This poses a reputational, financial, and safety risk as such errors could lead to lower trust in the company, lower sales, and harm to the public.	The autopilot code could contribute to an array of features on a vehicle such as the acceleration, steering, brakes, and identification of lines on roads or street signs.	Code engineers and designers who design and maintain the autopilot code.

Engineers	As the most critical asset, if qualified people are not available, the development of the system will be jeopardized.	skills in AI and edge computing	Engineers with skills in AI and edge computing
FSD Computer Chip	If the FSD SoC fails, the car's Autopilot may malfunction or fail to function entirely. This risks damage to people or the environment, as well as the cost of repair or the inconvenience of missing functionality.	The SoCs included within each Tesla handle input from the Tesla Vision camera array and contains the autopilot code or program.	Engineers who are able to effectively design and implement the FSD Computer SoC designs.

(Tucker, 2025, *Cyber Risk Workbook,* p. 3)

Table 3: Prioritizing Assets

As part of step 2, identifying the assets, prioritizing assets within a sub-group assists with budget planning and risk management. This was approached with a qualitative risk based approach, based on criterias such as business impact, sustainability, risk exposure and dependency mapping.

Organization's Asset	**Asset Rank (1-5, with 1 most critical)**
Qualified engineers with experience in AI and edge computing	4
Autopilot code	2
FSD Computer Chip	3
Supercharger Network	5
NVIDIA H100 Chips	1

(Tucker, 2025, *Cyber Risk Workbook,* p. 5)

Assumptions made:

NVIDIA H100 Chips are ranked critically high as they are irreplaceable in developing and training Tesla's advanced AI models. A shortage or compromise would stall Autopilot development across all models.

Autopilot code was ranked the second because they are the critical part for the self driving cars and their exposure to cyber threats

FSD Computer chips were ranked third because they are physical chips which help in running the autopilot code, so this is related to but not above the autopilot code.

Qualifying engineers were ranked 4th as they post internal threats, but smart staff within different teams can be trained to be engineers who are qualified to get the job done.

The Supercharger Network, while important for customer experience, was assigned the least priority, as it is operationally distinct from Tesla's priority autonomy and AI pipelines.

Table 4: High Value Assets

As part of step 3, document assets, identifying high value assets that pose high risk to the company if compromised can assist with other aspects of the step. Information in this table may overlap with information in other tables.

Category	Asset(s)
People	Engineers with skills in AI and edge computing are the critical assets for autopilot/self driving systems
Information	The autopilot code is an information technology asset critical for the successful operation of the autopilot/self-driving system. The code also contributes to the safety of the system as bugs in the code could lead to errors that put people at risk.
Facilities	Supercharger Network, Gigafactory Nevada, Gigafactory Texas, Gigafactory Berlin, Gigafactory Shanghai, Fremont Factory, Gigafactory Berlin-Brandenburg (Tesla Inc 10-K, 2024)
Technology	The "Tesla Vision" set of cameras, as well as the FSD (Full Self-Driving) Computer system on a chip (SoC) within each vehicle, allows for Tesla's autopilot and other camera-reliant systems to function.
External	NVIDIA H100 Chips used by Tesla to train its neural networks on a large real-time dataset of real-world driving data collected from its fleet of vehicles.

(Tucker, 2025, *Cyber Risk Workbook,* p. 2)

Table 5: Critical Assets

This table is also part of step 3, document assets, and builds on the consequences to be considered for risk management of these assets.

Critical Info Asset	Why Important	Issues your organization will face if asset is compromised
Supercharger Network	Enables fast and reliable charging for Tesla and non-Tesla EVs, supporting customer convenience and Tesla's competitive advantage. It integrates with Tesla's cloud-based infrastructure, storing user data, payment info, and charging logs. (*Supercharger | Tesla*, 2025)	A breach could expose customer payment details, location history, and vehicle usage patterns, leading to regulatory penalties and legal consequences. Additionally, Charging delays or failures will frustrate users, harming Tesla's reputation and reducing customer loyalty.
NVIDIA H100 Chips	Nvidia's H100 chips are crucial for the deep learning neural networks which are used to train the ML model that is used for the FSD system in Tesla Cars based on real-time data coming from tesla's fleet of vehicles.	If the chips are compromised, this can corrupt the training model and thus the trained model can cause issues when in production - ie, the self driving cars can end up meeting with accidents due to poor decision making. This can affect Tesla's brand which is built on innovation and security. This can even lead to lawsuits, reputational damage, operational costs, etc.

Autopilot code	This asset is important for the functionality of the autopilot system. Without it, the self-driving system would not know how to operate.	If the autopilot code is compromised, Tesla could face the threat of hostile actors seeking to change the functionality of the code by creating bugs or deleting critical aspects of the code.
FSD Computer Chip	This asset allows for the actual execution of the autopilot system. Cameras are connected to the car's SoCs, which acts on their input.	If the SoCs included within a Tesla fails, or are faulty prior to customer operation, Autopilot would not be able to properly function. While two are included within each car in the event of failure, damaged or malfunctioning chips could lead to crashes, harming customers. Even if crashes do not occur, limited or impeded functionality, as well as costly repairs, would frustrate customers, damaging reputation or similar.
Experienced engineers with expertise in AI and edge computing	People are strategic assets as they enable Tesla to create safe and intelligent self-driving systems.	Without People, Tesla's vision of fully autonomous and reliable vehicles would not be achieved.

(Tucker, 2025, *Cyber Risk Workbook,* p. 4)

Table 6: Asset Security

This table is part of step 3, asset documentation, and focuses on security requirements for High Value Assets. Identify which security element is most important.

	Confidentiality	Integrity	Availability
Supercharger Network	Protects user data, including payment information, location tracking, and charging history, from unauthorized access or breaches.	Ensures that charging session data, billing records, and software updates remain accurate and unaltered to prevent fraud or operational issues.	This is the most important element. Guarantees that charging stations are operational and accessible when needed, preventing downtime that could disrupt customer experience and Tesla's revenue.
NVIDIA H100 Chips	While these chips themselves don't store data, their configuration and usage must be restricted to authorized personnel only.	Authentic H100 chips are required for training the FSD / Autopilot system to its full potential. A compromised chip can alter how these models function.	This asset guarantees that the Autopilot / FSD system in tesla cars work efficiently. The shortage of these chips or the lack of proper integration can cause production delays which can affect the availability of autopilot services.
Autopilot code	The confidentiality of this asset protects Tesla's proprietary information.	Ensures proper functionality and limits to risk of features of the autopilot driving posing a safety risk due to the code receiving unauthorized edits.	The availability of this asset enables the autopilot system to function.

Engineers with skills in AI and edge computing	The personal information about the employees must be kept confidential as per employment contracts	They are experts and respected leaders in the industry to produce world-class autopilot products.	They should be available during the working hours as stipulated in the employment contracts.
FSD Computer Chip	The FSD Computer chip requires confidentiality to protect a key component of Tesla's competitiveness in the market	The SoC must remain fully operational, otherwise autopilot may malfunction and present a risk to the driver.	If the SoC fails, autopilot and "smart" or safety related features would not be able to function.

(Tucker, 2025, *Cyber Risk Workbook,* p. 6)

Table 7: Asset Documentation

Asset documentation is part of step 3, documenting assets, and ensures that there is a consistent understanding of what an asset is and who is responsible for it.

Name	Description	Importance	Owner & Custodian
Supercharger Network	A global network of fast-charging stations designed for Tesla and, in some locations, non-Tesla electric vehicles. It enables rapid battery charging and integrates with Tesla's vehicle software for real-time monitoring and payment processing. Superchargers are located at Tesla-owned sites, commercial properties, apartment buildings, shopping centers, and highway rest stops through partnerships or leases. (Supercharger | Tesla, 2025)	Essential for customer convenience, brand reputation, and revenue generation. Ensures Tesla vehicles remain a practical choice for long-distance travel. Supports sustainability initiatives by incorporating renewable energy sources where possible.	Owner: Tesla, Inc. (Infrastructure & Energy Division) Site Owners: Commercial property owners, apartment complexes, retail centers, highway service operators Custodian: Tesla Operations & Maintenance Teams, Tesla Software & Network Security Teams, Site Hosts (responsible for local site maintenance in some cases)
NVIDIA H100 Chips	The H100 GPU chip, developed by NVIDIA, stands out as a powerhouse in AI hardware. The H100 is the most powerful	Nvidia's H100 chips are crucial for Tesla's Full Self-Driving (FSD) development because they provide the	Owner : Tesla Supply Chain Operations Lead / Team Third Party Provider : Nvidia

	GPU chip on the market and is designed for artificial intelligence (AI) applications. (Infinitalab| Medium, 2024)	massive computational power needed to train and process the vast amounts of video data used in FSD AI models.	Custodians: ML Engineering Lead and ML engineers
Autopilot code	The autopilot code is Tesla's proprietary code used for the self-driving system that enables the use of autopilot for their enabled vehicles.	This code is important to the functionality of the self driving system because it provides the instructions and guidelines for the system.	Owner: Tesla Inc. Custodian: lead autopilot code developer
FSD Computer Chip	The SoC within each Tesla vehicle that connects to the Tesla Vision camera arrays. It enables autopilot and related "smart" or safety features.	Without this SoC, autopilot would not be able to exist. The cameras would not have their input utilized.	Owner: Tesla Inc. Custodian: Head of SoC development team
Engineers with skills in AI and edge computing	Tesla documents the involvement of the engineers in the development of the system and their performance reviews	Critical as people is the critical asset that drives the development of the system	Owner: Human resources department

(Tucker, 2025, *Cyber Risk Workbook,* p. 7)

Table 8: Asset Profile Catalog

The asset profile catalog is used as part of step 4: manage assets. Other tables may be edited during this step if necessary. This catalog provides a concise way to track important asset information. The columns loss of revenue, additional expenses, regulatory and legal, customer service, and goodwill refer to asset value and should be a monetary value. As the writers of this policy are not privy to budget information, we have not completed those sections, but the information should be gathered by the risk management program when this catalog is used.

ID	Name	Services Supported	Type (PIFTE)	Location	Owner	Custodian	Format	Security Classification	Backup Location	Loss of Revenue	Additional Expenses	Regulatory and Legal	Customer Service	Goodwill
1	Engineers with experience in AI and edge computing	System design and architecture, data engineering, software development and performance monitoring	P	Tesla offices	Tesla	HR Department	Work on-site	Integrity	Alternative workplaces such as their home offices	-	-	-	-	-

2	FSD Computer Chip	Physical hardware for autopilot, system architecture	T	Within the car itself	Tesla	Head of SoC development team	Physical	Integrity	Within each Tesla (two SoCs are included for failover)	-	-	-	-	-
3	Auto-pilot code	Autopilot system	I	Cloud storage	Lead code developer	Lead autopilot code developer	electronic	confidential	Secondary digital storage	-	-	-	-	-
4.	NVIDIA H100 Chips	ML model for autopilot training	E	On Prem facilities	Supply Chain Ops Lead	ML Engineering Lead and ML engineers	Physical	Availability	Supply chain storage	-	-	-	-	-
5	Supercharger Network	EV fast-charging services	F	Tesla-owned stations,	Infrastructure &	Site Hosts	Physical & Digital	Availability	Other locations with	-	-	-	-	-

				shopping centers, apartment building s, highway stops	Energy Division				supercharge rs					

(Tucker, 2025, *Cyber Risk Workbook)*

Appendix 2.A - Information Asset Example

Appendix 2.A contains 10 worksheets and 3 questionnaires to be completed for the risk analysis project and demonstrates their use with an information asset: the Autopilot Code. Each table corresponds to a step described in section 3, and includes a note for its purpose and corresponding step.

Allegro Worksheet A.1: Risk Measurement Criteria - Reputation and Customer Confidence

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of reputation and customer confidence. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 1			
Impact Area	**Risk Measurement Criteria – Reputation and Customer Confidence**		
	Low	**Moderate**	**High**
Reputation	Reputation is minimally affected if the code is buggy and does not pose a major threat to the functions; little or no effort or expense is required to recover.	Reputation is damaged if the autopilot code is leaked, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged if the autopilot code is compromised.

Customer Loss	Less than 5% reduction in customers due to loss of confidence	5 to 25% reduction in customers due to loss of confidence	More than 25% reduction in customers due to loss of confidence
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.2: Risk Measurement Criteria - Financial

This worksheet is used in the OCTAVE Allegro to assess impact severity in a financial context. The data was provided via assumptions, and will be affirmed or updated based on future survey results. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 2			
Impact Area	**Risk Measurement Criteria – Financial**		
	Low	**Moderate**	**High**
Operating Costs	Increase of less than 10% in yearly operating costs	Yearly operating costs increase by 10% to 30%.	Yearly operating costs increase by more than 30%.

Revenue Loss	Less than 1% yearly revenue loss	2 to 3% yearly revenue loss	Greater than 3% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $ 3bn	One-time financial cost of $ 3bn to $ 10bn	One-time financial cost greater than $ 10bn
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.3: Risk Measurement Criteria - Productivity

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of productivity. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 3			
Impact Area	**Risk Measurement Criteria – Productivity**		
	Low	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 10% for 1 to 2 day(s).	Staff work hours are increased between 10% and 20% for 2 to 3 day(s).	Staff work hours are increased by greater than 20% for 3 to 5 day(s).

Other: *Automation Time*	Increase in the time saved by automation due to the compromise in autopilot code by less than 10%	Increase in the time saved by automation due to the compromise in autopilot code by 10% to 30%	Increase in the time saved by automation due to the compromise in autopilot code by greater than 30%
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.4: Risk Measurement Criteria - Safety and Health

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of safety and health. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 4			
Impact Area	**Risk Measurement Criteria – Safety and Health**		
	Low	**Moderate**	**High**
Life	No loss or significant threat to customers' lives due to the autopilot code being compromised	Customers' lives are threatened due to accidents, but they will recover after receiving medical treatment.	Loss of customers' lives, leading to lawsuits and compensations

Health	Minimal, immediately treatable degradation in customers' health with recovery within four days	Temporary or recoverable impairment of customers' physical and mental health	Permanent impairment of significant aspects of customers' health in terms of mental stress and physical accidents
Safety	Safety questioned - Erratic and buggy performance of the autopilot code	Safety affected - Minor accidents due to the autopilot code	Safety violated - Major crashes and accidents leading to loss of life due to the code quality.
Other: *Cyber Security*	Low priority and severity CVEs and Bugs found in the code.	Medium severity bugs and CVEs found in the code.	High priority and severity bugs and CVEs found in the code which can be actively exploited endangering customer lives

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.5: Risk Measurement Criteria - Fines and Legal Penalties

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of fines and legal penalties. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 5			
Impact Area	**Risk Measurement Criteria – Fines and Legal Penalties**		
	Low	**Moderate**	**High**
Fines	Fines less than $100,000 are levied.	Fines between $100,000 and $200,000 are levied.	Fines greater than $200,000 are levied.

Lawsuits	Non-frivolous lawsuit or lawsuits less than $200,000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $200,000 and $10,000,000 are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $10,000,000 are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organizations request information or records (low-profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices and customer records
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.6: Risk Measurement Criteria - User Defined

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of user defined areas. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 6			
Impact Area	**Risk Measurement Criteria – User Defined**		
	Low	**Moderate**	**High**
AI Ethics & Algorithmic Bias	Minor inconsistencies in biases due to missing or improper implementation of ethical restrictions	Noticeable difference in performance in different demographics	Legal complaints and loss of public trust

Innovation Roadmap Disruption	Slight delay in model update; no impact to product launches.	Quarter-level delay in a major capability	Delay jeopardizes Tesla's competitive position against Waymo, Cruise, etc. in autonomy race.

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.7: Impact Area Prioritization Worksheet

This worksheet is used in OCTAVE Allegro to rank impact areas based on their importance to the organization. Each of the priorities must have one allocated sequence. The priority determinations are first allocated via assumptions, then later affirmed or modified by the results of internal surveys. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 7	Impact Area Prioritization Worksheet
Priority	**Impact Areas**
4	**Reputation and Customer Confidence**
5	**Financial**
1	**Productivity**
6	**Safety and Health**
2	**Fines and Legal Penalties**

3	**User Defined**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.8: OCTAVE Allegro Critical Asset Profile

This worksheet is designed to build a detailed profile of critical information assets within an organization. It helps identify an asset's value, ownership, and the security requirements: Confidentity, Integrity and Availability (CIA).

This worksheet corresponds with the 2nd step of the OCTAVE Allegro process: Develop an Asset Profile.

Worksheet 8	OCTAVE® ALLEGRO Critical Asset Profile	
(1) Critical Asset *What is the critical asset?*	**(2) Rationale for Selection** *Why is this asset important?*	**(3) Description** *What is the agreed-upon description of this asset?*
Autopilot Code	The FSD system developed by Tesla runs on the autopilot code. This code is thus important for maintaining the safety of self driving cars and is the backbone of innovation for Tesla.	The autopilot code is Tesla's proprietary code used for the self-driving system that enables the use of autopilot for their enabled vehicles.
(4) Owner(s) *Who owns this information asset?*		

Director of FSD Technology - Autopilot Software		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	Only authorized personnel can view this asset, as follows:	Developers, team leaders and Directors should have access to the autopilot code. Other teams and members who depend on the autopilot code can have view access to the code.
Integrity	Only authorized personnel can modify this asset, as follows:	Only Developers, QA and Team leaders should have edit access to the autopilot code
Availability	This asset must be available for these personnel to do their jobs, as follows:	All the teams and members who are dependent on the autopilot code should have access to the code.

	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	This asset must be available for 24 hours, 5 days/week, all year until the dependency is met. This must be set depending on the usage and the teams.
Other	This asset has special regulatory compliance aaaaaaa protection requirements, as follows:	Since this is a proprietary asset for Tesla this must not be shared outside permitted systems.

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

Confidentiality	Integrity	Availability	Other
	X		

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.9a: Asset Risk Environment Map (Technical)

This worksheet is used to identify and document the technical environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9a	ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Tesla's internal development environment or build pipeline (CI/CD) — e.g., Jenkins, Bazel	**FSD Dev Team (Internal)**
2. Autopilot integration testing or simulation pipeline using internal GPU clusters	**FSD QA Team (Internal)**

3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. External Code Library and Cloud Storage This includes the cloud repository where the autopilot code will be stored and accessed by the Dev team and the customers (if the code is open sourced)	Github (External)

2. External Deployment Containers These are the containers that hold the code while it is being deployed to different environments.	Deployment service used by tesla (External)
3. NVIDIA's cloud-hosted test lab for benchmarking H100 performance	Nvidia (External)
4. Application security testing tools that are used to test the security vulnerabilities in the code	Sonarqube (External)

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.9b: Asset Risk Environment Map (Physical)

This worksheet is used to identify and document the physical environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9b	ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Tesla's facilities and servers Tesla's Palo Alto HQ, AI labs, or secured sections of Gigafactory Nevada where source code is accessed or servers are housed.	Director of Infrastructure
2. Tesla-issued secure laptops or workstations used by authorized engineers for code development.	Head of the FSD Department

3. Tesla's internal storage systems: Internal SSDs or backup storage systems storing code snapshots or ML model weights related to Autopilot.	Head of the FSD Department
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. External Cloud storage containers These are the physical storage containers that are owned by external provides such as github, which are used to store the autopilot code in the cloud. These can be data centers owned by github.	Github (External)

2. Third party storage vendors These are the vendors hired by tesla for 3rd party storage used for disaster recovery of code repositories.	AWS (External)
3.	
4.	

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.9c: Asset Risk Environment Map (People)

This worksheet is used to identify and document the people's environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9c	ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1. Software developers These are the members of the development team responsible for writing the autopilot code.	FSD Dev Team
2. Testers & Security Engineers They are responsible for testing out the code that is written to ensure that all the functionalities are working as expected and that the code is free from any vulnerabilities	FSD SecOps and QA Team

3. Product Owners and Tech leads Those who are responsible to oversee the development of the FSD system.	Team of Product owners
4. ML engineers Handle build, testing, and deployment processes tied to the Machine Learning Model that feeds from the autopilot code.	ML Egineering team
External Personnel	
Contractor, Vendor, Etc.	**Organization**
1. Contracted Developers Third-party contributors or consultants who may temporarily access or review parts of the Autopilot Code.	Consulting organizations Eg: Deloitte

2. External Auditors / Pen Testers May review parts of the system for compliance or vulnerability testing.	External Testers eg: PwC

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet A.10: Asset Risk Worksheet

This worksheet is used to document and analyse risks associated with a critical asset. Information gathered in the previous worksheets are summarised here to help define the Threat Scenarios and their Impact and finally the risk scores. As a comprehensive worksheet, it covers step 4 to 8 of the OCTAVE Allegro process: Identify Areas of Concern, Identify Threat Scenarios,Identify Risks,Analyze Risk and Select Response Approach. The final Risk score is utilized as a comparison point with other scores to help prioritize risks and can vary from asset to asset based on the nature of the risks presented.

		OCTAVE® ALLEGRO Asset Risk Worksheet	
Asset Risk	**Threat**	**Asset**	Tesla's Autopilot Code
		Area of Concern	*Compromise of code integrity*
		(1) Actor *Who would exploit the area of concern or threat?*	Malicious hackers, Software engineers and security analysts

		(2) Means *How would the actor do it? What would they do?*	Compromising the code by exploiting the Common vulnerabilities (CVEs) or through phishing attacks and lateral movement once the code and networks are compromised
		(3) Motive *What is the actor's reason for doing it?*	Rogue threat actors, competitors, threat groups acting against Elon Musk due to his political stand
		(4) Outcome *What would be the resulting effect on the information asset?*	Disclosure Destruction Modification X Interruption X
		(5) Security Requirements *How would the information asset's security requirements be breached?*	The information asset's security requirement of Integrity will be breached if the malicious threat actors are able to change the autopilot code in the remote repository in such a way that can be used to cause accidents and loss of life.

		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High** X	**Medium**	**Low**

(7) Consequences *What are the consequences on the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Under the scenario where a threat actor maliciously gains access to the autopilot code, a lot of customers can be impacted. If the actor's intention is to cause harm on a large scale this can be easily taken care of with a single deployment of maliciously changed code to the production environment.	**Reputation & Customer Confidence**	**Moderate (2)**	**4**
	Financial	**Low (1)**	**5**
This can make the vehicles more accident prone which can lead to the death of customers among massive loss of trust in Tesla's software integrity and safety, negative press, social media backlash etc.	**Productivity**	**High (1)**	**1**
	Safety & Health	**High (1)**	**6**

		Fines & Legal Penalties	Moderate (2)	3
		User Defined Impact Area	Moderate (2)	2
Risk Score				**30**

(9) Risk Response			
Based on the total score for this risk, what action will you take?			
Accept	**Defer**	**Mitigate**	**Transfer**
		X	
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		

Code	This would be done by improving the access controls to limit the number of users that have access to the code base. This can be done by setting up RBAC (Role based access controls) and with the implementation of MFA. It can also involve regular code reviews and CVE monitoring and patching.
Supply Chain Security controls	This can help Tesla reduce the information leaks from code mishandling by third party vendors.
Personnel Training	Providing people with cyber awareness training to practice cyber hygiene such as not falling for phishing emails, etc, so that they can be more aware to prevent any losses due to human errors.
Technical Controls	Other technical controls like Least Privileged access, Network Segmentation, implementation EDR and SIEM tools can be used to reduce the likelihood of a breach
Physical controls	Improved badging to prevent piggybacking can help to reduce the impact and likelihood of an attack.

(OCTAVE Allegro Student Workbook v1.0, 2012)

Threat Scenario Questionnaire A.1: Technical Containers

This Questionnaire is used to assist in identifying potential threats that could arise due to the location of the technical asset. The process considers threats both within and external to the organization, and is used for each asset identified by Worksheet 9a. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. Underlining indicates selected answers. (We answered this to the best of our abilities using assumptions.)

[redacted]	**Technical Containers**
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. **Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.**	
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee could access one or more technical containers, *accidentally or intentionally*, causing your information asset to be:	

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?		**Yes (accidentally)**	**Yes (intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally or intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

(OCTAVE Allegro Student Workbook v1.0, 2012, p 52)

[redacted]	**Technical Containers**

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine if any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

Unintended disclosure to your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan Horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Other third-party problems or systems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Threat Scenario Questionnaire A.2: Physical Containers

This Questionnaire is used to assist in identifying potential threats that could arise due to the physical location of the asset. The process considers threats both within and external to the organization, and is used for each asset identified by Worksheet 9b. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. Underlining indicates selected answers in this example. (We answered this to the best of our abilities using assumptions.)

	Physical Containers
This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. **Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.**	
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee could access one or more physical containers, *accidentally or intentionally*, causing your asset to be:	

Disclosed to unauthorized individuals?	**No**	**Yes accidentally)**	**Yes intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes accidentally)**	**Yes intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes accidentally)**	**Yes intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more physical containers, *accidentally or intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes accidentally)**	**Yes intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes accidentally)**	**Yes intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes accidentally)**	**Yes intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes accidentally)**	**Yes intentionally)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

	Physical Containers

Scenario 3:

In this scenario, consider situations that could affect your physical containers, and by default, affect your information asset. Determine if any of the following could occur, and if yes, determine whether these situations would cause one or more of following outcomes:

Unintended disclosure to your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Threat Scenario Questionnaire A.3: People

This Questionnaire is used to assist in identifying potential threats that could arise due to individuals both within and external to the organization, and is used for each asset identified by Worksheet 9c. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. Underlining indicates selected answers in this example. (We answered this to the best of our abilities using assumptions.)

[redacted]	**People**
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.	
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee has detailed knowledge of your information asset and could, *accidentally or intentionally*, cause the information asset to be:	

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could, *accidentally or intentionally*, cause your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Appendix 2.B: Non-Information Asset Example

Appendix 2.B contains 10 worksheets and 3 questionnaires to be completed for the risk analysis project and demonstrates their use with an non-information asset: the Supercharger Network. Each table corresponds to a step described in section 3, and includes a note for its purpose and corresponding step.

Allegro Worksheet B.1 Risk Measurement Criteria - Reputation and Customer Confidence

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of reputation and customer confidence. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 1			
Impact Area	**Risk Measurement Criteria – Reputation and Customer Confidence**		
	Low	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.

Customer Loss	Less than 5% reduction in customers due to loss of confidence	6 to 25% reduction in customers due to loss of confidence	More than 25% reduction in customers due to loss of confidence
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.2 Risk Measurement Criteria - Financial

This worksheet is used in the OCTAVE Allegro to assess impact severity in a financial context. The data was provided via assumptions, and will be affirmed or updated based on future survey results. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 2			
Impact Area	**Risk Measurement Criteria – Financial**		
	Low	**Moderate**	**High**
Operating Costs	Increase of less than 2% in yearly operating costs	Yearly operating costs increase by 1 to 3%.	Yearly operating costs increase by more than 4%.

Revenue Loss	Less than 1% yearly revenue loss	1% to 3% yearly revenue loss	Greater than 3% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $5,000,000	One-time financial cost of $6,000,000 to $20,000,000	One-time financial cost greater than $21,000,000
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.3: Risk Measurement Criteria - Productivity

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of productivity. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 3			
Impact Area	**Risk Measurement Criteria – Productivity**		
	Low	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 5% for 1 to 2 day(s).	Staff work hours are increased between 6% and 10% for 2 to 3 day(s).	Staff work hours are increased by greater than 10% for 3 to 5 day(s).

Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.4: Risk Measurement Criteria - Safety and Health

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of safety and health. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 4			
Impact Area	**Risk Measurement Criteria – Safety and Health**		
	Low	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives

Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.5: Risk Measurement Criteria - Fines and Legal Penalties

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of fines and legal penalties. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 5			
Impact Area	**Risk Measurement Criteria – Fines and Legal Penalties**		
	Low	**Moderate**	**High**
Fines	Fines less than $100,000 are levied.	Fines between $100,000 and $200,000 are levied.	Fines greater than $200,000 are levied.

Lawsuits	Non-frivolous lawsuit or lawsuits less than $2,000,000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $2,000,000 and $10,000,000 are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $10,000,000 are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low-profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Other:			

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.6: Risk Measurement Criteria - User Defined

This worksheet is used in the OCTAVE Allegro to assess impact severity in the context of user defined areas. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 6			
Impact Area	**Risk Measurement Criteria – User Defined**		
	Low	**Moderate**	**High**
Cybersecurity	Embedded software is current and well-maintained; cybersecurity measures are robust and routinely updated to protect against vulnerabilities.	Software updates and patch management occur on a scheduled basis; some vulnerabilities are identified but remain manageable with moderate risk.	Legacy or outdated software increases cyber vulnerabilities; significant security gaps jeopardize system integrity and lead to

			potential operational breaches.
Hardware Durability & Reliability	Charging stations and physical components consistently perform with robust durability; very few failures occur.	Occasional hardware degradation or isolated component issues that require routine maintenance; brief service interruptions may occur.	Frequent hardware failures or accelerated wear lead to significant downtime and costly, extensive repairs.

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.7: Impact Area Prioritization Worksheet

This worksheet is used in OCTAVE Allegro to rank impact areas based on their importance to the organization. Each of the priorities must have one allocated sequence. The priority determinations are first allocated via assumptions, then later affirmed or modified by the results of internal surveys. This is one of the seven Worksheets to be completed for the step 1 of the process: Establish Risk Measurement Criteria.

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
1	**Reputation and Customer Confidence**
3	**Financial**
2	**Productivity**
4	**Safety and Health**
5	**Fines and Legal Penalties**

6	**User Defined**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.8: OCTAVE Allegro Critical Asset Profile

This worksheet is designed to build a detailed profile of critical information assets within an organization. It helps identify an asset's value, ownership, and the security requirements: Confidentity, Integrity and Availability (CIA).

This worksheet corresponds with the 2nd step of the OCTAVE Allegro process: Develop an Asset Profile.

Worksheet 8	**OCTAVE® ALLEGRO Critical Asset Profile**	
(1) Critical Asset *What is the critical asset?*	**(2) Rationale for Selection** *Why is this asset important?*	**(3) Description** *What is the agreed-upon description of this asset?*
Supercharger Network	The network is central to Tesla's business model, ensuring customer satisfaction, supporting vehicle sales, and reinforcing their brand leadership in the EV market.	A globally distributed network of high-speed charging stations comprising physical charging units, electrical infrastructure, embedded control systems, and real-time monitoring components.
(4) Owner(s)		

Who owns this information asset?		
Operations/Infrastructure and Energy divisions		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	Only authorized personnel can view this asset, as follows:	Network engineers, operations managers, maintenance supervisors, and select vendor partners have view access to system configurations, performance metrics, and maintenance records. Other teams (e.g., customer support and strategic planning) would receive summarized or non-sensitive information.
Integrity	Only authorized personnel can modify this asset, as follows:	This is limited to operations and IT/engineering teams, including field technicians, system administrators, and

		designated change-control managers who are responsible for updating software, firmware, and physical configurations.
Availability	This asset must be available for these personnel to do their jobs, as follows:	All teams relying on real-time data including operations, maintenance, and emergency response should have access.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	This asset must be available for 24 hours, 5 days/week, ensuring that service levels meet customer expectations and support dependency requirements.
Other	The supercharger network is a critical and proprietary asset for Tesla, subject to strict regulatory, safety, and environmental standards.	Detailed design, operational data, and system integration information must not be shared outside of approved systems and designated external partners.
(6) Most Important Security Requirement		

What is the most important security requirement for this information asset?			
Confidentiality	Integrity	Availability **X**	Other

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.9a: Asset Risk Environment Map (Technical)

This worksheet is used to identify and document the technical environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9a	ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Charging station control units to manage power delivery, monitor usage and communicate with Tesla network	Infrastructure team
	Operations Team
2. Data usage and billing system to analyse customer usage and charging customers	Date team
	Finance Team

4.	
5.	
External	
Container Description	**Owner(s)**
1. External service providers	Authorized 3rd party vendors
2. Payment processing system such as EFTPOS system to process credit cards	Finance Team

	Payment processing providers
3.	
4.	

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.9b: Asset Risk Environment Map (Physical)

This worksheet is used to identify and document the physical environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9b	ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Charging Station Control Systems	Tesla Operations/IT Teams
2. Embedded Firmware in Charging Hardware	Tesla Engineering Teams

3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Leased supercharger sites	Property owners

2. Public infrastructure such as shared telecommunication systems and utility boxes	Public authorities
	Unity providers
3.	
4.	

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.9c: Asset Risk Environment Map (People)

This worksheet is used to identify and document the people environment of a critical asset. Various internal and external technical containers and their ownership. This worksheet meets the requirements of step 3 of the OCTAVE Allegro process: Identify Asset Containers.

Allegro Worksheet 9c	ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1. Supercharger network technicians	Network Operation Team
2. Security analyst	Cybersecurity Team

3. Software developers who wrote codes for the Supercharger networks	Development Team
4.	
External Personnel	
Contractor, Vendor, Etc.	**Organization**
1. Customers who use the Supercharger Networks	Owners of Tesla vehicles

2. Government officials who regulate the networks	Government
3. Owners of the leased charging sites	The General Public
4.	

(OCTAVE Allegro Student Workbook v1.0, 2012)

Allegro Worksheet B.10: Asset Risk Worksheet

This worksheet is used to document and analyse risks associated with a critical asset. Information gathered in the previous worksheets are summarised here to help define the Threat Scenarios and their Impact and finally the risk scores. As a comprehensive worksheet, it covers step 4 to 8 of the OCTAVE Allegro process: Identify Areas of Concern, Identify Threat Scenarios,Identify Risks,Analyze Risk and Select Response Approach. The final Risk score is utilized as a comparison point with other scores to help prioritize risks and can vary from asset to asset based on the nature of the risks presented.

		OCTAVE® ALLEGRO Asset Risk Worksheet	
Asset Risk	**Threat**	**Asset**	Tesla's Supercharger Network
		Area of Concern	Physical destruction of charging infrastructure due to a natural disaster
		(1) Actor *Who would exploit the area of concern or threat?*	Nature event such as earthquake, flood wildfire

		(2) Means *How would the actor do it? What would they do?*	Supercharger units get damaged due to the natural disaster		
		(3) Motive *What is the actor's reason for doing it?*	N/A		
		(4) Outcome *What would be the resulting effect on the information asset?*	**Disclosure**	X **Destruction**	
			Modification	X **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Superchargers will not be available for public potential data loss may happen to corrupt the integrity.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	**Low** **X**
	(7) Consequences *What are the consequences on the organization or the information asset owner as a result of the outcome and breach of security requirements?*		**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		

		Impact Area	Value	Score
	Loss of availability in using the Supercharger in the areas affected by the nature diaster.	Reputation & Customer Confidence	Moderate (2)	3
		Financial	Moderate (2)	2
	Customer dissatisfaction will increase	Productivity	High (3)	1
		Safety & Health	Low (1)	5
	Loss of revenue and increase in expense	Fines & Legal Penalties	Low (1)	6

		User Defined Impact Area - environmental impact	Moderate (2)	4
Risk Score				**32**

(9) Risk Response			
Based on the total score for this risk, what action will you take?			
Accept	**Defer**	**Mitigate**	**Transfer**
		X	X
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		

Administrative	Purchase nature disaster insurance to transfer the risk
Physical	Install waterproof housing and stronger foundation for Superchargers
Technical	Data backup automatically to avoid data loss due to natural disasters

(OCTAVE Allegro Student Workbook v1.0, 2012)

Threat Scenario Questionnaire B.1: Technical Containers

This Questionnaire is used to assist in identifying potential threats that could arise due to the location of the technical asset. The process considers threats both within and external to the organization, and is used for each asset identified by Worksheet 9a. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. X's indicate selected answers in this example. (We answered this to the best of our abilities using assumptions.)

[redacted]	**Technical Containers**
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. **Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.**	
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee could access one or more technical containers, *accidentally or intentionally*, causing your information asset to be:	

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)** **X**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**

Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally or intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

		X	
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**

	Technical Containers

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine if any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

Unintended disclosure to your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset					
A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)** **X**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)** **X**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)** **X**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan Horse, or back door) is executed	**No**	**Yes (disclosure)** **X**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Power supply to technical containers is interrupted	**No**	**Yes (disclosure)** **X**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)** **X**	**Yes (interruption)**	**Yes (loss)**
Other third-party problems or systems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)** **X**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)** **X**

(OCTAVE Allegro Student Workbook v1.0, 2012, p 53)

Threat Scenario Questionnaire B.2: Physical Containers

This Questionnaire is used to assist in identifying potential threats that could arise due to the physical location of the asset. The process considers threats both within and external to the organization, and is used for each asset identified by Worksheet 9b. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. X's indicate selected answers in this example. (We answered this to the best of our abilities using assumptions.)

[redacted]	**Physical Containers**
This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. **Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.**	
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee could access one or more physical containers, *accidentally or intentionally*, causing your asset to be:	

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No** **X**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)** **X**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Scenario 2:			

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more physical containers, *accidentally or intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No** **X**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)** **X**

Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**

	Physical Containers

Scenario 3:

In this scenario, consider situations that could affect your physical containers, and by default, affect your information asset. Determine if any of the following could occur, and if yes, determine whether these situations would cause one or more of following outcomes:

Unintended disclosure to your information asset

Unintended modification of your information asset

Unintended interruption of the availability of your information asset

Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No** **X**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes** **(loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or ____ hurricane) occur	**No**	**Yes (disclosure)** **X**	**Yes (modification)**	**Yes (interruption)**	**Yes** **(loss)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Threat Scenario Questionnaire B.3: People

This Questionnaire is used to assist in identifying potential threats that could arise due to individuals both within and external to the organization, and is used for each asset identified by Worksheet 9c. This questionnaire is one of three utilized within step 5 of the OCTAVE Allegro process: Identifying Threat Scenarios. X's indicate selected answers in this example. (We answered this to the best of our abilities using assumptions.)

[redacted]	**People**		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally, or both.			
Scenario 1: Think about the people that work in your organization. Is there a situation where an employee has detailed knowledge of your information asset and could, *accidentally or intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

		X	
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)** **X**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)** **X**
Scenario 2:			

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could, *accidentally or intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)** **X**	**Yes (intentionally)**

(OCTAVE Allegro Student Workbook v1.0, 2012)

Appendix 3.1 : Risk Committee Charter

Tesla Inc.'s Risk Committee is tasked with ensuring the Executive Board has proper understanding of risks facing the organization, as well as coordinating risk assessments and other duties outlined in the governance structure. Meetings will be held every other month; any delays or cancellations must be agreed upon by the committee, and meetings must be quarterly at minimum (Tucker 2020).

Due to the heavy impact risks can have on the entire company, meeting attendance is expected to be 100%. In the case of an emergency, a Risk Committee member may send an alternate of one of their direct reports in their place. This alternate is considered the representative and voice of the committee member for the duration of the meeting and has full voting power (Tucker 2020).

Each meeting should have a secretary to take meeting minutes and share the minutes with the committee afterwards. This secretary may be a member of the Risk Committee, or another employee of Tesla that is trusted to safely handle any confidential information discussed in the meeting (Tucker 2020).

75% of the Risk Committee Members must be present for a meeting to occur. Decisions that necessitate a vote require majority agreement to pass (Tucker 2020).

Appendix 3.2 : Risk Subcommittee Charter

Tesla Inc.'s Risk Subcommittee is tasked with ensuring risk assessment use of the ERM process for prioritizing and managing risks related to specific activities and functionalities such as Cybersecurity, Product Safety, Supply Chain, AI/ML ethics, Environmental Risk and Financial risk. The RSC has the authority to prescribe ERM strategies and evaluate the effectiveness of ERM throughout Tesla Inc. (Tucker 2020)

Tesla's Risk Subcommittee membership is a core body of five to seven non-staff members, who are appointed by Tesla's Risk Committee. These are high-potential leaders who can effectively collaborate to govern, assess, and develop scenario plans for the most significant risks facing Tesla. (Tucker 2020)

Meetings will be held every month; any delays or rescheduling must be communicated to the Risk Committee for alignment. The target number of meetings in a year is 6 and no less than 2. (Tucker 2020)

The RSC has the following responsibilities (Tucker 2020):

- Report high-risk threats and opportunities to the RC when necessary.
- Counsel risk owners regarding risk assessment, response plans, and related actions.
- Evaluate the relevance of the Tesla's risk register in terms of meeting tactical and strategic business objectives, and update the register accordingly.
- Provide guidance to the ERM team about risks that need to be elevated to other corporate governance entities.
- Improve and implement changes to the ERM process, including proposing how to identify, assess, and manage risks across business lines and portfolios.
- Contribute to developing and the ongoing monitoring of Tesla's risk tolerance.
- Review and approve ERM policy exceptions when necessary.
- Leverage Tesla's resources to
    - help risk owners with response planning and
    - take measures to optimize the outcomes of all risks.

Each meeting should have a secretary to take meeting minutes and share the minutes with the committee afterwards. This secretary may be a member of the Risk Committee, or another employee of Tesla that is trusted to safely handle any confidential information discussed in the meeting (Tucker 2020).

75% of the Risk Committee Members must be present for a meeting to occur. Decisions that necessitate a vote require majority agreement to pass (Tucker 2020).

Appendix 4.1: Risk Appetite Statement

	Risk Appetite Statement by Category - Level of Attention		
	Executive	**Management**	**Front Line**
Technology	Complete failure or disruption of vehicle software rollout or AI/autopilot functions across markets	Significant delays (2+ weeks) in deploying OTA updates or production-ready models due to technology issues	Minor bugs or glitches in OTA updates or prototype demos
Operation	More than 5 consecutive days of halted Gigafactory production	More than 3 consecutive days of reduced production capacity	1 day of reduced production capacity
Finance	More than 10% deviation from quarterly financial targets (EBITDA, cash flow, or gross margin)	Any more than a 7% deviation from planned financial KPIs for a quarter	Any deviation noticed in financial performance dashboards
Regulatory	Regulatory violations leading to an inability to use a necessary product or work with a related market	Fines or penalties of any amount linked to regulatory violations	Warnings about any potential regulatory violations

	Cybersecurity	Data breach leading to loss of proprietary information that could impact another category	Any unusual or unauthorized access to proprietary information, particularly if there is access from an unanticipated location or a account	Awareness of cybersecurity threats to the industry within the last 6 months.
	Publicity	Downward trend in public image lasting longer than 2 weeks or loss of customers equal to >5% revenue	Negative press releases lasting longer than 1 week or loss of customers equal to 1-5% of revenue	Customer complaints or negative social media buzz lasting longer than 2 days
	Safety	Loss of life or permanent disability	Injury requiring time away or other reportable incidents	Bumps, strains, bruises

(Tucker, *Advancing Risk Management Capability Using the OCTAVE FORTE Process,* 2020)

Appendix 4.2 Assumptions Made

1. Technology Risk: Assumed Tesla's software-driven product model (e.g., OTA updates, FSD) implies tech failures are core business risks. Based on historical issues with Autopilot bugs, Tesla likely tolerates minor glitches but not widespread rollout issues.
2. Operation Risk: Assumed Tesla operates with lean inventory and tight production timelines. Tesla leverages a Just-in-Time (JIT) production strategy to minimize inventory and optimize cost efficiency. This approach leaves little buffer for disruptions, meaning even a few days of halted operations can result in: delays in global deliveries, missed quarterly targets, and bottlenecks in end-to-end EV and battery production.
3. Finance Risk: Tesla's financial metrics particularly margins and free cash flow are closely watched by institutional investors, analysts, and the media. As a publicly traded company with a volatile stock and high valuation multiples, even a 5-10% deviation from guidance can result in billions lost in market capitalization.
4. Regulatory: It is assumed that any regulatory violations to an extent that would prevent Tesla's ability to operate as expected should be the concern of executives. The assumptions are also made that warnings may be made inaccurately, but Tesla receiving any fines or penalties would indicate operational problems that should be addressed to avoid a disruption.
5. Cybersecurity: It is assumed that Tesla would want to protect customer personal information from being leaked to protect their one reputation and avoid legal fees, as well as avoid disruption to operations. Awareness of potential threats is beneficial in limiting the likelihood of being surprised.
6. Publicity: It is assumed that negative press for short periods of times may occur and not last, but consistent negative publicity should be addressed due to the potential of customer loss and in turn loss of revenue. The ranges for revenue loss were decided because while Tesla is multi-billion dollar company, small percentages of revenue loss can equate to many millions of dollars in loss.
7. Safety: It is assumed that simple injuries that do not qualify for an incident report are anticipated and can be addressed quickly. Injuries that require documentation or lead to loss of life must be assessed to determine the source of the safety failure.

Appendix 4.3 Likelihood of Risk Realization

Likelihood - Level of Attention		
Executive	**Management**	**Front Line**
Risk is between 75-100% likely to occur. Alternatively, this risk has become an issue within the organization within the past quarter and not yet been fully addressed or resolved.	Risk is between 30-75% likely to occur. Alternatively, this risk has become an issue within the organization within the past month and not yet been fully addressed or resolved.	Risk is between 1-30% likely to occur. Alternatively this risk has become an issue within the organization within the past week and not yet been fully addressed or resolved.

(Tucker, *Advancing Risk Management Capability Using the OCTAVE FORTE Process,* 2020)

Appendix 4.4 Heat Risk Map

For this heat map, risks are placed higher on the y axis to indicate greater assumed likelihood and further to the right on the x axis to indicate greater assumed impact.

Bumps and Bruises	Unplanned Outage	Safety Incident, Insider Threat
Broken Part Temporarily Lowers Productivity During a Shift	Cyber Security Breach	Loss of Customer
Overregulation	Compliance Violation	Natural Disaster

(Tucker, *Advancing Risk Management Capability Using the OCTAVE FORTE Process,* 2020)

References

Chipeta, C. (2025, January 14). What is Shadow IT? Benefits & Risks. Retrieved from UpGuard: https://www.upguard.com/blog/shadow-it

CISCO. (2025, March 21). What Is Shadow IT? Retrieved from CISCO: https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Ingram, D. (20215, March 11). Trump turns the White House lawn into a Tesla showroom. Retrieved from NBC News: https://www.nbcnews.com/tech/elon-musk/trump-musk-tesla-white-house-showroom-buys-car-rcna195905

Maverick, J. B. (2024, November 8). Tesla suppliers: Key and rumored parts suppliers. Retrieved from Investopedia: https://www.investopedia.com/ask/answers/052815/who-are-teslas-tsla-main-suppliers.asp

Montoya, R. (2024, January 12). What is the percentage of electric cars in the U.S.? Retrieved from Edmunds: https://www.edmunds.com/electric-car/articles/percentage-of-electric-cars-in-us.html

Nasdaq. (2025, March 23). Tesla, Inc. common stock (TSLA) institutional holdings. Retrieved from Nasdaq: https://www.nasdaq.com/market-activity/stocks/tsla/institutional-holdings

Powell, O. (2023, August 21). Tesla data breach caused by ‘insider wrongdoing’. Retrieved from Cybersecurity Hub: https://www.cshub.com/attacks/news/telsa-data-breach-caused-by-insider-wrongdoing

Scarfone, K. (2022, September 15). Use shadow IT discovery to find unauthorized devices and apps. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/tip/Use-shadow-IT-discovery-to-find-unauthorized-devices-and-apps

Infinita Lab. (2024, February 16). ‘What Is the H100 GPU Chip and Why Is It So Important for Advancements in AI?’ Retrieved from Medium.

https://infinitalab.medium.com/what-is-the-h100-gpu-chip-and-why-is-it-so-important-for-advancements-in-ai-c1ef3ae4395b

Tucker, B. (2025, March 10). *Cyber Risk Workbook* [Word Document].

Tucker, B. (2025, March 10). *Module 2_Asset Management_Tucker_Spring_2024* [Powerpoint Slides].

Tesla Inc. (2025, April 5). *About Us*. Retrieved from Tesla Inc. Website: https://www.tesla.com/about

Tucker, B. A. (2020). *Advancing Risk Management Capability Using the OCTAVE FORTE Process.* Pittsburgh: Carnegie Mellon University.

Black Hat Ethical Hacking. (2025, March 7). *Major Cyber Attacks that shaped 2024*. Retrieved from Black Hat Ethical Hacking Web site: https://www.blackhatethicalhacking.com/articles/major-cyber-attacks-that-shaped-2024/#:~:text=Cyberattacks%20skyrocketed%20in%202024%2C%20with%20an%20average%20of,due%20to%20its%20high%20volume%20of%20personal%20data.

dwang. (2023, October 17). *Tesla: More than just autopilot*. Retrieved from Harvard Business School: https://d3.harvard.edu/platform-digit/submission/tesla-more-than-just-autopilot/

Giaccone, S. C., & Magnusson, M. (2021). Unveiling the role of risk-taking in innovation: antecedents and effects. *R&D Management*, 103.

Team Mediaocean . (2022, September 16). *The competitive advantage of operational efficiency* . Retrieved from Mediaocean Web site: https://www.mediaocean.com/competitive-advantage-of-operational-efficiency

Tucker, B. A. (2012). *OCTAVE Allego student workbook v1.0*. Pittsburgh: Carnegie Mellon University

Williams, C. (2021, November 24). *What Risk Ownership Is and Isn't*. Retrieved from Strategic Decision Solutions: https://strategicdecisionsolutions.com/risk-ownership-what-it-is-isnt/

Zhu, A. C. (2020, September 23). *The Past, Present and Future of Tesla and the Emerging Market for Electronic Vehicles*. Retrieved from CAINZ Web site: https://cainz.org/8810/