TESLA

Risk Assessment for Tesla Inc.

TABLE OF CONTENTS

Introduction

In the critical manufacturing industry, Tesla is a leader. The unique position presents opportunities and difficulties, especially in cybersecurity, supply chain resilience, and regulatory compliance. Maintaining excellence in operations and protecting sensitive systems and data now need the ability to predict, evaluate, and react to risks.

Any firm security policy must start with risk assessment, which helps Tesla find weaknesses, analyze possible effects, and take preventative action. A thorough approach for evaluating risks throughout Tesla's supply chains, systems, and operations is provided in the following document. It guarantees that Tesla satisfies and surpasses regulatory requirements while tackling the particular difficulties of its operating environment by conforming to industry standards defined in FedRAMP and NIST SP 800-53. Through this framework, the document seeks to uphold Tesla's dedication to preserving resilience, safeguarding consumer confidence, and sustaining its position as a market leader.

Several important areas of emphasis form the basis of this risk assessment. The report assesses Tesla's systems' security classification and its digital and physical infrastructure weaknesses. It integrates a thorough supply chain risk management system to handle reliance on outside providers and minimize possible interruptions. In addition, it highlights how crucial contingency planning is to guarantee the quick recovery and reinstatement of vital business operations in the event of unanticipated circumstances. The controls offer a comprehensive picture of Tesla's risk environment and the steps needed to strengthen its defenses.

Tesla has a more outstanding obligation to adhere to best practices in risk management because of its position in the critical manufacturing industry. In addition to protecting its business, Tesla supports the integrity of the global energy infrastructure, supply networks, and technology ecosystem. As a result, the risk management document highlights creativity, flexibility, and teamwork. Also, it identifies and prioritizes risks and offers workable mitigation and reaction solutions.

Tesla emphasizes its dedication to operational security and risk management excellence with this risk assessment. The risk assessment is essential for strengthening the organization's resilience, safeguarding its resources, and ensuring long-term growth in an evolving threat environment that is becoming more complex and dynamic. Tesla continues to set the bar for risk management in the vital manufacturing industry by addressing risks, planning for emergencies, and cultivating a culture of security awareness.

Critical Infrastructure and Tesla

Tesla’s Role in the Critical Manufacturing Sector

Of the 16 sectors designated by the US federal government as vital to the United States' national security, economic stability, and public safety, Tesla’s operations fall mostly under the Critical Manufacturing sector. The sector encompasses industries responsible for manufacturing essential products that support critical systems, including those involved in the energy, transportation, water, and chemical sectors. Tesla’s activities, which encompass vehicle assembly, battery production, and renewable energy technology, demonstrate its integral role in supporting national infrastructure resilience and advancing sustainable innovation.

The Critical Manufacturing sector is responsible for manufacturing the components for other critical infrastructure sectors such as the Transportation, Energy, Chemical, and Water Sectors, and requires its manufacturers to use its precise manufacturing and cutting edge technology to support these critical sectors. Tesla exemplifies this through its Gigafactories, such as the Gigafactory Nevada, which focus on large-scale production of electric vehicles, batteries, energy storage devices, powertrains, and other such products to support critical systems in the energy and transportation sectors. These facilities not only produce critical components for Tesla’s EVs but also the products which Tesla produces to progress the broader adoption of sustainable energy solutions, such as lithium-ion battery cells and energy storage systems. Through the production of these components, Tesla supports the transition to a renewable energy future, addressing key priorities in energy security and environmental sustainability as a key part of the Critical Manufacturing sector which is becoming increasingly important as the United States moves more and more towards renewable energy and away from fossil fuels.

By bridging the Critical Manufacturing, Energy, and Transportation sectors, Tesla plays a multifaceted role in national infrastructure. For support in the Energy sector, Tesla’s batteries and energy storage solutions, such as the Powerwall and Powerpack, are integral to grid stability and the integration of renewable energy sources. For supporting the Transportation sector, Tesla advances the electrification of vehicles, enhancing the resilience and sustainability of transportation systems. The synergy of these contributions underscores Tesla’s significance within critical infrastructure.

Tesla has reporting obligations to the Department of Homeland Security (DHS). The DHS oversees risk assessments, audits, and resilience planning for the Critical Manufacturing sector, ensuring that companies like Tesla can mitigate vulnerabilities and enhance operational security. Tesla’s ability to innovate while maintaining compliance with national standards strengthens the security and reliability of the nation’s critical infrastructure.

In conclusion, Tesla’s contributions to the Critical Manufacturing sector extend beyond automotive production. By integrating advanced manufacturing techniques, renewable energy technologies, and innovative transportation solutions, Tesla solidifies its position as a cornerstone of national infrastructure. Its work supports the transition to sustainable energy and transportation systems, ensuring resilience in the face of evolving challenges and advancing U.S. infrastructure goals.

Protection Accommodations for Critical Manufacturing

Tesla stands at the forefront of the critical manufacturing sector, a domain deemed essential for national security, economic stability, and public safety by the U.S. federal government. The company takes its responsibility seriously, actively mitigating a wide array of risks that could jeopardize its critical infrastructure. A comprehensive risk assessment strategy is not just important; it is vital to ensure operational integrity and resilience against an array of threats.

Key Risks to Critical Infrastructure

Tesla has clearly identified several significant risks that demand immediate attention due to their potential impact on critical infrastructure:

1. **Cybersecurity Threats to Autonomous Systems:** The threat of nation-state actors targeting Tesla's autonomous driving systems is a serious concern. A successful breach could lead to widespread chaos on roads and in public spaces, endangering lives and disrupting transportation networks. This looming threat requires an unyielding cybersecurity framework, characterized by constant monitoring, thorough audits, and advanced encryption to protect vehicle communication systems.
2. **Supply Chain Integrity for the Optimus Gen 3 Robot:** The development and launch of the Optimus Gen 3 robot depend on strict adherence to supply chain provenance. Failure to ensure proper sourcing could result in catastrophic malfunctions reminiscent of past industrial failures just like the pager attack by hazebollah militants, endangering public safety and tarnishing Tesla’s reputation.
3. **Weaponization and Misuse of Robotics:** The risk of robots, including the Optimus model, being repurposed for malicious uses—such as forming unauthorized autonomous armies—cannot be overlooked. This concern highlights the necessity for stringent controls in the development and deployment of robotic technologies, enforcing robust physical and digital security measures to prevent misuse.

Tesla's Strategic Response

In response to these critical challenges, Tesla is implementing decisive strategies:

Enhanced Manufacturing Processes: Tesla enforces rigorous manufacturing protocols that mandate strict tracking of material and component provenance. By conducting thorough vendor assessments and maintaining transparency throughout the supply chain, Tesla is committed to mitigating risks associated with material integrity and compliance.

Training AI Against Adversarial Attacks: Tesla has adopted a proactive approach to counter the threats of data poisoning and adversarial attacks on AI models. Utilizing cutting-edge techniques such as adversarial training, Tesla's AI systems are designed to identify and neutralize potential threats, bolstering resilience against manipulation and ensuring operational safety.

Intrusion Detection Systems (IDS): The company employs advanced intrusion detection systems to vigilantly monitor and safeguard both physical and digital assets. These systems are essential for swiftly identifying potential threats, allowing Tesla to react immediately to detected anomalies, regardless of whether they stem from cyberattacks or attempts to breach operational protocols.

Tesla's commitment to these strategies underscores its determination to secure its critical infrastructure and uphold its reputation as a leader in innovation and safety.

Cyberattack Scenario

The following is a brief description of a potential cyberattack meant to disrupt Tesla’s operations. A malicious actor targets the Gigafactory Nevada as a prime target to steal proprietary data and disrupt Tesla operations, harming both Tesla’s productions as well as the US critical manufacturing sector. The first step of the malicious actor’s plan is to conduct reconnaissance, looking over social media such as LinkedIn or Instagram of Tesla employees and contractors to find the most vulnerable links to target for spear phishing attacks. Once enough information has been gathered, targeted phishing emails will be sent to mimic internal communications between Tesla employees, or emails from outside sources which an employee would plausibly get. These emails will contain links to malware that an employee will unknowingly install if they click the link.

Once malware is installed on an employee’s workstation, the malicious actor will have access to Tesla’s network, enabling movement to critical systems controlling manufacturing processes. Using compromised administrator credentials, the attackers inject malicious code into the factory's industrial control systems (ICS). This malicious code will halt production lines, cause equipment malfunctions which will snowball into massive downtime for the factory, disrupted supply chains for electric vehicle and energy storage production, and massive financial losses for Tesla. Simultaneously, the attacks will be able to extract sensitive intellectual property from the systems.

Vulnerabilities Exposed

1. **Insufficient Employee Training**
    a. **Problem:** Employees which have insufficient training may fall victim to phishing attacks or fail to recognize social engineering attempts.

    b. **Mitigation:** Implement comprehensive, role-based security training tailored to different employee groups. Conduct regular phishing simulations and offer immediate feedback to improve awareness.

2. **Inadequate Segmentation**
    a. **Problem:** Without proper segmentation of different systems in Tesla's factory, the attackers could easily move from system to system once they have access to one of them.

    b. **Mitigation:** Deploy strict network segmentation, separating critical manufacturing systems, corporate networks, and external-facing components. Enforce segmentation to limit access between systems.

3. **Insecure Industrial Control Systems (ICS)**
    a. **Problem:** Insecure ICS components can be targeted to disrupt manufacturing processes due to having known or easy exploits for attacks to take advantage of.

    b. **Mitigation:** Regularly update ICS software, implement intrusion detection systems tailored to ICS environments, and apply strict access controls to ICS networks.

4. **Insufficient Monitoring and Detection of Threats**
    a. **Problem:** Time is critical during ongoing incidents, and having a fast response could mean the difference of billions of dollars to both Tesla and the US economy, so swift detection and constant monitoring of threats is crucial.

    b. **Mitigation:** Invest in advanced threat detection tools, and establish a dedicated Security Operations Center (SOC) for real-time monitoring.

5. **Inadequate Email Screening**
    a. **Problem:** Malicious emails may bypass basic filters, exposing employees to phishing attacks or malware delivery.

    b. **Mitigation:** Deploy advanced email screening solutions, such as those using machine learning to detect malicious intent.

POA&Ms

Access Control Example

1. **POAM ID:** POAM-2025-TESLA-AC-017
2. **System Name:** Remote Access Security Plan
3. **Security Control:** AC-17 Remote Access
4. **Weakness Description:**
    a. Currently, remote access to Tesla systems represents a security risk due to a lack of proper monitoring or control for unauthorized access or misuse. There is also a lack of automated enforcement mechanisms to enforce compliance with Tesla's remote access security policies. Both of these lead to a potential vulnerability where a malicious actor or unauthorized employee could use remote access to gain access to Tesla systems.
5. **Risk Level:** High
6. **Recommendations:**
    a. **Implement automated mechanisms** to monitor and control remote access methods.
    b. **Integrate logging and auditing capabilities** to track remote access activities.
    c. **Introduce encryption** to protect remote access confidentiality and integrity.
    d. **Ensure remote access training** for eligible employees to understand security requirements.
7. **Resources Required:**
    a. **Vendor support** to install and configure automated tools for remote access.
    b. **Tesla's Security Team** to deploy, monitor, and maintain remote access systems.
    c. **Awareness and training** for all employees eligible for remote access.
    d. **Tesla's Financial Team** to determine and allocate the budget for implementing solutions.
8. **Scheduled Completion Date:** 2025-04-30
9. **Milestones:**
    a. **Milestone 1:** Identify and select automated remote access monitoring and control tools.
        i. **Planned Start Date**: 2025-01-05
        ii. **Planned End Date**: 2025-01-30

iii. **Status**: In Planning

iv. **Milestone Completion Date**: TBD

b. **Milestone 2:** Configure and deploy automated tools for monitoring remote access and encryption.

i. **Planned Start Date**: 2025-02-01

ii. **Planned End Date**: 2025-02-28

iii. **Status**: Pending

iv. **Milestone Completion Date**: TBD

c. **Milestone 3:** Conduct remote access awareness and training sessions for all employees.

i. **Planned Start Date**: 2025-03-01

ii. **Planned End Date**: 2025-03-30

iii. **Status**: Pending

iv. **Milestone Completion Date**: TBD

d. **Milestone 4:** Final review and testing of new remote access security tools and controls.

i. **Planned Start Date**: 2025-04-01

ii. **Planned End Date**: 2025-04-30

iii. **Status**: Pending

iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD

11. **Remarks:**

a. This plan is laid out to secure the currently unsecure remote access protocols and until this plan is fully completed, remote access should not be authorized for any usage to ensure security for Tesla Systems.

12. **POAM Owner:**

a. **Name:** Ainsley Arn

b. **Title:** Information Security Manager

c. **Contact:** ainsleyarn@tesla.com

13. **Approval:**

i. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)

ii. **Date of Signature:** 2024-11-25

iii. **CIO or Equivalent:** Michael Christabelle**,** Chief Information Officer (CIO)

iv. **Date of Signature:** 2024-11-26

Awareness and Training Example

1. **POAM ID:** POAM-2025-TESLA-AT-002
2. **System Name:** Training Program Rework Plan
3. **Security Control:** AT-2 Literacy Training and Awareness
4. **Weakness Description:**
    a. Internal data recorded about Tesla's employees and contractors regarding their assigned literacy training and awareness skills are not up to the standard necessary to mitigate major security risks. Current training modules show low engagement, with employees skipping through content and not retaining the necessary information. To address this, the Chief Learning Officer (CLO) has recommended gamifying the training to increase engagement and retention of security and privacy concepts.
5. **Risk Level:** High
6. **Recommendations:**
    a. Redesign the training program with a gamified approach to increase user engagement and retention.
    b. Monitor user interactions and feedback to ensure effectiveness of the new training format.
    c. Integrate interactive quizzes, badges, and progress tracking to motivate completion and learning.
7. **Resources Required:**
    a. **Training Development Team** to design the gamified system.
    b. **Software Developers** for game mechanics (e.g., points, rewards, badges).
    c. **IT infrastructure** to support the updated training platform.
    d. **Tesla's Financial Team** to determine and allocate the budget for implementing solutions.
8. **Scheduled Completion Date:** 2025-10-25
9. **Milestones:**
    a. **Milestone 1:** Develop and prototype gamified training module.
        i. **Planned Start Date:** 2025-01-10
        ii. **Planned End Date:** 2025-03-25

iii. **Status:** Planned

iv. **Milestone Completion Date**: TBD

b. **Milestone 2:** Pilot gamified training with a small group of employees and contractors.

i. **Planned Start Date:** 2025-03-30

ii. **Planned End Date:** 2025-05-15

iii. **Status:** Planned

iv. **Milestone Completion Date**: TBD

c. **Milestone 3:** Improve and update the gamified training module based on the responses from the pilot test.

i. **Planned Start Date:** 2025-05-20

ii. **Planned End Date:** 2025-07-15

iii. **Status:** Planned

d. **Milestone 4:** Full rollout of the gamified training program to all employees and contractors.

i. **Planned Start Date:** 2025-07-20

ii. **Planned End Date:** 2025-10-25

iii. **Status:** Planned

iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD

11. **Remarks:**

a. Since this security vulnerability is about something which cannot be immediately stopped waiting for the fix, department heads are encouraged to send out newsletters, discuss in meetings, or otherwise communicate to their teams the literacy awareness information that they feel like their teams needs to hear to safely and effectively achieve their teams goal while this new training program is being developed.

12. **POAM Owner:**

a. **Name:** Dariel Claire

b. **Title:** Training Manager

c. **Contact:** dclaire@tesla.com

13. Approval:

i. **Designation and Name:** Wrenley Arron, Chief Learning Officer (CLO)

ii. **Date of Signature:** 2024-11-25

iii. **CIO or Equivalent:** Michael Christabelle**,** Chief Information Officer (CIO)

iv. **Date of Signature:** 2024-11-24

Assessment, Authorization, and Monitoring Example

1. **POAM ID**: POAM-2025-TESLA-CA-008
2. **System Name**: Tesla Web Applications, Mobile Applications, Vehicles, and IoT Devices
3. **Security Control**: CA-8 - Penetration Testing
4. **Weakness Description**:
   a. Tesla's current penetration testing practices are insufficient, failing to thoroughly address all critical components such as web and mobile applications, vehicles and their embedded systems, cloud infrastructure, and essential communication protocols like Over-The-Air (OTA) updates and Vehicle-to-Everything (V2X) communications. This lack of comprehensive testing creates significant vulnerabilities that adversaries could easily exploit, particularly concerning IoT devices like the Powerwall and Tesla's physical security systems, including key fobs. Furthermore, current methodologies do not adequately tackle adversarial attacks on AI systems and supply chain security, posing serious risks that must be addressed.
5. **Risk Level**: High
6. **Recommendations**:
   a. Conduct thorough and rigorous penetration testing each year across all key security domains, including vehicles, software applications, embedded systems, IoT devices, and internal IT infrastructure.
   b. Leverage the FedRAMP Penetration Test Guidance to strengthen our testing protocols and ensure full compliance with industry standards.
   c. Establish targeted testing strategies that concentrate on adversarial AI attacks and data management vulnerabilities within Tesla’s operational frameworks.
   d. It's essential to bring on board highly skilled personnel with comprehensive knowledge in defending against AI attacks. By leveraging their basic penetration testing skills, we can effectively simulate real-world attacker scenarios and thoroughly explore a wide range of potential use cases. This proactive approach will strengthen our defense mechanisms and enhance our overall security strategy.
7. **Resources Required**:
   a. Budget allocation for hiring specialized cybersecurity firms with expertise in testing automotive and AI systems.

b. Deployment of advanced penetration testing tools that assess both software vulnerabilities and hardware security, including key fob systems.

c. Continuous training for internal IT and security personnel to stay current with the latest penetration testing practices and threats.

8. **Scheduled Completion Date**: 2025-12-30

9. **Milestones**:

   a. **Milestone 1**: CA-8 - Preparation for Annual Penetration Testing

      i. **Planned Start Date**: 2025-01-15

      ii. **Planned End Date**: 2025-02-15

      iii. **Status**: In Planning

      iv. **Milestone Completion Date**: TBD

   b. **Milestone 2**: CA-8 - Execution of Penetration Tests

      i. **Planned Start Date**: 2025-03-01

      ii. **Planned End Date**: 2025-11-30

      iii. **Status**: Pending

      iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date**: TBD

11. **Remarks**:

    a. The project is firmly in the planning phase, prioritizing the identification of external vendors and the precise definition of the penetration testing scope according to the latest industry standards and emerging threats. It is imperative that we ensure comprehensive coverage of all critical systems to effectively mitigate potential vulnerabilities linked to adversarial attacks and data integrity concerns.

12. **POAM Owner**:

    Name: Jarod Silvester

    Title: Chief Information Security Officer (CISO)

    Contact: jsilvester@tesla.comCISO

13. **Approval**:

    a. **Designation and Name**: Jarod Silvester, Chief Information Security Officer (CISO)

b. **Date of Signature**: 2024-11-28

c. **CIO or Equivalent**: Michael Christabelle, Chief Information Officer (CIO)

d. **Date of Signature**: 2024-11-29

Contingency Planning Example

1. **POAM ID:** POAM-2025-TESLA-CP-002
2. **System Name:** Contingency Planning Enhancement Initiative
3. **Security Control:** CP-2 Contingency Plan
4. **Weakness Description:**
    a. Tesla's current contingency planning documentation lacks sufficient detail regarding dependencies, alternate processing sites, and system recovery priorities. Recent simulations revealed unclear roles and responsibilities during disruptions, which resulted in delayed response times and a lack of coordination among teams.
5. **Risk Level:** High
6. **Recommendations:**
    a. Revise the contingency plan to address gaps, including detailed roles, responsibilities, and recovery for critical systems.
    b. Conduct bi-annual contingency plan testing, including exercises simulating a variety of disruption scenarios.
    c. Formalize and test agreements with alternate storage and processing sites to ensure readiness.
    d. Integrate training for staff to clarify roles during disruption scenarios and improve plan execution.
    e. Implement a centralized tracking system for monitoring contingency plan updates, testing schedules, and results.
7. **Resources Required:**
    a. **Contingency Planning Team**: Responsible for revising and testing the plan.
    b. **IT Infrastructure Team**: Support for system simulations and recovery environment.
    c. **Legal and Procurement Team**: Review and finalize agreements with alternate sites.
    d. **Financial Team**: Budget allocation for testing, training, and potential system upgrades.
8. **Scheduled Completion Date:** 2025-12-30
9. **Milestones:**

a. **Milestone 1:** Review and update contingency planning documentation, including detailed roles and alternate site details.
    i. **Planned Start Date:** 2025-01-10
    ii. **Planned End Date:** 2025-03-25
    iii. **Status:** Planned
    iv. **Milestone Completion Date**: TBD
b. **Milestone 2:** Formalize agreements with alternate storage and processing sites.
    i. **Planned Start Date:** 2025-03-30
    ii. **Planned End Date:** 2025-05-15
    iii. **Status:** Planned
    iv. **Milestone Completion Date**: TBD
c. **Milestone 3:** Conduct the first bi-annual exercise simulating a disruption at the primary processing site.
    i. **Planned Start Date:** 2025-05-20
    ii. **Planned End Date:** 2025-07-15
    iii. **Status:** Planned
    iv. **Milestone Completion Date**: TBD
d. **Milestone 4:** Update the contingency plan based on findings from the exercise.
    i. **Planned Start Date:** 2025-07-20
    ii. **Planned End Date:** 2025-10-25
    iii. **Status:** Planned
    iv. **Milestone Completion Date**: TBD
e. **Milestone 5:** Train employees on the updated contingency plan and their roles in a disruption scenario.
    i. **Planned Start Date:** 2025-10-25
    ii. **Planned End Date:** 2025-12-30
    iii. **Status:** Planned
    iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD
11. **Remarks:**
    a. While the enhanced contingency plan is under development, department heads are encouraged to ensure their teams have localized backup procedures and clear communication strategies to handle disruptions. All teams should review current roles and responsibilities as defined in existing plans and provide feedback for improvements.
12. **POAM Owner:**
    a. **Name:** James Fletcher
    b. **Title:** Contingency Planning Manager
    c. **Contact:** jfletcher@tesla.com
13. **Approval:**
    a. **Designation and Name:** Wrenley Arron, Chief Learning Officer (CLO)
    b. **Date of Signature:** 2024-11-25
    c. **CIO or Equivalent:** Michael Christabelle**,** Chief Information Officer (CIO)
    d. **Date of Signature:** 2024-11-26

Physical and Environmental Protection Example

1. **POAM ID**: POAM-2025-TESLA-PE-005
2. **System Name**: Tesla Output Devices and Reporting Systems
3. **Security Control**: PE-5 - Access Control for Output Devices
4. **Weakness Description**:
    a. Current access controls for physical output from devices such as printers, KPI dashboards, and energy output systems (including Powerwall, Powerpack, Megapack, and Optimus Gen 3 robot report screens) are insufficient to effectively prevent unauthorized access. There is a notable risk of insider threats, as employees or contractors may misuse their authorized access to obtain sensitive data for personal or competitive advantage. Furthermore, hacking attempts directed at output screens could result in unauthorized data exposure, presenting a significant threat to Tesla's operational integrity and security. Immediate action is necessary to bolster these controls and safeguard our sensitive information.
5. **Risk Level**: High
6. **Recommendations**:
    a. Implement secure print release systems to rigorously control access to printed materials, ensuring that only authorized personnel can retrieve sensitive output.
    b. Enhance physical security measures surrounding output devices by enforcing strict access controls and deploying robust monitoring systems.
    c. Conduct regular security training for employees, emphasizing the critical risks posed by insider threats and the necessity of safeguarding sensitive information.
    d. Establish a comprehensive incident response protocol to swiftly and effectively address any potential breaches of output data.
7. **Resources Required**:
    a. Investment in secure print release technology.
    b. Budget allocation for upgrading physical access controls and monitoring systems.
    c. Development of a security training program tailored to educate employees about the risks associated with output devices and data protection.
8. **Scheduled Completion Date**: 2026-06-30

9. **Milestones**:
    a. **Milestone 1**: PE-5 - Assessment of Current Physical Access Controls
        i. **Planned Start Date**: 2025-01-15
        ii. **Planned End Date**: 2025-02-15
        iii. **Status**: In Planning
        iv. **Milestone Completion Date**: TBD
    b. **Milestone 2**: PE-5 - Implementation of Secure Print Release Systems
        i. **Planned Start Date**: 2025-03-01
        ii. **Planned End Date**: 2025-04-30
        iii. **Status**: Pending
        iv. **Milestone Completion Date**: TBD
    c. **Milestone 3**: PE-5 - Enhancement of Physical Security Measures
        v. **Planned Start Date**: 2025-05-01
        vi. **Planned End Date**: 2025-06-15
        vii. **Status**: Pending
        viii. **Milestone Completion Date**: TBD
    d. **Milestone 4**: PE-5 - Employee Security Awareness Training Deployment
        ix. **Planned Start Date**: 2025-06-16
        x. **Planned End Date**: 2025-07-15
        xi. **Status**: Pending
        xii. **Milestone Completion Date**: TBD
10. **Milestone Completion Date**: TBD
11. **Remarks**:
    a. Since this security vulnerability is about something which cannot be immediately stopped waiting for the fix, temporary physical security measures might be taken in the interim while the plan is being implemented.
12. **POAM Owner**:
    a. **Name**: Jarod Silvester

b. **Title**: Chief Information Security Officer (CISO)

c. **Contact**: jsilvester@tesla.comCISO

13. **Approval**:

a. **Designation and Name**: Jarod Silvester, Chief Information Security Officer (CISO)

b. **Date of Signature**: 2024-11-28

c. **CIO or Equivalent**: Michael Christabelle, Chief Information Officer (CIO)

d. **Date of Signature**: 2024-11-29

Risk Assessment Example

1. **POAM ID:** POAM-2025-TESLA-RA-003
2. **System Name:** Risk Assessment Enhancement Initiative
3. **Security Control:** RA-3 Risk Assessment
4. **Weakness Description:**
    a. Tesla's current risk assessment practices lack comprehensive coverage of all system components and services, particularly in identifying and evaluating third-party risks. Additionally, risk assessments are not always updated after significant changes, which leaves some decisions based on outdated information.
5. **Risk Level:** High
6. **Recommendations:**
    a. Develop a unified risk assessment framework that includes third-party risks and privacy assessments.
    b. Automate portions of the risk assessment process using risk management tools.
    c. Require updates to risk assessments after significant changes to systems, services, or threat environment.
    d. Train relevant personnel to conduct and analyze risk assessments consistently across all organizational levels.
7. **Resources Required:**
    a. **Risk Management Team:** For implementing new assessment processes.
    b. **Third-party Auditors:** For evaluating vendor and supply chain risks.
    c. **Technology Tools:** Risk management platforms (e.g., OneTrust).
    d. **Training Materials:** For staff and system owners.
8. **Scheduled Completion Date:** 2025-10-25
9. **Milestones:**
    a. **Milestone 1:** Develop and document a comprehensive risk assessment framework.
        i. **Planned Start Date:** 2025-01-10
        ii. **Planned End Date:** 2025-03-25
        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

   b. **Milestone 2:** Automate risk assessments using new tools and integrate with Tesla's security infrastructure.

        i. **Planned Start Date:** 2025-03-30
        ii. **Planned End Date:** 2025-05-15
        iii. **Status:** Planned
        iv. **Milestone Completion Date**: TBD

   c. **Milestone 3:** Conduct pilot risk assessments with the new framework and tools.

        i. **Planned Start Date:** 2025-05-20
        ii. **Planned End Date:** 2025-07-15
        iii. **Status:** Planned
        iv. **Milestone Completion Date**: TBD

   d. **Milestone 4:** Update risk assessments for all critical systems and services based on findings.

        i. **Planned Start Date:** 2025-07-20
        ii. **Planned End Date:** 2025-10-25
        iii. **Status:** Planned
        iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD
11. **Remarks:**
    a. While the enhanced risk assessment framework is under development, department heads are advised to use the current framework for evaluating critical risks and escalate major findings to the Risk Management Team.
12. **POAM Owner:**
    a. **Name:** Sarah Thompson
    b. **Title:** Risk Manager
    c. **Contact:** sthompson@tesla.com
13. **Approval:**
    a. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)

b. **Date of Signature:** 2024-11-25

c. **CIO or Equivalent:** Michael Christabelle**,** Chief Information Officer (CIO)

d. **Date of Signature:** 2024-11-26

Supply Chain Risk Management Example

1. **POAM ID:** POAM-2024-TESLA-SR-006
2. **System Name:** Supply Chain Risk Mitigation Framework
3. **Security Control:** SR-2 Supply Chain Risk Assessment
4. **Weakness Description:**
    a. Tesla's current supply chain risk management framework lacks detailed visibility into third-party vendors' cybersecurity practices and dependencies. Recent audits identified significant gaps in tracking vendor risks, contract clauses for security compliance, and incident response coordination with suppliers. The significant gaps pose a high risk of potential supply chain disruptions or security vulnerabilities.
5. **Risk Level:** High
6. **Recommendations:**
    a. Develop a comprehensive framework for assessing third-party risks, including cybersecurity, and geographic vulnerabilities.
    b. Require all vendors to comply with Tesla's security standards by updating contracts.
    c. Implement a centralized vendor risk management tool to track supplier risks.
    d. Conduct annual assessments of high-priority suppliers and audit medium- to low-priority suppliers every three years.
    e. Establish a communication channel for vendors to report vulnerabilities or incidents affecting Tesla.
7. **Resources Required:**
    a. **Supply Chain Team** to work with vendors and revise contracts.
    b. **Legal Team** to draft and review updated contractual clauses.
    c. **IT Team** to implement and maintain vendor risk management tools.
    d. **Cybersecurity Team** to conduct supplier audits and risk assessments.
8. **Scheduled Completion Date:** 2025-10-25
9. **Milestones:**
    a. **Milestone 1:** Develop a comprehensive supply chain risk assessment framework.
        i. **Planned Start Date:** 2025-01-10

        ii. **Planned End Date:** 2025-03-25

        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

    b. **Milestone 2:** Revise contracts for high-priority vendors, including security compliance requirements.

        i. **Planned Start Date:** 2025-03-30

        ii. **Planned End Date:** 2025-05-15

        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

    c. **Milestone 3:** Implement and configure a centralized vendor risk management tool.

        i. **Planned Start Date:** 2025-05-20

        ii. **Planned End Date:** 2025-07-15

        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

    d. **Milestone 4:** Perform initial assessments and audits of high-priority vendors using the new framework and tools.

        i. **Planned Start Date:** 2025-07-20

        ii. **Planned End Date:** 2025-10-25

        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD
11. **Remarks:**

    a. Until the new supply chain risk management framework is fully implemented, Tesla will continue to monitor vendor risks using the current process. Department heads are encouraged to proactively discuss security expectations with their vendors and report potential risks to the Supply Chain Risk Management Team.

12. **POAM Owner:**

    a. **Name:** Marcus Eldridge

    b. **Title:** Supply Chain Risk Manager

c. **Contact:** meldridge@tesla.com

13. **Approval:**

    a. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)

    b. **Date of Signature:** 2024-11-25

    c. **CIO or Equivalent:** Michael Christabelle**,** Chief Information Officer (CIO)

    d. **Date of Signature:** 2024-11-26

Identification Authentication Example

1. **POAM ID:** POAM-2025-TESLA-IA-002
2. **System Name:** Internal Enterprise Management System (IEMS)
3. **Security Control:** IA-2 User Identification and Authentication
4. **Weakness Description:**
    a. The current authentication mechanism that Tesla employs within the IEMS is only based on single-factor authentication. This can result in a vulnerability that might expose the system to potential unauthorized access, which could be in the form of phishing, or brute-force attacks.This is a critical issue because of the sensitive nature of the data that is managed within IEMS.
5. **Risk Level:** High
6. **Recommendations:**
    a. There is the need to implement multi-factor authentication (MFA) across all IEMS modules.
    b. Additionally, we need to provide MFA options such as biometric authentication and authenticator apps.
    c. Training the employees and contractors on MFA usage is crucial.
7. **Resources Required:**
    a. Security engineering team for MFA integration into IEMS.
    b. IT infrastructure upgrades for biometric authentication.
    c. External consultancy for risk assessment.
8. **Scheduled Completion Date:** 2025-06-30
9. **Milestones:**
    a. **Milestone 1:** Define MFA requirements and develop an integration plan for IEMS.
        i. Planned Start Date: 2025-01-07
        ii. Planned End Date: 2025-02-22
        iii. Status: Planned
        iv. Milestone Completion Date: TBD
    b. **Milestone 2:** Deploy MFA for high-risk IEMS users (e.g., administrators, privileged accounts).
        i. Planned Start Date: 2025-03-01
        ii. Planned End Date: 2025-04-19

iii. **Status:** Planned

iv. **Milestone Completion Date:** TBD

c. **Milestone 3:** Roll out MFA to all users within IEMS.

i. **Planned Start Date**: 2025-05-13

ii. **Planned End Date:** 2025-06-29

iii. **Status:** Planned

iv. **Milestone Completion Date:** TBD

10. **Milestone Completion Date:** TBD
11. **Remarks:**
    a. While the implementation of the MFA is in progress, it is important to enhance the monitoring process, in order to reduce potential incidents.
12. **POAM Owner:**
    a. Name: Charles Sainz
    b. Title: Cybersecurity Program Manager
    c. Contact: csainz@tesla.com
13. **Approval:**
    a. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)
    b. **Date of Signature:** 2024-11-23
    c. **CIO or Equivalent:** Michael Christabelle, Chief Information Officer (CIO)
    d. **Date of Signature:** 2024-11-24

Incident Response Example

1. **POAM ID:** POAM-2025-TESLA-IR-004
2. **System Name:** Security Incident Management Platform (SIMP)
3. **Security Control:** IR-4 Incident Handling
4. **Weakness Description:**
    a. Currently, SIMP does not have a standardized incident handling procedures for responding to cyber threats. This gap might result in inconsistent responses to incidents and an inadequate document of recent security breaches.
5. **Risk Level:** High
6. **Recommendations:**
    a. We need to develop a standardized Incident Response (IR) document which is tailored to Tesla's systems and threat landscape.
    b. Further, we need to implement a ticketing system for tracking incident responses and their resolutions.
7. **Resources Required:**
    a. Incident Response team to design and implement the above mentioned document.
    b. Budget is required for upgrading SIMP to include ticketing and workflow management capabilities.
8. **Scheduled Completion Date:** 2025-09-17
9. **Milestones:**
    a. **Milestone 1:** Develop a draft IR document with standardized procedures for incident identification, containment, and recovery.
        i. **Planned Start Date:** 2025-02-13
        ii. **Planned End Date:** 2025-03-19
        iii. **Status:** Planned
        iv. **Milestone Completion Date**: TBD
    b. **Milestone 2:** Integrate a ticketing system within SIMP for tracking incident response processes.
        i. **Planned Start Date:** 2025-03-20

        ii. **Planned End Date:** 2025-09-16

        iii. **Status:** Planned

        iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date**: TBD
11. **Remarks:**
    a. Till the time the standardized IR procedures are in progress, interim guidelines will be provided to the relevant personnel, in order to make sure that the incidents are being consistently handled.
12. **POAM Owner:**
    a. **Name:** Raymond Holt
    b. **Title:** Incident Response Manager
    c. **Contact:** rholt@tesla.com
13. **Approval:**
    a. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)
    b. **Date of Signature:** 2024-11-23
    c. **CIO or Equivalent:** Michael Christabelle, Chief Information Officer (CIO)
    d. **Date of Signature:** 2024-11-24

Audit and Accountability Example

1. **POAM ID:** POAM-2025-TESLA-AU-006
2. **System Name:** Operational Monitoring Analytics System (OMAS)
3. **Security Control:** AU-6 Audit Review, Analysis, and Reporting
4. **Weakness Description:**
    a. The current OMAS system in our organization lacks the capability of automated altering in the occurrence of a critical security event. Additionally, even though the audit logs are being collected, they are not reviewed regularly due to lack of a system that can flag anomalies like unusual system activity patterns or unauthorized access, which might result in delayed detection and response to any potential threats.
5. **Risk Level:** High
6. **Recommendations:**
    a. Tesla needs to implement a Security Information and Event Management (SIEM) solution to automate log analysis and provide real-time alerts for critical security events.
    b. Also, we need to schedule weekly automated reports summarizing audit log activities for management review.
7. **Resources Required:**
    a. SIEM software and necessary hardware for deployment.
    b. Budget for acquiring the SIEM tool.
8. **Scheduled Completion Date:** 2025-11-01
9. **Milestones:**
    a. **Milestone 1:** Obtain and deploy a SIEM solution for automated log review and alerting.
        i. **Planned Start Date:** 2025-01-10
        ii. **Planned End Date:** 2025-03-25
        iii. **Status:** Planned
        iv. **Milestone Completion Date**: TBD
    b. **Milestone 2:** Implement regular automated reporting for audit log activities.
        i. **Planned Start Date:** 2025-04-01
        ii. **Planned End Date:** 2025-11-01

   iii. **Status:** Planned
   iv. **Milestone Completion Date**: TBD

10. **Milestone Completion Date:** TBD
11. **Remarks:**
    a. Tesla needs to increase the frequency of weekly manual reviews of audit logs till the time the SIEM solution is being implemented. This will help us in identifying any potential anomalies. For this, we would need to allocate additional personnel temporarily that's working towards these reviews.
12. **POAM Owner:**
    a. **Name:** Jay Dixit
    b. **Title:** Security Operations Lead
    c. **Contact:** jdixit@tesla.com
13. **Approval:**
    a. **Designation and Name:** Jarod Silvester, Chief Information Security Officer (CISO)
    b. **Date of Signature:** 2024-11-23
    c. **CIO or Equivalent:** Michael Christabelle, Chief Information Officer (CIO)
    d. **Date of Signature:** 2024-11-24

Access Control

AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **all Tesla Employees or Contractors which have access to Tesla Information Systems**:

   1. **Organization-level and system-level access** access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an **Chief Information Security Officer (CISO)** to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

   1. Policy **at least every 3 years** and following **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla's operation or information systems structure, or any other necessary event as determined by the CISO;** and

   2. Procedures **at least annually** and following **significant changes**.

AC-1 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-1(a): all Tesla Employees or Contractors which have access to Tesla Information Systems.
Parameter AC-1(a)(1): organization-level and system-level
Parameter AC-1(b): Chief Information Security Officer (CISO)
Parameter AC-1(c)(1)-1: At least every 3 years

	Parameter AC-1(c)(1)-2: major updates to the cybersecurity law, breaches in the industry, updates to Tesla’s operation or information systems structure, or any other necessary event as determined by the CISO
	Parameter AC-1(c)(2)-1: at least annually
	Parameter AC-1(c)(2)-2: significant changes
☐ Planned	Implementation Status:
	Control Origination: ☐ Service Provider Corporate

	AC-1 Implementation Risks
	Part a: Access control policy might be improperly documented such that policy and procedures are not followed, leading to insecure accessing and modification, compromising the integrity, confidentiality, and availability of Tesla information systems. Access control policy might not be properly developed to be consistent with the applicable laws concerning Tesla operations, putting Tesla in risk of being in legal trouble if found in violation.
	Part b: The CISO might not be able to properly manage the development of the access controls due to having a lot of responsibilities, leading to insecure AC policy and procedures which jeopardize Tesla information systems.
	Part c: The CISO might miss events that should’ve triggered a review and update to AC policies and/or procedures due to having a lot of responsibilities, leading to an outdated and therefore insecure AC policy and procedures which jeopardizes TEsla Information systems.

AC-2 Account Management (L)(M)(H)

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require **approval of an System Administrator that has checked the associated prerequisites and criteria** for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

   3. Access authorizations (i.e., privileges) and **approved actions** for each account;

e. Require approvals by **IT** for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with **policy, procedures, prerequisites, and criteria as determined by the CISO;**

g. Monitor the use of accounts;

h. Notify account managers and **associated IT personnel** within:

   1. **Twenty-four (24) hours** when accounts are no longer required;

   2. **Eight (8) hours** when users are terminated or transferred; and

   3. **Eight (8) hours** when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

   1. A valid access authorization;

   2. Intended system usage; and

   3. **Associated account role, group, and individual permissions;**

j. Review accounts for compliance with account management requirements **quarterly for privileged access, annually for non-privileged access**;

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

AC-2 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(c): approval of an System Administrator that has checked the associated prerequisites and criteria
Parameter AC-2(d)(3): approved actions
Parameter AC-2(e): IT
Parameter AC-2(f): with policy, procedures, prerequisites, and criteria as determined by the CISO
Parameter AC-2(h): associated IT personnel
Parameter AC-2(h)(1): Twenty-four hours
Parameter AC-2(h)(2): Eight hours
Parameter AC-2(h)(3): Eight hours
Parameter AC-2(i)(3): Associated account role, group, and individual permissions
Parameter AC-2(j): quarterly for privileged access, annually for non-privileged access
Implementation Status: ☐ Planned
Control Origination: ☐ Service Provider Corporate

AC-2 Implementation Risks
Part a: Poor documentation of the accounts allowed or prohibited in the system could lead to outdated systems that fail to manage the accounts and enable insecure access to Tesla systems, compromising them.

Part b: Poor choice in account managers could lead to poor management of accounts while would lead to improper and lose access control which enable insecure access to Tesla systems.
Part c: Poor choice in System Administrators could lead to administrators not properly checking prerequisites for group and role membership, leading to people having access to groups or roles that they should not have and enabling insecure access to Tesla systems. Overworking of System Administrators could lead to either a massive backlog of work for them, slowing down the operations of Tesla, or lead to System Administrators cutting corners and potentially leading to improper checking of group or role prerequisites and enabling insecure access to Tesla Systems.
Part d: Broadly defined access authorization and approved actions for given groups and roles could lead to potentially malicious internal actors to have greater control over the system than they should to do their job, leading to an increased risk of compromising of Tesla Systems.
Part e: IT could be inundated with work such that there becomes a backlog which slows down the approval of new accounts and slows down the operations of Tesla.
Part f: The CISO might be overworked such that the policy and procedures defined are lacking in terms of security quality, leading to insecure account management which could lead people with permissions that they shouldn’t have, increasing risk of compromising Tesla Systems.
Part g: Automated monitoring of accounts might flag actions incorrectly, leading to delays in the operations of Tesla Systems.
Part h: Failure to notify the necessary individuals of the changes to their accounts/account management requirements could lead to complications caused by misunderstandings of the

current account settings which could lead to delays in the operations of Tesla Systems or otherwise improper management that could lead to insecure management of Tesla Systems.
Part i: Roles and permissions to do certain actions might not be properly applied in a timely manner, leading to delays in Tesla’s production.
Part j: The distinction between privileged and non privileged actions is vague and could lead to confusion with implementing the regulations on Tesla’s Information Systems, causing delays or breaches in information security.
Part k: A disgruntled employee could abuse the group authenticator to sabotage a group’s information system responsibilities.
Part l: A complex account management process might be a discouraging factor in terminating someone’s employment leading to an inefficient work environment.

AC-2(1) Automated System Account Management (M)(H)

Support the management of system accounts using **automated mechanisms to notify account managers when an account is created, enabled, modified, disabled, or removed, automatic account management to handle when users are terminated or transferred; automatic systems which monitor system account usage and report atypical system account usage to IT.**

AC-2(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(1): automated mechanisms to notify account managers when an account is created, enabled, modified, disabled, or removed, automatic account management to handle when users are terminated or transferred; automatic systems which monitor system account usage and report atypical system account usage to IT.

Implementation Status: ☐ Planned
Control Origination: ☐ Service Provider Corporate

AC-2(1) Implementation Risks
Automated system mechanisms which too frequently notify about atypical system account usage might cause the responsible IT employees to ignore the messages and miss important notifications that need attention.

AC-2(2) Automated Temporary and Emergency Account Management (M)(H)

Automatically **disables** temporary and emergency accounts after **no more than 96 hours from last use.**

AC-2(2) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(2)-1: disables
Parameter AC-2(2)-2: no more than 96 hours from last use.
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(2) Implementation Risks
Improper disabling of emergency accounts could leave a backdoor vulnerability in Tesla’s information systems.

AC-2(3) Disable Accounts (M)(H)

Disable accounts within **twenty-four (24) hours for user accounts** when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for **ninety (90) days (See additional requirements and guidance.)**.

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP https://public.cyber.mil/dccs/

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

(d) Requirement: The service provider defines the time period of inactivity for device identifiers.

AC-2(3) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(3): twenty-four (24) hours for user accounts
Parameter AC-2(3)(d): ninety (90) days (See additional requirements and guidance.)
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(3) Implementation Risks
Part a:

There is no definition for an expired account so if expiration is not properly implemented for accounts, it will lead to clutter in the Tesla information systems that also pose a security vulnerability.
Part b: If an account is under the process of being transferred over to another user or individual, but is then disabled by this control, this could cause issues for those users leading to delays in Tesla's production or loss of revenue.
Part c: Accounts in violation of organization policy could potentially use the 24 hours before their account is disabled to compromise tesla information systems.
Part d: Accounts which are associated with individuals who have excuses to be inactivity for 90 days could lose their account due to this control, leading to delays in Tesla's production or loss of revenue.

AC-2(4) Automated Audit Actions (M)(H)

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-2(4) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(4) Implementation Risks
System misconfigurations or failures in the automated auditing process, could lead to incomplete or inaccurate logging of critical account actions.

AC-2(5) Inactivity Logout (M)(H)

Require that users log out when for privileged users, it is the end of a user's standard work period.

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12.

AC-2(5) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(5): for privileged users, it is the end of a user's standard work period.
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(5) Implementation Risks
This control, if automated, might cause issues for users who are working non-standard hours for whatever reason, delaying Tesla's operations.

AC-2(7) Privileged User Accounts (M)(H)

(a) Establish and administer privileged user accounts in accordance with a **role-based access scheme**;

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

AC-2(7) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(7)(a): **role-based access scheme**
Implementation Status (check all that apply):

☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(7) Implementation Risks
Part a: A role based access scheme might get overly bloated and complicated due to the number of roles employees can have, leading to delays or slowing down of the information systems and therefore operations of Tesla.
Part b: Monitoring might not be handled properly due to an overwhelming amount of role assignments, leading to insecure role assignments slipping through the cracks and leading to security vulnerabilities.
Part c: Monitoring might not be handled properly due to an overwhelming amount of role changes, leading to insecure role assignments slipping through the cracks and leading to security vulnerabilities.
Part d: Revoking of access might not be done due to those who are supposed to be monitoring the assignments having a lot on their plate, leading to security vulnerabilities where roles aren’t properly removed once they are no longer needed.

AC-2(9) Restrictions on Use of Shared and Group Accounts (M)(H)

Only permit the use of shared and group accounts that meet **organization-defined need with justification statement that explains why such accounts are necessary**.

AC-2 (9) Additional FedRAMP Requirements and Guidance:

Requirement: Required if shared/group accounts are deployed.

AC-2(9) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(9): **organization-defined need with justification statement that explains why such accounts are necessary**.
Implementation Status (check all that apply):

☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(9) Implementation Risks
If a shared account is handed out which is not actually needed, it opens up a security vulnerability which compromises Tesla’s systems.

AC-2(12) Account Monitoring for Atypical Usage (M)(H)

(a) Monitor system accounts for **atypical usage**; and

(b) Report atypical usage of system accounts to **at a minimum, the ISSO and/or similar role within the organization**.

AC-2 (12) Additional FedRAMP Requirements and Guidance:

(a) Requirement: Required for privileged accounts.

(b) Requirement: Required for privileged accounts.

AC-2(12) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(12)(a): **atypical usage**
Parameter AC-2(12)(b): **at a minimum, the ISSO and/or similar role within the organization**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(12) Implementation Risks

Part a: This control, if automated, might cause issues for users if normal work is flagged as atypical, causing delays in Tesla’s operations.
Part b: If there are a lot of atypical usages of system accounts, reviewing all those reports might lead to the ISSO being overloaded with work, opening up delays or security vulnerabilities.

AC-2(13) Disable Accounts for High-risk Individuals (M)(H)

Disable accounts of individuals **within one (1) hour** of discovery of **activity flagged as a significant security risk, or attempt to go beyond their assigned role parameters.**

AC-2(13) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-2(13)-1: **within one (1) hour**
Parameter AC-2(13)-2: **activity flagged as a significant security risk, or attempt to go beyond their assigned role parameters**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-2(13) Implementation Risks
This control, if automated, might cause issues for users if normal work is flagged as a significant security risk, causing delays in Tesla’s operations.

AC-3 Access Enforcement (L)(M)(H)

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-3 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)

Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-3 Implementation Risks
If roles and permissions are not carefully defined or implemented, users might gain unauthorized access to sensitive data or systems.

AC-4 Information Flow Enforcement (M)(H)

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on **data classification level, cross system information flow, and communication to and from external systems**.

AC-4 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-4: **data classification level, cross system information flow, and communication to and from external systems**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-4 Implementation Risks
If information flow control policies are incomplete or vague, enforcement mechanisms may not address all potential risks.

Improper configuration of network devices, firewalls, or data transfer systems can lead to unintended data leaks or block legitimate data flows.

AC-4(21) Physical or Logical Separation of Information Flows (M)(H)

Separate information flows logically or physically using **VLANs, Data tagging and filtering, Encrypted tunnels** to accomplish **separation of information flows for operational, regulatory, and data sensitivity purposes.**

AC-4(21) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-4(21)-1: **LANs, Data tagging and filtering, Encrypted tunnels**
Parameter AC-4(21)-2: **separation of information flows for operational, regulatory, and data sensitivity purposes.**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-4(21) Implementation Risks
Improper configuration in VLANs, firewalls, or routing rules can undermine the separation, leading to data leakage or unauthorized access. Incomplete documentation of separation requirements and mechanisms can lead to inconsistent implementation.

AC-5 Separation of Duties (M)(H)

a. Identify and document **engineering design approvals, financial transaction approvals, cybersecurity monitoring, and IT system administration as duties requiring separation**; and

b. Define system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.

AC-5 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-5(a): **engineering design approvals, financial transaction approvals, cybersecurity monitoring, and IT system administration as duties requiring separation**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-5 Implementation Risks
Part a: Missing critical duties requiring separation could leave gaps in control, which opens up Tesla's systems to being compromised. Incomplete documentation of separation requirements and mechanisms can lead to inconsistent implementation which could lead to insecure information systems or delays in production.
Part b: Excessively limiting access can hinder efficiency, potentially delaying the operations of Tesla's systems.

AC-6 Least Privilege (M)(H)

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-6 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply):

☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6 Implementation Risks
Overgranting of roles to favor efficiency over security could lead to security vulnerabilities as users have more permissions than they need to do their job. If not properly updated and reassessed, users might accumulate privileges, again leading them to have more permissions than they need.

AC-6(1) Authorize Access to Security Functions (M)(H)

Authorize access for **System Administrators** to:

(a) **establish system accounts, configure access authorizations, set events to be audited, and set intrusion detection parameter**; and

(b) **filtering rules for routers/firewalls, configuration parameters for security services, and access control lists.**

AC-6(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-6(1): **System Administrators**
Parameter AC-6(1)(a): **establish system accounts, configure access authorizations, set events to be audited, and set intrusion detection parameter**
Parameter AC-6(1)(b): **filtering rules for routers/firewalls, configuration parameters for security services, and access control lists.**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(1) Implementation Risks
Part a: If there isn't proper logging of changes to security critical actions such as changing access authorizations, there becomes a security and incident response risk of not being able to track things back to those actions or flag them to rectify poor changes.
Part b: It's possible that System Administrators are poorly trained and improperly change the security configurations in a way which causes security vulnerabilities to be opened up.

AC-6(2) Non-privileged Access for Nonsecurity Functions (M)(H)

Require that users of system accounts (or roles) with access to **all security functions** use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

AC-6(2) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-6(2): **all security functions**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(2) Implementation Risks

If there is inconsistent enforcement of this control because those with security functionality find it more efficient to not use a non-privileged account, it leads to potential security vulnerabilities if a non-privileged user was able to gain access to that account.

AC-6(5) Privileged Accounts (M)(H)

Restrict privileged accounts on the system to **System Administrators**.

AC-6(5) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-6(5): **System Administrators**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(5) Implementation Risks
Restricting privileged accounts to System Administrators runs the risk of overloading them with work, leading to delays in production due to them having a backlog of work and/or increased security vulnerabilities due to lower quality of work.

AC-6(7) Review of User Privileges (M)(H)

(a) Review **at a minimum, annually** the privileges assigned to **all users with privileges** to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6(7) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-6(7)(a)-1: **at a minimum, annually**

Parameter AC-6(7)(a)-2: **all users with privileges**
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(7) Implementation Risks
Part a: Annually reviewing privileges might leave a gap in security where someone only needed a role for a brief period but has the role for potentially up to a year before it is removed.
Part b: Reviewing the permissions of everyone in the company with permissions to do everything is a big task that if not properly divided up could take a long time and cause delays in tesla's operations.

AC-6(9) Log Use of Privileged Functions (M)(H)

Log the execution of privileged functions.

AC-6(9) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(9) Implementation Risks

If a shared/group account does a privileged action, it’s possible that there is no way to actually track which individual in the shared account did the privileged action, leading to a potential issue with accountability for that action.

AC-6(10) Prohibit Non-privileged Users from Executing Privileged Functions (M)(H)

Prevent non-privileged users from executing privileged functions.

AC-6(10) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Planned
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-6(10) Implementation Risks
The system setup to prevent non-privileged users from executing privileged functions could be improperly implemented with ways for users to bypass it, leading to security vulnerabilities which might compromise Tesla’s Systems.

AC-7 Unsuccessful Logon Attempts (L)(M)(H)

a. Enforce a limit of **5** consecutive invalid logon attempts by a user during a **12 hour time period**; and

b. Automatically **lock the account or node until released by an administrator;** when the maximum number of unsuccessful attempts is exceeded.

AC-7 Additional FedRAMP Requirements and Guidance:

Requirement: In alignment with NIST SP 800-63B

AC-7 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)

Parameter AC-7(a)-1: **5**
Parameter AC-7(a)-2: **12 hour time period**
Parameter AC-7(b): **lock the account or node until released by an administrator;**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-7 Implementation Risks
Part a: There is a risk of employees genuinely failing to log into their account 5 times and their work being delayed, therefore delaying Tesla's operations.
Part b: It's possible that administrators have a lot of work, so they won't be able to unlock employees who accidentally got logged out for a significant chunk of time, leading to significant delays in an employee's work.

AC-8 System Use Notification (L)(M)(H)

a. Display **see additional Requirements and Guidance** to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

   1. Users are accessing a U.S. Government system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information **see additional Requirements and Guidance**, before granting further access to the publicly accessible system
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

AC-8 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-8(a): **see additional Requirements and Guidance**
Parameter AC-8(c)(1): **see additional Requirements and Guidance**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-8 Implementation Risks
Part a: Users might not properly read or understand the warning before they use the system, leading to them using the system in an improper/insecure way.
Part b: Verification could be overly cumbersome to users, causing delays in user's work and delaying Tesla Operations.
Part c: The authorized action list might be too long for users to properly understand, leading to them either using the system in an improper/insecure way or not understanding why their unauthorized actions are not working and getting frustrated, leading to delays in their work and Tesla operations. The authorized action list might include actions that the user does not need to perform to achieve their job, violating the least privilege principle and opening potential security vulnerabilities.

AC-11 Device Lock (M)(H)

a. Prevent further access to the system by **initiating a device lock after fifteen (15) minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended**; and

b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

AC-11 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-11(a): **initiating a device lock after fifteen (15) minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended**
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

AC-11 Implementation Risks
Part a: Inconsistent enforcement of requiring a user to initiate a device lock before leaving a system unattended could lead to a user leaving their device unattended and open which gives a malicious actor potentially 15 minutes to gain access to the system and compromise Tesla's Systems.
Part b: Device locks for particular privileged users could require tedious identification and authentication procedures which harm the productivity of users leading to delays in Tesla operations.

AC-11(1) Pattern-hiding Displays (M)(H)

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

AC-11(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-11(1) Implementation Risks
If the proper security programs and procedures are not handled properly on the hardware side, a malicious user could still gain information about the system even from a locked laptop or desktop due to the machine storing information about the state of the machine for a quick boot up back to what the user was doing before, which is a potential security vulnerability.

AC-12 Session Termination (M)(H)

Automatically terminate a user session after **suspicious activity, the end of the workday, when a user's roles/privileges are changed, and inactivity timeout**.

AC-12 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-12: **suspicious activity, the end of the workday, when a user's roles/privileges are changed, and inactivity timeout**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-12 Implementation Risks
Overly aggressive monitoring of activity might lead to normal activity by an employee being flagged as suspicious activity which triggers a logout, leading to a delay in Tesla operations. Poorly implemented end of workday rules might lead to users who are working non-standard hours getting logged out in the middle of their work.

AC-14 Permitted Actions Without Identification or Authentication (L)(M)(H)

a. Identify **none** that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

AC-14 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)

Parameter AC-14(a): **none**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-14 Implementation Risks
Part a: Implementing overly strict identification or authentication for all actions may inadvertently hinder legitimate, necessary user activities for low-risk tasks, causing unnecessary delays in Tesla operations.
Part b: Improper documentation of the supporting rationale for the security plan could lead to future individuals assessing the policies to not properly understand why the decisions were made. This is bad because either they fail to understand that it was a necessary change and change it for the worse, or they leave it and potentially leave in outdated security policies.

AC-17 Remote Access (L)(M)(H)

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

AC-17 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate

AC-17 Implementation Risks
Part a: Improper configuration on the restrictions on remote access can lead to remote access being used to access Tesla systems in an insecure way which exposes the systems to leaking information or to a malicious actor to attack.
Part b: The process for authorizing remote access could be delayed leading to unauthorized remote access could occur before approval is granted, increasing the risk of exposure to malicious actors or unauthorized insiders accessing the system.

AC-17(1) Monitoring and Control (M)(H)

Employ automated mechanisms to monitor and control remote access methods.

AC-17(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-17(1) Implementation Risks
Automated monitoring tools may generate false positives, flagging legitimate remote access activities as suspicious or malicious. This can lead to unnecessary disruptions and delays in Tesla’s operations.

AC-17(2) Protection of Confidentiality and Integrity Using Encryption (M)(H)

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(2) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-17(2) Implementation Risks
Incorrectly configured encryption settings could undermine the effectiveness of encryption and leave remote access sessions vulnerable to attacks.

AC-17(3) Managed Access Control Points (M)(H)

Route remote accesses through authorized and managed network access control points.

AC-17(3) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-17(3) Implementation Risks
Routing all remote access traffic through centralized access control points could create performance bottlenecks, delaying remote access work and therefore Tesla operations.

AC-17(4) Privileged Commands and Access (M)(H)

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: **time and mission critical actions which cannot be done non-remotely**; and

(b) Document the rationale for remote access in the security plan for the system.

AC-17(4) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-17(4)(a): **time and mission critical actions which cannot be done non-remotely**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-17(4) Implementation Risks
Part a: Privileged actions being able to be performed remotely represents a very large security threat to Tesla's information security systems, so if any remote access is approved beforehand, it needs to be secured very concretely, as the risk of a malicious actor hijacking or mimicking a remote access request to compromise Tesla's systems is a very big risk.
Part b: Improper documentation of the supporting rationale for the security plan could lead to future individuals assessing the policies to not properly understand why the decisions were made. This is bad because either they fail to understand that it was a necessary change and change it for the worse, or they leave it and potentially leave in outdated security policies.

AC-18 Wireless Access (L)(M)(H)

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

AC-18 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-18 Implementation Risks
Part a: Improper configuration requirements could lead to insecure wireless access being approved, leaving the network vulnerable to attacks Overlapping wireless connections might lead to potential security gaps.
Part b: Failure to monitor wireless connections and enforce disconnection of unauthorized wireless access could lead to unauthorized access to Tesla Systems which compromises the system.

AC-18(1) Authentication and Encryption (M)(H)

Protect wireless access to the system using authentication of **users; devices** and encryption.

AC-18(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-18(1): **users; devices**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-18(1) Implementation Risks
Improper authentication of both users and devices, or failing to connect users with devices in the authentication, could lead to security gaps where a malicious actor can use an authorized device to gain access to Tesla Systems wirelessly.

AC-18(3) Disable Wireless Networking (M)(H)

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AC-18(3) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-18(3) Implementation Risks
Wireless capabilities might not be properly disabled across all components, leading to security gaps which can be taken advantage of. The disabling of these wireless capabilities might be overlooked by the individuals assigned to do it during the system configuration process.

AC-19 Access Control for Mobile Devices (L)(M)(H)

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

AC-19 Control Summary Information

Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-19 Implementation Risks
Part a: Inconsistent configuration of mobile devices, especially different types of mobile devices, could lead to security gaps. Improper configuration of mobile devices to handle secure information which outside of control areas could lead to the leaking of Tesla information.
Part b: Authorizing approved mobile devices to connect to Tesla systems could lead to a malicious actor gaining access to Tesla systems through a stolen employee phone.

AC-19(5) Full Device or Container-based Encryption (M)(H)

Employ **full-device encryption** to protect the confidentiality and integrity of information on **mobile devices given to employees for work usage**.

AC-19(5) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-19(5)-1: **full-device encryption**
Parameter AC-19(5)-2: **mobile devices given to employees for work usage**.
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate

AC-19(5) Implementation Risks
Insecure encryption could lead to malicious actors still being able to get sensitive information from the information stored on phones if they gain physical access to an employee’s phone.

AC-20 Use of External Systems (L)(M)(H)

a. **Establish terms and conditions**, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of **personally owned information systems/devices, privately owned computing and communications devices resident in commercial or public facilities, information systems owned or controlled by non approved organizations**

AC-20 Additional FedRAMP Requirements and Guidance:

Guidance: The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows:

AC-20 describes system access to and from external systems.

CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system.

SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.

AC-20 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-20(a): **Establish terms and conditions**
Parameter AC-20(b): **personally owned information systems/devices, privately owned computing and communications devices resident in commercial or public facilities, information systems owned or controlled by non approved organizations**

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-20 Implementation Risks
Part a: Failure to adequately define and document the terms and conditions for external system use can result in ambiguous security requirements and inconsistent enforcement. Mismanagement of trust relationships between the organization and external system owners can lead to unauthorized access or data breaches.
Part b: Inconsistent enforcement of this prohibition could lead to security vulnerabilities where employees try to access sensitive information on their personal devices, or try to connect with their employee devices to unsecure public wifi.

AC-20(1) Limits on Authorized Use (M)(H)

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization’s security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

AC-20(1) Implementation Risks
Part a: Verification might be improperly or hastily done, or not enough information might be provided to the verifier to confirm that the controls have been implemented. Both of these lead to improper verification of controls which mean that connection to the external system would be insecure.
Part b: Employees might use unauthorized devices to access unauthorized external systems which creates a security vulnerability.

AC-20(2) Portable Storage Devices — Restricted Use (M)(H)

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using **device authorization, encryption, logging and monitoring, whitelisted system restrictions**.

AC-20(2) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-20(2): **device authorization, encryption, logging and monitoring, whitelisted system restrictions**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-20(2) Implementation Risks

Unauthorized devices could bypass these controls, which opens up a security vulnerability if tesla information is put on an unauthorized device and then connected to an external system. Authorized users might not comply with external system restrictions, opening up security gaps.

AC-21 Information Sharing (M)(H)

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for **sensitive information such as contract-sensitive information, proprietary information, personally identifiable information, or other information as determined by the CISO**; and

b. Employ **data classification systems** to assist users in making information sharing and collaboration decisions.

AC-21 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-21(a): **sensitive information such as contract-sensitive information, proprietary information, personally identifiable information, or other information as determined by the CISO**;
Parameter AC-21(b): **data classification systems**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-21 Implementation Risks
Part a: Users might improperly assess the data authorizations assigned to a sharing partner and share information that does not match its use restrictions.

Access authorizations assigned to a sharing partner might be out of date meaning that information shared with them is a security risk.
Part b: The data classification systems might be out of date for certain information and sharing partners, leading to people making uninformed and insecure decisions based on it.

AC-22 Publicly Accessible Content (L)(M)(H)

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information **at least quarterly** and remove such information, if discovered.

AC-22 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter AC-22(d): **at least quarterly**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AC-22 Implementation Risks
Part a: If a disgruntled employee who was previously authorized to make information publicly accessible, they could sabotage the company by releasing information that would harm Tesla’s reputation or shareholders.

Part b: If the training is poor or insufficient, authorized employees could accidently post non-public information without approval.
Part c: Reviews for public information posts might be rushed due to an overloaded amount of requests, leading to the leaking of non-public information.
Part d: The quarterly reviews of the public information might not catch all the non-public information due to not being thorough enough.

Awareness and Training

AT-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **all Tesla Employees or Contractors**:

   1. **Organization-level and system-level access** awareness and training policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an **Chief Learning Officer (CLO)** to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

   1. Policy **at least every three (3) years** and following **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla's operation or information systems structure, or any other necessary event as determined by the CLO**; and

   2. Procedures **at least annually** and following **significant changes**.

AT-1 Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Parameter AT-1(a): **all Tesla Employees or Contractors**
Parameter AT-1(a)(1): **Organization-level and system-level access**
Parameter AT-1(b): **Chief Learning Officer (CLO)**
Parameter AT-1(c)(1)-1: **at least every three (3) years**
Parameter AT-1(c)(1)-2: **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla's operation or information systems structure, or any other necessary event as determined by the CLO**
Parameter AT-1(c)(2)-1: **at least annually**
Parameter AT-1(c)(2)-2: **significant changes**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-1 Implementation Risks
Part a: Awareness and training policy might be improperly documented such that policy and procedures are not followed, leading to insufficient training of Tesla employees. Awareness and training policy might not be properly developed to be consistent with the applicable laws concerning Tesla operations, putting Tesla in risk of being in legal trouble if found in violation.
Part b:

	The CLO might not be able to properly manage the development of the AT policy due to having a lot of responsibilities, leading to insecure AT policy and procedures and improper training of employees.
	Part c: The CLO might miss events that should’ve triggered a review and update to AT policies and/or procedures due to having a lot of responsibilities, leading to an outdated and therefore insecure AT policy and procedures.

AT-2 Literacy Training and Awareness (L)(M)(H)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

    1. As part of initial training for new users and **at least annually** thereafter; and

    2. When required by system changes or following **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla’s operation or information systems structure, or any other necessary event as determined by the CLO**;

b. Employ the following techniques to increase the security and privacy awareness of system users **interactive training modules, simulations, training newsletters** ;

c. Update literacy training and awareness content **at least annually** and following **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla’s operation or information systems structure, or any other necessary event as determined by the CLO**; and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

AT-2 Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Parameter AT-2(a)(1): **at least annually**
Parameter AT-2(a)(2): **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla’s operation or information systems structure, or any other necessary event as determined by the CLO**

Parameter AT-2(b): **interactive training modules, simulations, training newsletters**
Parameter AT-2(c)-1: **at least annually**
Parameter AT-2(c)-2: **major updates to applicable laws, updated industry standards, breaches in the industry, updates to Tesla's operation or information systems structure, or any other necessary event as determined by the CLO**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-2 Implementation Risks
Part a: Inadequate training, particularly for new users and contractors, could lead to security gaps and vulnerability to attacks like phishing.
Part b: Unengaging training could lead to users not properly absorbing all of the information and just breezing through the training, leading to security gaps and vulnerability to attacks. Simulations could fail to properly replicate real life incidents, leading to a false sense of security.
Part c: Outdated training might fail to capture new and upcoming types of attacks and vulnerabilities, leaving tesla susceptible to those types of attacks.
Part d: Proper lessons might not be able to be taken away from incidents due to a poor or chaotic incident response which fails to properly document everything that lead to a given incident.

AT-2(2) Insider Threat (L)(M)(H)

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2(2) Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-2(2) Implementation Risks
Employees might not recognize the indicators of an insider threat that is their friend due to their emotional attachment to the person, and they might be reluctant to report them even if they do recognize the indicators. Employees reporting other employees for minor indicators and getting them fired might lead to a toxic work environment where people are constantly stressed about being seen as a potential insider threat.

AT-2(3) Social Engineering and Mining (M)(H)

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-2(3) Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-2(3) Implementation Risks

Users might not recognize social engineering tactics which are not covered in the training course, or are more complicated to pick up on, leading to certain new types of attacks working on them.

AT-3 Role-based Training (L)(M)(H)

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: **Chief Information Security Officer, System Administrators, IT Personnel, Developers, Customer Support Representatives**:

   1. Before authorizing access to the system, information, or performing assigned duties, and **at least annually** thereafter; and

   2. When required by system changes;

b. Update role-based training content **at least annually** and following **major incidents, updates to roles or responsibilities, or other events as determined by the CLO**; and

c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

AT-3 Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Parameter AT-3(a): **Chief Information Security Officer, System Administrators, IT Personnel, Developers, Customer Support Representatives**
Parameter AT-3(a)(1): **at least annually**
Parameter AT-3(b)-1: **at least annually**
Parameter AT-3(b)-2: **major incidents, updates to roles or responsibilities, or other events as determined by the CLO**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-3 Implementation Risks
Part a: If the training is not adequate for a given role's specific responsibilities, it could lead to employees not knowing how to do their role in a secure manner.
Part b: Out of date training and awareness for role based training could lead to employees continuing to act in an insecure manner, unaware of the new strategies and procedures they should be aware of.
Part c: Proper lessons might not be able to be taken away from incidents due to a poor or chaotic incident response which fails to properly document everything that leads to a given incident. Additionally, the lessons that are taken away from any given incident might be inconsistently applied or considered across different roles or departments, leading to security gaps.

AT-4 Training Records (L)(M)(H)

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for **at least one (1) year or one (1) year after completion of a specific training program**.

AT-4 Control Summary Information
Responsible Role: Chief Learning Officer (CLO)
Parameter AT-4(b): **at least one (1) year or one (1) year after completion of a specific training program**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AT-4 Implementation Risks
Part a: Incomplete documentation of training that employees undergo could lead to gaps in an individual's training records, which could lead to non-compliance or lack of preparedness. If training records are improperly stored, there is a risk related to the data integrity of those records being manipulated.
Part b: For training that is not a part of digitally tracked modules, it is possible that the training records are not recorded properly, leading to the potential failure of compliance audits.

Audit and Accountability

AU-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **relevant personnel, including IT security staff and audit team members**:

   1. **Organization-level** audit and accountability policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate a **Compliance Officer** to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

   1. Policy **at least every three (3) years** and following **significant incidents, regulatory updates, or internal audits**; and

   2. Procedures **at least annually** and following **significant changes in organizational structure**.

AU-1 Control Summary Information
Responsible Role: Compliance Officer (CCO)
Parameter AU-1(a): relevant personnel, including IT security staff and audit team members
Parameter AU-1(a)(1): Organization-level
Parameter AU-1(b): Compliance Officer
Parameter AU-1(c)(1)-1: at least every three (3) years
Parameter AU-1(c)(1)-2: significant incidents, regulatory updates, or internal audits
Parameter AU-1(c)(2)-1: at least annually
Parameter AU-1(c)(2)-2: significant changes in organizational structure
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-1 Implementation Risks
Part a: If the procedures are inadequate, it can cause a lot of confusion during audits, which can lead to errors and potential security breaches.
Part b: Delays in appointing a Compliance Office can result in accountability gaps.
Part c: It is possible that Tesla's fast paced innovation can lead to policies becoming outdated before the scheduled update cycle.

AU-2 Event Logging (L)(M)(H)

a. Identify the types of events that the system is capable of logging in support of the audit function: **successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications:**

all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: **a subset of the auditable events defined in AU-2a to be audited continually, including logon failures, privilege escalations, and policy changes**;

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging **annually and whenever there is a change in the threat environment**.

AU-2 Additional FedRAMP Requirements and Guidance:

(e) Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

AU-2 Control Summary Information
Responsible Role: System Owner (SO)
Parameter AU-2(a): successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes
Parameter AU-2(c): a subset of the auditable events defined in AU-2a to be audited continually, including logon failures, privilege escalations, and policy changes
Parameter AU-2(e): annually and whenever there is a change in the threat environment
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate

AU-2 Implementation Risks
Part a: If the set of identified events is not extensive enough to cover all the critical events, it can result in incomplete logging, which will leave certain incidents undetected.
Part b: Coordinating with multiple organizational entities may slow down the process.
Part c: Continually logging events like logon failures may impact system performance, especially in high-traffic areas like customer platforms.
Part d: Without proper jurisdiction, certain critical events may be overlooked and cause problems later.
Part e: Frequently updating the logging criteria on the basis of changing threats can be very resource intensive and might lead to delayed updates.

AU-3 Content of Audit Records (L)(M)(H)

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate

AU-3 Implementation Risks
Part a: If the types of even haven't been defined clearly, it can lead to a lot of confusion during the analysis.
Part b: If events are not accurately timestamped, it can lead to hindrance during the investigation, especially in the case of different time zones.
Part c: As Tesla operates across multiple platforms and departments, it can be difficult to capture a standardized location for each event.
Part d: It can be difficult to locate the epicenter of the event because of the sheer number of systems involved and a lot of the times things happen in parallel.
Part e: Tesla's complex systems may generate multiple outcomes, making it difficult to standardize it.
Part f: Identifying all the individuals can be tough if there are third-party contractors involved. Tesla will have to rely on contractor's provided data and take their word for it.

AU-3(1) Additional Audit Information (M)(H)

Generate audit records containing the following additional information: **session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands.**

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

AU-3(1) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-3(1): session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to

diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-3(1) Implementation Risks
Logging the full text of privileged commands can increase the risk of exposing critical data, if the logs are not secured properly. This is especially important for the case of commands that contain sensitive information like credentials.

AU-4 Audit Log Storage Capacity (L)(M)(H)

Allocate audit log storage capacity to accommodate **the retention of logs for three years**.

AU-4 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-4: the retention of logs for three years
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-4 Implementation Risks
Given the data intensive nature of Tesla’s operations, it can be very costly to maintain adequate storage for three years.

AU-5 Response to Audit Logging Process Failures (L)(M)(H)

a. Alert the **System Administrators** within **20 minutes** in the event of an audit logging process failure; and

b. Take the following additional actions: **overwrite oldest record**.

AU-5 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-5(a)-1: System Administrators
Parameter AU-5(a)-2: 20 minutes
Parameter AU-5(b): overwrite oldest record
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-5 Implementation Risks
Part a: In the event of network issues, there’s a risk that the alerting system is not able to notify the Administrators within the 20 minute window.
Part b: Overwriting the oldest records can result in loss of valuable data and cause trouble during long term investigations.

AU-6 Audit Record Review, Analysis, and Reporting (L)(M)(H)

a. Review and analyze system audit records **at least weekly** for indications of **unauthorized access attempts, or unusual login patterns** and the potential impact of the inappropriate or unusual activity;

b. Report findings to **Chief Information Security Officer (CISO)**; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

AU-6 Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Parameter AU-6(a)-1: at least weekly
Parameter AU-6(a)-2: unauthorized access attempts, or unusual login patterns
Parameter AU-6(b): Chief Information Security Officer (CISO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-6 Implementation Risks
Part a: Reviewing records only once per week can lead to delays in identifying unauthorized access that might have occurred shortly after a review.
Part b: Any delays in sharing the findings with the CISO can impact Tesla's ability to take quick actions and lead to potential threats.
Part c: Adjusting audit levels may require coordination across various departments, which can lead to potential delays.

AU-6(1) Automated Process Integration (M)(H)

Integrate audit record review, analysis, and reporting processes using **automated mechanisms such as anomaly detection tools, and automated alerting systems**.

AU-6(1) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-6(1): automated mechanisms such as anomaly detection tools, and automated alerting systems
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-6(1) Implementation Risks
The anomaly detection tools may lead to a lot of false positives, which can lead to unnecessary alerts.

AU-6(3) Correlate Audit Record Repositories (M)(H)

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6(3) Control Summary Information
Responsible Role: Security Operations Center (SOC) Analyst
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-6(3) Implementation Risks
The audit records across different repositories might be using various formats, which can complicate the process and also lead to data inconsistencies.

AU-7 Audit Record Reduction and Report Generation (M)(H)

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

AU-7 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-7 Implementation Risks
Part a: Performing the on-demand analysis of a large volume of audit records might require a lot of processing power. If the configuration is not able to support it, it can lead to system shutdowns.
Part b: If the report generation process is not implemented properly, there is a risk of altering the original audit records.

AU-7(1) Automatic Processing (M)(H)

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: **timestamp, user ID, and IP address**.

AU-7(1) Control Summary Information

Responsible Role: System Administrator (SA)
Parameter AU-7(1): timestamp, user ID, and IP address
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

AU-7(1) Implementation Risks
As Tesla might have a vast amount of audit data being generated daily, processing all of it can lead to data overload.

AU-8 Time Stamps (L)(M)(H)

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet **one second granularity of time measurement** and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-8 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-8(b): one second granularity of time measurement
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-8 Implementation Risks
Part a: There’s a possibility of the internal system clocks suffering from time drift, which can result in inaccurate timestamps for audit records.
Part b: If different time zones are used inconsistently in the time stamps, it can lead to confusion when comparing logs from systems in different locations.

AU-9 Protection of Audit Information (L)(M)(H)

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert the **System Administrators** upon detection of unauthorized access, modification, or deletion of audit information.

AU-9 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-9(b): System Administrators
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-9 Implementation Risks
Part a: Accidental deletion of audit logs can result in data loss, which can hinder Tesla’s future investigations that might have required those logs.
Part b: If the alerts are delayed, it can lead to potential escalation of security issues.

AU-9(4) Access by Subset of Privileged Users (M)(H)

Authorize access to management of audit logging functionality to only **senior System Administrators**.

AU-9(4) Control Summary Information
Responsible Role: Senior System Administrator
Parameter AU-9(4): Senior System Administrators
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-9(4) Implementation Risks
Even among the senior System Administrators, there is a risk of insider threat, meaning a privileged user might misuse their access to do some harm.

AU-11 Audit Record Retention (L)(M)(H)

Retain audit records **for a minimum of 7 years, which exceeds the compliance requirements of M-21-31,** to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Guidance: The service provider is encouraged to align with M-21-31 where possible

Requirement: The service provider retains audit records on-line for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf)

AU-11 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-11: for a minimum of 7 years, which exceeds the compliance requirements of M-21-31

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-11 Implementation Risks
Retaining the records for a minimum of 7 years will require a significant amount of storage, considering the fact that Tesla's operations are very data-intensive.

AU-12 Audit Record Generation (L)(M)(H)

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on **all information system and network components where audit capability is deployed/available**;

b. Allow **System Administrators** to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

AU-12 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter AU-12(a): all information system and network components where audit capability is deployed/available
Parameter AU-12(b): System Administrators
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

AU-12 Implementation Risks
Part a: Integrating audit logs across all components might be challenging because Tesla has a diverse number of systems and departments.
Part b: The System Administrators might misconfigure the event types mistakenly.
Part c: If the generated records don't contain all the required content as specified in AU-3, it can lead to gaps in the future incident investigations.

Assessment, Authorization, and Monitoring

CA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **Tesla's Compliance and Risk Management Team**:

   1. **Organization-level** assessment, authorization, and monitoring policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an **Chief Information Security Officer** to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

   1. Policy **at least every three (3) years** and following **major organizational events which include new product launches like Tesla's AI-driven Optimus robots at the We, Robot event, restructuring of organizational hierarchy and changes in regulations**; and

   2. Procedures **at least annually** and following **significant changes such as new software implementations or infrastructure upgrades**.

CA-1 Control Summary Information
Responsible Role: Chief Compliance Officer & Compliance and Risk Management Team

Parameter CA-1(a): Tesla's Compliance and Risk Management Team
Parameter CA-1(a)(1): Organization-level
Parameter CA-1(b): Chief Information Security Officer
Parameter CA-1(c)(1)-1: at least every three (3) years
Parameter CA-1(c)(1)-2: major organizational events which include new product launches like Tesla's AI-driven Optimus robots at the We, Robot Event, restructuring of organizational hierarchy and changes in regulations
Parameter CA-1(c)(2)-1: at least annually
Parameter CA-1(c)(2)-2: significant changes such as new software implementations or infrastructure upgrades
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-1 Implementation Risks
Part a: Engaging stakeholders in the policy formulation process is essential; failing to do so will lead to policies that overlook critical operational needs and compliance mandates.
Part b: When a CEO and CISO disagree, implementing controls becomes challenging. Therefore, it's essential for the CISO to have strategic planning authority in the security department.
Part c: Neglecting to update policies and procedures can result in outdated practices that don't align with current threats or regulations.

CA-2 Control Assessments (L)(M)(H)

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;
2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation **at least annually** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to **Tesla's executive leadership, FedRAMP PMO, and other regulatory bodies as required**.

CA-2 Additional FedRAMP Requirements and Guidance:

Guidance: Reference FedRAMP Annual Assessment Guidance.

CA-2 Control Summary Information
Responsible Role: Chief Compliance Officer
Parameter CA-2(d): at least annually
Parameter CA-2(f): Tesla's executive leadership, FedRAMP PMO, and other regulatory bodies as required
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-2 Implementation Risks
Part a: Selecting inappropriate assessors for an assessment can result in incomplete evaluations and overlooked critical controls.

Part b: Risks include not clearly outlining the controls and procedures for assessment, which can lead to ineffective evaluations.
Part c: Delays in obtaining approval from multiple layers could postpone assessments.
Part d: CA-2 requires annual assessments, and neglecting this due to resource issues or oversight could expose Tesla to security risks.
Part e: A control assessment report lacking detail may hinder informed decisions about compliance and improvements.
Part f: If control assessment results aren't properly shared in a timely manner with key individuals, including the FedRAMP PMO, it may lead to a lack of awareness about compliance issues and necessary actions for resolution.

CA-2(1) Independent Assessors (L)(M)(H)

Employ independent assessors or assessment teams to conduct control assessments.

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited 3PAO.

CA-2(1) Control Summary Information
Responsible Role: Chief Compliance Officer
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-2(1) Implementation Risks
Not using an accredited 3PAO could prevent Tesla from obtaining FedRAMP JAB authorization. Additionally, there's a risk of conflicts of interest if assessors have prior ties to Tesla or are involved with the assessed systems, potentially compromising assessment objectivity.

CA-2(3) Leveraging Results from External Organizations (M)(H)

Leverage the results of control assessments performed by **any FedRAMP Accredited 3PAO** on **critical cloud systems and IT infrastructure** when the assessment meets **Tesla's internal control effectiveness criteria and adhere to regulatory frameworks such as FedRAMP Moderate or High baselines.**

CA-2(3) Control Summary Information
Responsible Role: Information Security Officer & Compliance and Risk Management Team
Parameter CA-2(3)-1: any FedRAMP Accredited 3PAO
Parameter CA-2(3)-2: critical cloud systems and IT infrastructure
Parameter CA-2(3)-3: Tesla's internal control effectiveness criteria and adhere to regulatory frameworks such as FedRAMP Moderate or High baselines.
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-2(3) Implementation Risks
An outsider cannot understand your house's layout better than you. Relying too much on external assessments can lead to complacency in Tesla's internal evaluations. If Tesla depends solely on these assessments, it risks missing vital insights into its security and compliance status.

CA-3 Information Exchange (L)(M)(H)

a. Approve and manage the exchange of information between the system and other systems using **interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements**;

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements **at least annually and on input from JAB/AO**.

CA-3 Control Summary Information
Responsible Role: Information Security Officer
Parameter CA-3(a): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements
Parameter CA-3(c): at least annually and on input from JAB/AO
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-3 Implementation Risks
Part a: One risk in managing information exchange agreements is inadequate approval processes, which can lead to unauthorized exchanges of sensitive information. Without thorough vetting or standardized procedures, security weaknesses and compliance failures may occur.
Part b: The main risk of documentation lies in incomplete or unclear agreements that do not specify interface characteristics, security requirements, and responsibilities. These deficiencies can lead to misunderstandings or breaches, resulting in data leaks or vulnerabilities.
Part c: Delays in reviewing and updating information exchange agreements pose risks to Tesla as any changes in regulations or technology could lead to security or compliance gaps if agreements aren't regularly reassessed.

CA-5 Plan of Action and Milestones (L)(M)(H)

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones **at least monthly** based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Guidance: Reference FedRAMP-POAM-Template.

Requirement: POA&Ms must be provided at least monthly.

CA-5 Control Summary Information
Responsible Role: Chief Compliance Officer & Compliance and Risk Management Team
Parameter CA-5(b): at least monthly
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-5 Implementation Risks
Part a: Inadequate documentation of vulnerabilities and remediation actions in the POA&M can lead to prolonged security risks and confusion about implementation responsibilities. Misidentified weaknesses may result in ineffective remediation, jeopardizing system security.
Part b: Frequent updates to the POA&M pose risks, like delays in incorporating assessment findings. If updates are not timely, Tesla may rely on outdated information, negatively impacting its compliance posture.

CA-6 Authorization (L)(M)(H)

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations **in accordance with OMB A-130 requirements or when a significant change occurs which include updates to Gigafactory control systems, EV Supercharger software, or AI-integrated manufacturing processes**.

CA-6 Additional FedRAMP Requirements and Guidance:

(e) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

CA-6 Control Summary Information
Responsible Role: Chief Compliance Officer
Parameter CA-6(e): in accordance with OMB A-130 requirements or when a significant change occurs which include updates to Gigafactory control systems, EV Supercharger software, or AI-integrated manufacturing processes
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-6 Implementation Risks
Part a: If the appointed senior official lacks the necessary authority or experience in system security management, it can compromise the authorization process and increase risk exposure. Inefficient communication with other departments may also hinder decision-making, leading to misunderstandings and delays in addressing cybersecurity concerns.

Part b: An authorizing official may lack understanding of the functions and importance of common controls for inheritance, leading to underutilization of security measures.
Part c: If the inherited controls are not properly assessed its broader nature might miss out on addressing a few security issues which would need system specific controls.
Part d: If the authorizations happen over the internet or through portals there are possibilities of hacker targeting those portals to mislead the organization without being noticed.
Part e: Failing to comply with OMB A-130 requirements will lead to heightened scrutiny from regulators and adversely affect operational capabilities.

CA-7 Continuous Monitoring (L)(M)(H)

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: **organization-defined system-level metrics like solar power efficiency, EV Supercharger uptime, AI performance (e.g., Optimus Gen 3), network latency, and cybersecurity incident frequency**;

b. Establishing **organization-defined frequencies to be on a daily basis** for monitoring and **organization-defined frequencies to be on a monthly basis** for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to **Tesla's executive leadership, external stakeholders and JAB/AO on a monthly basis.**

CA-7 Additional FedRAMP Requirements and Guidance:

Guidance: FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan.

Requirement: Operating System, Database, Web Application, Container, and Service Configuration Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Requirement: CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (Con Mon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing Con Mon oversight. It does not apply to CSPs authorized via the JAB path because the JAB performs Con Mon oversight.

CA-7 Control Summary Information
Responsible Role: Chief Information Security Officer
Parameter CA-7(a): organization-defined system-level metrics like solar power efficiency, EV Supercharger uptime, AI performance (e.g., Optimus Gen 3), network latency, and cybersecurity incident frequency
Parameter CA-7(b)-1: organization-defined frequencies to be on a daily basis
Parameter CA-7(b)-2: organization-defined frequencies to be on a monthly basis
Parameter CA-7(g)-1: Tesla’s executive leadership, external stakeholders and JAB/AO
Parameter CA-7(g)-2: on a monthly basis
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-7 Implementation Risks
Part a: If system-level metrics selected don’t align with Tesla's operational needs, critical security concerns may go overlooked.

Part b: Excessive monitoring can strain resources, distract from critical areas, and lead to operational fatigue among security personnel, reducing their effectiveness in handling security incidents.
Part c: Security environments are always changing. If assessments do not adjust to new threats, some vulnerabilities may remain hidden. This increases the risk of successful cyber incidents.
Part d: Malicious actors can hack into the monitoring systems and gather data about the Optimus robot and execute data poisoning on the training data.
Part e: If the collected data is not comprehensively converted into insights then its just data which is of no use. Therefore, absence of quicker analytical tools would increase would slow down the process identification of key factors.
Part f: Inadequate prioritization of response actions for vulnerabilities can result in ongoing security issues. If Tesla neglects high-risk areas, it may face greater costs later. Additionally, the lack of training exacerbates the problem.
Part g: If the reports are not submitted on time there might be compliance violations resulting in fines. In addition, inconsistent reporting formats or insufficient data can hinder the JAB/AO's ability to make informed decisions about security risks and compliance.

CA-7(1) Independent Assessment (M)(H)

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7(1) Control Summary Information
Responsible Role: Chief Information Security Officer
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-7(1) Implementation Risks

Tesla faces risks in securing competent independent assessors knowledgeable in electric vehicle technologies and operational challenges, which could impact the effectiveness of assessments. Additionally, poor data accuracy from monitoring systems may further compromise assessment outcomes.

CA-7(4) Risk Monitoring (L)(M)(H)

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

CA-7(4) Control Summary Information
Responsible Role: Chief Risk Officer
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-7(4) Implementation Risks
Part a: A key risk in effectiveness monitoring is failing to identify metrics that accurately reflect Tesla's security posture. Inadequate metrics can create false confidence in security controls, allowing undetected vulnerabilities to remain.
Part b: Tesla must navigate a rapidly changing regulatory environment concerning data protection and automotive safety. Non-compliance could lead to fines, operational restrictions, or reputational harm. The recent EU AI Act adds to these risks, especially for AI-based robots.
Part c: Tesla's interconnected systems pose challenges for change monitoring, as modifications in one area can unintentionally affect others, leading to unforeseen vulnerabilities. Limited

	visibility into these interdependencies can impede effective risk assessment and management.

CA-8 Penetration Testing (L)(M)(H)

Conduct penetration testing **at least annually** on **web and mobile applications, vehicles and their embedded systems, cloud infrastructure, and communication protocols like OTA updates and V2X communications. Other critical areas include IoT devices like Powerwall, physical security systems (e.g., key fobs, NFC), and internal IT infrastructure, including corporate networks and Active Directory. Additionally, Tesla’s AI and autonomous systems for adversarial attacks, supply chain security, data management practices, Tesla’s energy products and supercharger networks in penetration testing scope.**

CA-8 Additional FedRAMP Requirements and Guidance:

Guidance: Reference the FedRAMP Penetration Test Guidance.

CA-8 Control Summary Information
Responsible Role: Chief Information Security Officer & Security Operations Center (SOC) Team
Parameter CA-8-1: at least annually
Parameter CA-8-2: web and mobile applications, vehicles and their embedded systems, cloud infrastructure, and communication protocols like OTA updates and V2X communications. Other critical areas include IoT devices like Powerwall, physical security systems (e.g., key fobs, NFC), and internal IT infrastructure, including corporate networks and Active Directory. Additionally, Tesla’s AI and autonomous systems for adversarial attacks, supply chain security, data management practices, Tesla’s energy products and supercharger networks in penetration testing scope.
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-8 Implementation Risks

Penetration testing on live systems can disrupt operations, particularly in energy grids or autonomous vehicles. It's challenging to cover all use cases, as we need to adopt an attacker's mindset using minimal tools. Finding personnel with this perspective is difficult. Lastly, the boom in AI has increased the threat landscape to adversarial AI attacks and data poisoning.

CA-8(1) Independent Penetration Testing Agent or Team (M)(H)

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

CA-8(1) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-8(1) Implementation Risks
Allowing an independent penetration testing team access to Tesla's systems raises concerns about potential misuse of sensitive data, risking data breaches or leaks that could impact customer privacy and intellectual property.

CA-8(2) Red Team Exercises (M)(H)

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: **simulate attacks on energy grids, test the ability to manipulate the autopilo algorithms for autonomous vehicles, have adversarial AI and data poisoning attack Optimus robots, simulating breaches in Tesla's telemetry and control systems hosted in cloud environments.**

CA-8(2) Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page > Penetration Test Guidance https://www.FedRAMP.gov/documents/.

CA-8(2) Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter CA-8(2): simulate attacks on energy grids, test the ability to manipulate the autopilo algorithms for autonomous vehicles, have adversarial AI and data poisoning attack Optimus robots, simulating breaches in Tesla's telemetry and control systems hosted in cloud environments..
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-8(2) Implementation Risks
Some attacks cannot be simulated, making it difficult to understand and defend against them. Additionally, if testing leads to data leaks, the organization may incur fines.

CA-9 Internal System Connections (L)(M)(H)

a. Authorize internal connections of **Optimus Gen 3 robots, Tesla Vision, and AI technologies connected to centralized databases; Autopilot and Full Self-Driving (FSD) modules linked to Tesla Cloud for data updates; factory automation systems like PLCs and SCADA integrated with Tesla's production management** to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after **system decommissioning; detection of persistent vulnerabilities; breaches of internal policy**.; and

d. Review **at least annually** the continued need for each internal connection.

CA-9 Control Summary Information
Responsible Role: Information Security Officer (ISO)

Parameter CA-9(a): Optimus Gen 3 robots, Tesla Vision, and AI technologies connected to centralized databases; Autopilot and Full Self-Driving (FSD) modules linked to Tesla Cloud for data updates; factory automation systems like PLCs and SCADA integrated with Tesla’s production management
Parameter CA-9(c): system decommissioning; detection of persistent vulnerabilities; breaches of internal policy
Parameter CA-9(d): at least annually
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CA-9 Implementation Risks
Part a: Unauthorized or unvetted connections will undoubtedly introduce vulnerabilities.
Part b: Documenting interface characteristics and security requirements for internal connections carries significant risks. Incomplete documentation can cause misunderstandings about data transmission and protection, potentially exposing sensitive information. Additionally, lacking comprehensive records makes it challenging to track security implications, hindering the implementation of necessary safeguards against breaches.
Part c: Poorly defined or enforced conditions can delay the termination of inactive connections, risking exploitation of outdated systems.
Part d: A lack of clear guidelines in the review process may result in unnecessary connections being deemed essential, increasing risk in the infrastructure. In Tesla's fast-paced environment, oversight during reviews could lead to significant gaps in risk management.

Contingency Planning

CP-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **IT personnel, risk management team members, system administrators, and department heads**:

   1. **Organization-level; mission/business process-level; system-level** contingency planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an **Contingency Planning Manager** to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

   1. Policy **at least every three (3) years** and following **Security incidents or breaches, Audit findings, Changes in regulatory or legal requirements, Organizational restructuring**; and

   2. Procedures **annually** and following **significant changes include new technology being introduced, organization restructuring**.

CP-1 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-1(a): **IT personnel, risk management team members, system administrators, and department heads**
Parameter CP-1(a)(1): **Organization-level; mission/business process-level; system-level**
Parameter CP-1(b): **Contingency Planning Manager**
Parameter CP-1(c)(1)-1: **at least every three (3) years**

Parameter CP-1(c)(1)-2: **Security incidents or breaches, Audit findings, Changes in regulatory or legal requirements, Organizational restructuring**
Parameter CP-1(c)(2)-1: **annually**
Parameter CP-1(c)(2)-2: **significant changes include new technology being introduced, organization restructuring**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-1 Implementation Risks
Part a: Documenting can be complex, and inconsistencies or gaps in documentation can lead to ineffective contingency planning.
Part b: Ensuring that contingency planning policies are consistent with all relevant laws, regulations, and standards may be challenging due to the frequent updates.
Part c: Reviewing and updating policies every three years can be resource-intensive.

CP-2 Contingency Plan (L)(M)(H)

a. Develop a contingency plan for the system that:

  1. Identifies essential mission and business functions and associated contingency requirements;
  2. Provides recovery objectives, restoration priorities, and metrics;
  3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by **Chief Information Security Officer (CISO)**;

b. Distribute copies of the contingency plan to **department heads, incident response team, and business continuity team**;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system **annually**;

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to **Chief Information Security Officer (CISO), department heads, incident response team, and business continuity team**;

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

Requirement: CSPs must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-G-Information-System-Contingency-Plan-(ISCP)-Template.docx).

CP-2 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-2(a)(7): **Chief Information Security Officer (CISO)**
Parameter CP-2(b): **department heads, incident response team, and business continuity team**

Parameter CP-2(d): **annually**
Parameter CP-2(f): **Chief Information Security Officer (CISO), department heads, incident response team, and business continuity team**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-2 Implementation Risks
Part a: Failing to accurately identify all critical functions can lead to gaps in recovery
Part b: Unauthorized access to distributed copies could lead to data leaks.
Part c: Misalignment between contingency and incident response plans may lead to conflicting actions.
Part d: Neglecting updates or thorough reviews may render the plan ineffective over time.
Part e: Failure to capture organizational, system, or operational changes may leave gaps in the plan.
Part f: Delayed or incomplete communication may lead to relying on outdated information.
Part g: Ignoring lessons learned may perpetuate previous mistakes or inefficiencies.
Part h: Weak access controls or accidental sharing may expose sensitive information.

CP-2(1) Coordinate with Related Plans (M)(H)

Coordinate contingency plan development with organizational elements responsible for related plans.

CP-2(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status: ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

CP-2(1) Implementation Risks
If there is no schedule during coordination that could have adverse effects and cause inefficiencies.

CP-2(3) Resume Mission and Business Functions (M)(H)

Plan for the resumption of **all** mission and business functions within **24 hours, or another time period based on Tesla's SLA with customers and internal requirements** of contingency plan activation.

CP-2(3) Control Summary Information
Responsible Role: **Business Continuity Manager**
Parameter CP-2(3)-1: **all**
Parameter CP-2(3)-2: **24 hours, or another time period based on Tesla's SLA with customers and internal requirements**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

CP-2(3) Implementation Risks
Inadequate resources could delay recovery efforts within the required timeframe.

CP-2(8) Identify Critical Assets (M)(H)

Identify critical system assets supporting **all; essential** mission and business functions.

CP-2(8) Control Summary Information
Responsible Role: **Contingency Planning Manager**

Parameter CP-2(8): **all; essential**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-2(8) Implementation Risks
Misclassifying critical assets can lead to gaps in the contingency plan which could cause disruptions in the future.

CP-3 Contingency Training (L)(M)(H)

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within ***See Additional Requirements** of assuming a contingency role or responsibility;
2. When required by system changes; and
3. **Annually** thereafter; and

b. Review and update contingency training content **annually** and following **annual review, major security incidents, regulatory changes, technology or infrastructure updates, audit findings & business process changes.**

.

CP-3 Additional FedRAMP Requirements and Guidance:

(a) Requirement: Privileged admins and engineers must take the basic contingency training within ten (10) days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within sixty (60) days of hire date when the training will have more impact.

CP-3 Control Summary Information

Responsible Role: **Contingency Planning Manager**
Parameter CP-3(a)(1): ***See Additional Requirements**
Parameter CP-3(a)(3): **Annually**
Parameter CP-3(b)-1: **annually**
Parameter CP-3(b)-2: **annual review, major security incidents, regulatory changes, technology or infrastructure updates, audit findings & business process changes.**
Implementation Status: ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

CP-3 Implementation Risks
Part a: Delayed or incomplete training for newly assigned roles can leave the company unprepared during an emergency.
Part b: Missing updates due to major incidents, audits, or process changes could leave training irrelevant or incomplete.

CP-4 Contingency Plan Testing (L)(M)(H)

a. Test the contingency plan for the system **annually** using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: **Functional exercises include simulating emergency scenarios involving live environment but limited scope, allowing participants to practice executing parts of the contingency plan.**

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

CP-4 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the JAB/AO prior to initiating testing.

(a) Requirement: The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report).

CP-4 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-4(a)-1: **annually**
Parameter CP-4(a)-2: **Functional exercises include simulating emergency scenarios involving live environment but limited scope, allowing participants to practice executing parts of the contingency plan.**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-4 Implementation Risks
Part a: Testing in a live environment could unintentionally disrupt operations or expose sensitive data.
Part b: Incomplete or biased reviews might overlook critical gaps or missteps in the plan.
Part c: Delays in implementing corrective actions might leave vulnerabilities unaddressed.

CP-4(1) Coordinate with Related Plans (M)(H)

Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-4(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status: ☐ Partially Implemented

Control Origination: ☐ Service Provider Corporate

CP-4(1) Implementation Risks
Lack of synchronization between related plans could result in conflicting actions during testing, causing confusion and inefficiencies.

CP-6 Alternate Storage Site (M)(H)

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

CP-6 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-6 Implementation Risks
Part a: Failure to establish or maintain agreements with the alternate storage site could result in delays or inability to access backup data during an emergency.
Part b: Disparity in security controls between sites may expose backups to unauthorized access or data breaches.

CP-6(1) Separation from Primary Site (M)(H)

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-6(1) Implementation Risks
The alternate storage site may not be far enough from the primary site, making it vulnerable to the same threats

CP-6(3) Accessibility (M)(H)

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-6(3) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

CP-6(3) Implementation Risks
Transportation or communication issues may prevent timely access to the alternate storage site during a disaster.

CP-7 Alternate Processing Site (M)(H)

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of **data security system and cybersecurity monitoring system** for essential mission and business functions within **2 weeks** when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

CP-7 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

CP-7 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-7(a)-1: **data security system and cybersecurity monitoring system**
Parameter CP-7(a)-2: **2 weeks**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Shared (Service Provider and Customer Responsibility)

CP-7 Implementation Risks

Part a: Delays in establishing agreements with the alternate site could hinder transfer and resumption of operations during an emergency.
Part b: Unavailability in providing necessary equipment and supplies at the alternate site may disrupt operations.
Part c: The alternate site may lack equivalent security increasing vulnerability to data breaches or operational inefficiencies.

CP-7(1) Separation from Primary Site (M)(H)

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (1) Additional FedRAMP Requirements and Guidance:

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant.

CP-7(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Shared (Service Provider and Customer Responsibility)

CP-7(1) Implementation Risks
Insufficient geographic separation between the primary and alternate sites can result in failure.

CP-7(2) Accessibility (M)(H)

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7(2) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

CP-7(2) Implementation Risks
Uncharacteristic natural disasters cannot be predicted so there might not be a mitigation plan for that particular disaster.

CP-7(3) Priority of Service (M)(H)

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-7(3) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply):

☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-7(3) Implementation Risks
The alternate site provider may have competing obligations to other clients during a widespread disruption.

CP-8 Telecommunications Services (M)(H)

Establish alternate telecommunications services, including necessary agreements to permit the resumption of **Slack or Microsoft Teams** for essential mission and business functions within **5 hours** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

CP-8 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-8-1: **Slack or Microsoft Teams**
Parameter CP-8-2: **5 hours**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-8 Implementation Risks
In case of a natural disaster, internet services may be down to the degree where video class might not be possible.

CP-8(1) Priority of Service Provisions (M)(H)

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-8(1) Implementation Risks
Part a: During widespread emergencies, providers may face resource constraints.
Part b: The process of obtaining TSP designation from authorities may take longer than expected.

CP-8(2) Single Points of Failure (M)(H)

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8(2) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-8(2) Implementation Risks
If the alternate services are owned by the same company and if their servers go down then the primary and alternate telecommunication services would also be down.

CP-9 System Backup (L)(M)(H)

a. Conduct backups of user-level information contained in **user files, application data, and user-created configurations daily incremental; weekly full**;

b. Conduct backups of system-level information contained in the system **daily incremental; weekly full**;

c. Conduct backups of system documentation, including security- and privacy-related documentation **daily incremental; weekly full**; and

d. Protect the confidentiality, integrity, and availability of backup information.

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

(a) Requirement: The service provider maintains at least three (3) backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative.

(b) Requirement: The service provider maintains at least three (3) backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative.

(c) Requirement: The service provider maintains at least three (3) backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.

CP-9 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-9(a)-1: **user files, application data, and user-created configurations, daily incremental; weekly full**
Parameter CP-9(a)-2: **daily incremental; weekly full**;
Parameter CP-9(b): **daily incremental; weekly full**;
Parameter CP-9(c):
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-9 Implementation Risks
Part a: Incomplete or missed backups due to system misconfigurations or user files stored outside designated directories could lead to data loss.
Part b: Backup operations might consume significant system resources, impacting live operations.
Part c: Changes to system documentation may not be captured in backups if not updated promptly.

Part d: Lack of encryption could lead to data breaches or malicious alterations.

CP-9(1) Testing for Reliability and Integrity (M)(H)

Test backup information **at least annually** to verify media reliability and information integrity.

CP-9(1) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-9(1): **at least annually**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-9(1) Implementation Risks
Failure to conduct or properly execute tests might result in undetected backup failures until an actual disaster occurs.

CP-9(8) Cryptographic Protection (M)(H)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of **all backup files**.

CP-9 (8) Additional FedRAMP Requirements and Guidance:

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or National Security Agency (NSA) approved cryptography (see SC-13).

CP-9(8) Control Summary Information
Responsible Role: **Contingency Planning Manager**

Parameter CP-9(8): **all backup files**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-9(8) Implementation Risks
Improperly implemented encryption may leave backups vulnerable to unauthorized access or tampering.

CP-10 System Recovery and Reconstitution (L)(M)(H)

Provide for the recovery and reconstitution of the system to a known state within **8 hours** after a disruption, compromise, or failure.

CP-10 Control Summary Information
Responsible Role: **Contingency Planning Manager**
Parameter CP-10: **8 hours**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

CP-10 Implementation Risks
Dependencies, such as third-party services may not be identified or prioritized correctly.

CP-10(2) Transaction Recovery (M)(H)

Implement transaction recovery for systems that are transaction-based.

CP-10(2) Control Summary Information
Responsible Role: **Contingency Planning Manager**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Shared (Service Provider and Customer Responsibility)

CP-10(2) Implementation Risks
Failure to implement reliable transaction recovery mechanisms could result in partial or missing data.

Identification and Authentication

IA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **Tesla’s Security Team and System Administrators**:

1. **System-level** identification and authentication policy that:

   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate the **Chief Information Security Officer (CISO)** to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy **at least every 3 years** and following **a major policy or regulatory changes, or significant upgrades**; and

2. Procedures **at least annually** and following **significant changes**.

IA-1 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter IA-1(a): Tesla’s Security Team and System Administrators
Parameter IA-1(a)(1): System-level
Parameter IA-1(b): Chief Information Security Officer (CISO)
Parameter IA-1(c)(1)-1: At least every 3 years
Parameter IA-1(c)(1)-2: A major policy or regulatory changes, or significant upgrades
Parameter IA-1(c)(2)-1: At least annually
Parameter IA-1(c)(2)-2: Significant changes
Implementation Status : ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-1 Implementation Risks

Part a: If the scope of the policies don't cover all the necessary elements, it can lead to gaps in Tesla's IA approach.
Part b: If the CISO is not actively involved in managing the policy, it can lead to gaps in accountability.
Part c: Regular updates might require a lot of time and resources, which can lead to potential delays.

IA-2 Identification and Authentication (Organizational Users) (L)(M)(H)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-2 Additional FedRAMP Requirements and Guidance:

Guidance: "Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

Requirement: For all control enhancements that specify multifactor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B.

Requirement: Multi-factor authentication must be phishing-resistant.

Requirement: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate.

IA-2 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-2 Implementation Risks

If the system allows users to have shared user identifiers, it can become difficult to track actions of a specific user.

IA-2(1) Multi-factor Authentication to Privileged Accounts (L)(M)(H)

Implement multi-factor authentication for access to privileged accounts.

IA-2 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2(1) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status: ☐ Partially Implemented
Control Origination ☐ Service Provider Corporate

IA-2(1) Implementation Risks
If the multi-factor authentication is not implemented across all the privileged accounts, some accounts may still remain vulnerable to unauthorized access.

IA-2(2) Multi-factor Authentication to Non-privileged Accounts (L)(M)(H)

Implement multi-factor authentication for access to non-privileged accounts.

IA-2 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2(2) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-2(2) Implementation Risks
If the multi-factor authentication is not implemented across all the non-privileged accounts, some accounts may still remain vulnerable to unauthorized access.

IA-2(5) Individual Authentication with Group Authentication (M)(H)

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

IA-2(5) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-2(5) Implementation Risks

Requiring users to be individually authenticated before granting access to the shared accounts or resources might increase the number of authentication steps, which can lead to delays and frustration among users.

IA-2(6) Access to Accounts —separate Device (M)(H)

Implement multi-factor authentication for **local, network and remote** access to **privileged accounts and non-privileged accounts such that**:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets **FIPS-validated or NSA-approved cryptography**.

IA-2 (6) Additional FedRAMP Requirements and Guidance:

Guidance: PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.

Guidance: See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.

IA-2(6) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-2(6)-1: local, network and remote
Parameter IA-2(6)-2: privileged accounts and non-privileged accounts
Parameter IA-2(6)(b): FIPS-validated or NSA-approved cryptography
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

IA-2(6) Implementation Risks
Part a: If the user misplaces their authentication device, it can lead to potential delays in accessing the critical systems.

Part b: Making the device meet FIPS-validated or NSA-approved cryptography can be complex and might require specialized knowledge.

IA-2(8) Access to Accounts — Replay Resistant (L)(M)(H)

Implement replay-resistant authentication mechanisms for access to **privileged accounts and non-privileged accounts**.

IA-2(8) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-2(8): privileged accounts and non-privileged accounts
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-2(8) Implementation Risks
Some legacy systems in Tesla's environment may not be compatible with the replay-resistant authentication mechanisms.

IA-2(12) Acceptance of PIV Credentials (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

IA-2(12) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status: ☐ Partially Implemented

Control Origination: ☐ Service Provider Corporate

IA-2(12) Implementation Risks
If Tesla’s Personal Identity Verification faces any downtime, the employees may not be able to authenticate, which can affect their access to critical systems.

IA-3 Device Identification and Authentication (M)(H)

Uniquely identify and authenticate **all company-issued laptops and mobile devices** before establishing a **network** connection.

IA-3 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-3-1: all company-issued laptops and mobile devices
Parameter IA-3-2: network
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-3 Implementation Risks
If some company-issued laptops are not properly registered, they may not be uniquely identified, which can lead to gaps in security.

IA-4 Identifier Management (L)(M)(H)

Manage system identifiers by:

a. Receiving authorization from the **Information System Security Officer (ISSO)** to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for **at least two (2) years**.

IA-4 Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Parameter IA-4(a): Information System Security Officer
Parameter IA-4(d): at least two (2) years
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-4 Implementation Risks
Part a: If there are any delays in receiving ISSO authorization, it can slow down the process of granting access to new users and devices.
Part b: Different systems and departments in Tesla might mistakenly use different identifier formats, which can lead to a lot of inconsistencies.
Part c: If identifiers are reassigned without any proper oversight, it can lead to improper access and potential breaches.
Part d: Within systems that use frequent assignments, preventing reuse of identifiers for two years may lead to exhaustion of the identifier pool.

IA-4(4) Identify User Status (M)(H)

Manage individual identifiers by uniquely identifying each individual as **contractors and foreign nationals**.

IA-4(4) Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Parameter IA-4(4): contractors and foreign nationals
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-4(4) Implementation Risks
If the status of contractors and foreign nations is not frequently updated, Tesla may have outdated records, which can potentially lead to unauthorized access.

IA-5 Authenticator Management (L)(M)(H)

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators **every 90 days for passwords, annually for security tokens**, or **immediately when a security breach or suspected compromise occurs**;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

Guidance: SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE).

Requirement: Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 2. Link https://pages.nist.gov/800-63-3.

IA-5 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-5(f)-1: every 90 days for passwords, annually for security tokens
Parameter IA-5(f)-2: immediately when a security breach or suspected compromise occurs
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-5 Implementation Risks
Part a: If the verification process is insufficient, unauthorized users might gain access to authenticators, which can pose a security risk.
Part b: Initial authenticators might be weak, which can increase vulnerability to unauthorized access.
Part c: The metric of sufficient strength of mechanism isn’t specified. It may result in weak authenticators that may not be able to provide adequate protection.
Part d: Any delays in replacing compromised authenticators can expose Tesla to security risks.
Part e: If the default authenticators are accidentally not changed prior to the first use, they may be exploited by attackers who can guess them.

Part f: If there’s a delay in identifying the security breach, Tesla will remain very vulnerable till it is identified and the authenticators are consequently changed.
Part g: Inadequate protection of the authenticators may lead them to be intercepted and accessed by attackers.
Part h: A user may fail to follow specific controls, which can result in the authenticators being compromised.
Part i: Any delays in updating authenticators when the membership of accounts change can potentially lead to unauthorized access of authenticators, as former members may retain access to group or role accounts.

IA-5(1) Password-based Authentication (L)(M)(H)

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list **every 45 days** and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: **Tesla requires passwords to be at least 12 characters, containing a mix of uppercase, lowercase, numbers, and special characters**.

IA-5 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13).

Requirement: Password policies must be compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or One-Time-Passwords (OTP). Password policies shall not enforce special character or minimum password rotation requirements for memorized secrets of users.

(h) Requirement: For cases where technology doesn't allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters.

For emergency use accounts, these rules should be enforced: must have a minimum length of 14 characters, must support all printable ASCII characters, and passwords must be changed if used.

IA-5(1) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-5(1)(a): every 45 days
Parameter IA-5(1)(h): Tesla requires passwords to be at least 12 characters, containing a mix of uppercase, lowercase, numbers, and special characters
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-5(1) Implementation Risks
Part a: If the list of compromised passwords isn't updated regularly, users may still be choosing vulnerable passwords, which increases the risk of unauthorized access.
Part b: If the verification process is not configured properly, it might lead to expected passwords passing the check, which can increase the security risk.

Part c: Outdated protocols in cryptographic methods can leave the passwords vulnerable to interception despite the encryption.
Part d: Even with proper hashing, the attackers can crack the hash and obtain the passwords if they have enough computational power.
Part e: If the recovery channel itself is compromised, like the email of the user, the attack can initiate account recovery and gain access before the user even gets a chance to set a new password.
Part f: Users may utilize common passphrases, which makes them vulnerable despite their length.
Part g: The presence of suggestion tools doesn't guarantee that the user will use them. Instead, the user might skip it and choose a weak password still.
Part h: Strict complexity requirements might lead users to use predictable patterns in their password, which can weaken the security.

IA-5(2) Public Key-based Authentication (M)(H)

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

IA-5(2) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate

IA-5(2) Implementation Risks
Part a: Despite the authorized access, there is still the risk of insider threat. A privileged user might misuse the details of their private keys.
Part b: In high traffic environments, the certificate validation can bring in a lot of latency, which will slow down access for even legitimate users.

IA-5(6) Protection of Authenticators (M)(H)

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5(6) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-5(6) Implementation Risks
Even if the authenticators are properly secured, the attack can still target them through alternate means like phishing and social engineering.

IA-5(7) No Embedded Unencrypted Static Authenticators (M)(H)

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

IA-5 (7) Additional FedRAMP Requirements and Guidance:

Guidance: In this context, prohibited static storage refers to any storage where unencrypted authenticators, such as passwords, persist beyond the time required to complete the access process.

IA-5(7) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-5(7) Implementation Risks
If unencrypted static authenticators are accidentally embedded in applications, attackers might gain access to the codebase and could gain access to credentials.

IA-6 Authentication Feedback (L)(M)(H)

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

IA-6 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-6 Implementation Risks

Even when the feedback of authentication is obscured, if an attacker is physically present near a user, they can observe the keystroke patterns, which can potentially compromise the user’s credentials.

IA-7 Cryptographic Module Authentication (L)(M)(H)

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

IA-7 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-7 Implementation Risks
The advancements that occur in computing power could weaken the cryptographic algorithms over time, making the previously secure mechanisms for authentication to become vulnerable.

IA-8 Identification and Authentication (Non-organizational Users) (L)(M)(H)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IA-8 Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

IA-8 Implementation Risks
Non-organizational users might share their credentials within their organization, which can pose a potential security threat.

IA-8(1) Acceptance of PIV Credentials from Other Agencies (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-8(1) Control Summary Information
Responsible Role: System Administrator (SA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-8(1) Implementation Risks
If Tesla's systems experience downtime, it can result in failure of PIV credential verification, which can delay authorized user access to critical systems.

IA-8(2) Acceptance of External Authenticators (L)(M)(H)

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

IA-8(2) Control Summary Information
Responsible Role: System Administrator (SA)

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-8(2) Implementation Risks
Part a: If Tesla's systems don't strictly enforce NIST compliance checks, it can lead to weak authenticators to be accepted, which can lead to gaps in security.
Part b: If the list of accepted external authenticators is not updated regularly, it will become outdated and might even allow unauthorized authenticators to still remain in use, posing a security threat.

IA-8(4) Use of Defined Profiles (L)(M)(H)

Conform to the following profiles for identity management: **employee, contractor, and third-party vendor profiles, each with distinct access and authentication requirements**

IA-8(4) Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Parameter IA-8(4): employee, contractor, and third-party vendor profiles, each with distinct access and authentication requirements
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-8(4) Implementation Risks

If there is any ambiguity in distinguishing the profiles, it can lead to misclassification and open up security gaps.

IA-11 Re-authentication (L)(M)(H)

Require users to re-authenticate **after 15 minutes of inactivity, during high-risk actions, or upon reconnection.**

IA-11 Additional FedRAMP Requirements and Guidance:

Guidance: The fixed time period cannot exceed the limits set in SP 800-63. At this time they are:

- AAL2 (moderate baseline)
  - o Twelve (12) hours or
  - o Thirty (30) minutes of inactivity.

IA-11 Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IA-11: after 15 minutes of inactivity, during high-risk actions, or upon reconnection
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-11 Implementation Risks
Any delays in triggering the re-authentication can potentially give the chance to attackers to do more damage to the system.

IA-12 Identity Proofing (M)(H)

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

IA-12 Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing.

IA-12 Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-12 Implementation Risks
Part a: Even with proper identity proofing, a skilled attacker might still be able to impersonate a legitimate user through social engineering.
Part b: Synchronization delays between the various systems at Tesla could lead to temporary mismatches of user identities.
Part c: If not secured properly, collecting and storing sensitive identity evidence could lead to privacy violations.

IA-12(2) Identity Evidence (M)(H)

Require evidence of individual identification be presented to the registration authority.

IA-12(2) Control Summary Information
Responsible Role: Registration Authority (RA)
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

IA-12(2) Implementation Risks
As providing the evidence for the identification process is manual, it brings in the possibility of human error.

IA-12(3) Identity Evidence Validation and Verification (M)(H)

Require that the presented identity evidence be validated and verified through **biometric checks, government-issued ID verification, and multi-factor authentication.**

IA-12(3) Control Summary Information
Responsible Role: Registration Authority (RA)
Parameter IA-12(3): biometric checks, government-issued ID verification, and multi-factor authentication.
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-12(3) Implementation Risks
If the biometric data is of low-quality (unclear fingerprints for example), it can lead to a lot of false positives.

IA-12(5) Address Confirmation (M)(H)

Require that a **registration code** be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.

IA-12 (5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing.

IA-12(5) Control Summary Information

Responsible Role: Registration Authority (RA)
Parameter IA-12(5): registration code
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IA-12(5) Implementation Risks
If the out-of-band channel is not secure enough, then the attackers might be able to intercept the registration code, which poses a potential security risk.

Incident Response

IR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **all incident response team members, IT security personnel, and relevant management roles**:

1. **System-level** incident response policy that:

   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an **Incident Response Coordinator** to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy **at least every three (3) years** and following **major security incidents or regulatory updates**; and

2. Procedures **at least annually** and following **significant changes to the system or security environment**.

IR-1 Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-1(a): all incident response team members, IT security personnel, and relevant management roles
Parameter IR-1(a)(1): System-level
Parameter IR-1(b): Incident Response Coordinator
Parameter IR-1(c)(1)-1: at least every three (3) years
Parameter IR-1(c)(1)-2: major security incidents or regulatory updates
Parameter IR-1(c)(2)-1: at least annually
Parameter IR-1(c)(2)-2: significant changes to the system or security environment
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-1 Implementation Risks
Part a: If the incident response policy fails to fully address all the critical aspects, it can lead to a lot of confusion during incidents.
Part b: Over reliance on a single Incident Response Coordinator can pose a security risk if that person is not available during the occurrence of a critical incident.
Part c: If the updates are not conducted as per schedule, it can lead to policies becoming outdated, which will reduce their effectiveness in addressing the threats during an incident.

IR-2 Incident Response Training (L)(M)(H)

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

   1. Within **ten (10) days for privileged users and thirty (30) days for Incident Response roles** of assuming an incident response role or responsibility or acquiring system access;

   2. When required by system changes; and

   3. **At least annually** thereafter; and

b. Review and update incident response training content **at least annually** and following **significant security incidents or policy changes**.

IR-2 Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-2(a)(1): ten (10) days for privileged users and thirty (30) days for Incident Response roles
Parameter IR-2(a)(3): At least annually
Parameter IR-2(b)-1: at least annually
Parameter IR-2(b)-2: significant security incidents or policy changes
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-2 Implementation Risks
Part a: Training doesn’t guarantee that the system users are effectively learning the lessons. They could just go through the training for namesake and not pay any attention.

Part b: If the training content is updated too frequently and changed a lot, it may overwhelm the system users.

IR-3 Incident Response Testing (M)(H)

Test the effectiveness of the incident response capability for the system **functionally, at least annually** using the following tests: **simulated phishing attacks, and breach simulations**.

IR-3-2 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to test commencing.

IR-3 Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-3-1: functionally, at least annually
Parameter IR-3-2: simulated phishing attacks, and breach simulations
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-3 Implementation Risks
The simulated phishing attacks might fail to mimic real world scenarios. In that case, even if the employees are able to pass the simulated attacks, it doesn’t guarantee that they have developed effective detection skills.

IR-3(2) Coordination with Related Plans (M)(H)

Coordinate incident response testing with organizational elements responsible for related plans.

IR-3(2) Control Summary Information
Responsible Role: Incident Response Coordinator
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-3(2) Implementation Risks
If the related plans are not well synchronized, it may lead to conflicting procedures in the incident response testing, which will reduce its overall effectiveness.

IR-4 Incident Handling (L)(M)(H)

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

IR-4 Control Summary Information
Responsible Role: Incident Response Coordinator
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-4 Implementation Risks
Part a: If the detection mechanism is not configured properly, it can lead to delayed identification of the incident, which can potentially increase the damage.
Part b: If there is a lack of coordination between teams responsible for incident handling, it can result in incomplete responses, which leads to security gaps.
Part c: If there are any delays in updating the procedures based on the lessons learned, it might still leave Tesla vulnerable to repeated incidents.
Part d: No tangible metric has been specified to compare the incident handling activities across the organization. It can lead to conflicts and gaps in the procedure to handle the incident.

IR-4(1) Automated Incident Handling Processes (M)(H)

Support the incident handling process using **automated mechanisms such as intrusion detection systems, and automated alerting systems**.

IR-4(1) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IR-4(1): automated mechanisms such as intrusion detection systems, and automated alerting systems
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

IR-4(1) Implementation Risks
Any delays in the automated alerting system might leave Tesla vulnerable for a longer time during a critical incident.

IR-5 Incident Monitoring (L)(M)(H)

Track and document incidents.

IR-5 Control Summary Information
Responsible Role: Incident Response Coordinator
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-5 Implementation Risks
Concrete standardized guidelines as to how to track incidents aren't specified. It can lead to ambiguity as to how to go about tracking and different organizations might approach tracking in conflicting ways.

IR-6 Incident Reporting (L)(M)(H)

a. Require personnel to report suspected incidents to the organizational incident response capability within **US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)**; and

b. Report incident information to **Chief Information Security Officer (CISO), incident response team leads, and relevant regulatory bodies**.

IR-6 Additional FedRAMP Requirements and Guidance:

Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure.

IR-6 Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-6(a): US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)
Parameter IR-6(b): Chief Information Security Officer (CISO), incident response team leads, and relevant regulatory bodies
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-6 Implementation Risks
Part a: If the reporting process is not defined clearly, the personnel might be unsure as to where to report the incidents.
Part b: Incident reports might contain sensitive information. If the reports are not properly shared, it can lead to data leaks.

IR-6(1) Automated Reporting (M)(H)

Report incidents using **automated mechanisms such as automated email alerts, and incident tracking software**.

IR-6(1) Control Summary Information
Responsible Role: System Administrator (SA)

Parameter IR-6(1): automated mechanisms such as automated email alerts, and incident tracking software
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-6(1) Implementation Risks
Automated reporting mechanisms might misidentify events, potentially leading to a lot of false positives, which can disrupt the normal workings within Tesla.

IR-6(3) Supply Chain Coordination (M)(H)

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-6(3) Control Summary Information
Responsible Role: Incident Response Coordinator
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-6(3) Implementation Risks
If the incident information shared with the supply chain partners is incomplete, it might hinder their capability of responding effectively.

IR-7 Incident Response Assistance (L)(M)(H)

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-7 Control Summary Information
Responsible Role: Incident Response Coordinator
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-7 Implementation Risks
If the advice provided by the support personnel is counterproductive, it might lead to ineffective incident handling of incidents.

IR-7(1) Automation Support for Availability of Information and Support (M)(H)

Increase the availability of incident response information and support using **automated mechanisms such as centralized incident response dashboards, and real-time alerting systems**.

IR-7(1) Control Summary Information
Responsible Role: System Administrator (SA)
Parameter IR-7(1): automated mechanisms such as centralized incident response dashboards, and real-time alerting systems
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-7(1) Implementation Risks
Over reliance on these automated systems might lead to a slack in manual oversight, which can result in context sensitive incidents to be missed.

IR-8 Incident Response Plan (L)(M)(H)

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by the C**hief Information Security Officer (CISO) at least annually**; and
10. Explicitly designates responsibility for incident response to the **Incident Response Team and designated personnel within the IT security department**.

b. Distribute copies of the incident response plan to **key stakeholders, including the executive leadership, IT security staff, and relevant federal oversight agencies**;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to **all relevant stakeholders, including executive leadership and the incident response team**; and

e. Protect the incident response plan from unauthorized disclosure and modification.

IR-8 Additional FedRAMP Requirements and Guidance:

(b) Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

(d) Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

IR-8 Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-8(a)(9)-1: Chief Information Security Officer (CISO)
Parameter IR-8(a)(9)-2: at least annually
Parameter IR-8(a)(10): the Incident Response Team and designated personnel within the IT security department
Parameter IR-8(b): key stakeholders, including the executive leadership, IT security staff, and relevant federal oversight agencies
Parameter IR-8(d): all relevant stakeholders, including executive leadership and the incident response team
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-8 Implementation Risks
Part a: If the plan doesn’t clearly define what constitutes a reportable incident, it might lead to critical issues to go unreported.

Part b: Distributing the copies might not be sufficient in and by itself. It's important to make sure that key stakeholders are actually going through the plan.
Part c: If the updates fail to account for all the relevant changes, it can result in gaps in the plan.
Part d: There should be a body that makes sure that the stakeholders are informed about the changes. Else, it might be possible the few stakeholders were accidentally not informed.
Part e: Any accidental changes to the plan can lead to potential vulnerabilities.

IR-9 Information Spillage Response (M)(H)

Respond to information spills by:

a. Assigning the **Incident Response Team and Data Protection Officer** with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting the **Chief Information Security Officer (CISO) and relevant IT security personnel** of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: **conducting a root cause analysis and reviewing containment procedures**.

IR-9 Control Summary Information
Responsible Role: Incident Response Team Lead
Parameter IR-9(a): Incident Response Team and Data Protection Officer
Parameter IR-9(c): Chief Information Security Officer (CISO) and relevant IT security personnel
Parameter IR-9(g): conducting a root cause analysis and reviewing containment procedures
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

IR-9 Implementation Risks
Part a: Lack of coordination between Incident Response Team and Data Protection Officer might lead to inconsistencies in responding to information spills.
Part b: If the spilled information is not accurately identified, it might result in some contaminated information to be overlooked, which can cause further contamination.
Part c: If the alert is sent through a compromised communication channel, the attacker might be able to intercept it.
Part d: In a complex organization like Tesla, the systems might be so deeply intertwined that it will be difficult to isolate specific systems.
Part e: If the data eradication is done improperly, it might delete important data that might have been non-contaminated.
Part f: There might be systems which were indirectly affected by the spill and they might be overlooked, leading the contamination to spread further.
Part g: If the root cause is not thoroughly investigated, it can result in similar spills to even occur in the future.

IR-9(2) Training (M)(H)

Provide information spillage response training **at least annually**.

IR-9(2) Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-9(2): at least annually
Implementation Status (check all that apply): ☐ Partially Implemented

Control Origination (check all that apply): ☐ Service Provider Corporate

IR-9(2) Implementation Risks
Employees might just view the annual training as a formality, which would result in them not retaining any of the critical information that was taught.

IR-9(3) Post-spill Operations (M)(H)

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: **establish secure alternate workstations, and implement data recovery protocols**.

IR-9(3) Control Summary Information
Responsible Role: Incident Response Coordinator
Parameter IR-9(3): establish secure alternate workstations, and implement data recovery protocols
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-9(3) Implementation Risks
There is a possibility that the recovered data might reintroduce the contaminated information if it was not properly sanitized.

IR-9(4) Exposure to Unauthorized Personnel (M)(H)

Employ the following controls for personnel exposed to information not within assigned access authorizations: **initiate a security debriefing, restrict further access to sensitive areas, and provide retraining on access policies**.

IR-9(4) Control Summary Information
Responsible Role: Information System Security Officer (ISSO)
Parameter IR-9(4): initiate a security debriefing, restrict further access to sensitive areas, and provide retraining on access policies
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate

IR-9(4) Implementation Risks
If the retraining on access policies is too generic, it might fail to prevent any future incidents.

Physical and Environmental Protection

PE-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **Cybersecurity and Physical Security teams, Facility Management, Environmental Health and Safety (EHS) teams, and Compliance Office.**

   1. **Organization-level; mission/business process-level; system-level** physical and environmental protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an **Chief Compliance Officer** to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy **at least every three (3) years** and following **organizational changes and new factories being setup or when new disposal mechanisms devised**; and
2. Procedures **at least annually** and following **natural disasters, security breaches, new factories being set up, when new disposal mechanisms devised or regulatory changes.**

PE-1 Control Summary Information
Responsible Role: Chief Compliance Officer
Parameter PE-1(a): Cybersecurity and Physical Security teams, Facility Management, Environmental Health and Safety (EHS) teams, and Compliance Office.
Parameter PE-1(a)(1): Organization-level; mission/business process-level; system-level
Parameter PE-1(b): Chief Compliance Officer
Parameter PE-1(c)(1)-1: at least every three (3) years
Parameter PE-1(c)(1)-2: organizational changes and new factories being setup or when new disposal mechanisms devised
Parameter PE-1(c)(2)-1: at least annually
Parameter PE-1(c)(2)-2: natural disasters, security breaches, or regulatory changes.
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-1 Implementation Risks
Part a: The challenge of coordinating efforts across different departments can lead to inconsistencies in policy implementation, heightening the risk of compliance gaps and leaving the organization vulnerable to regulatory penalties or security breaches.
Part b: As Tesla expands its operations across various regions, it is imperative for the Chief Compliance Officer (CCO) to be thoroughly informed about the local legalities,

	environmental safety regulations, and other critical details. This knowledge is essential for effectively navigating the responsibilities of the role and ensuring successful operations.
Part c:	The frequency of policy reviews—every three years for policies and annually for procedures—can create compliance complexity for Tesla, which operates in a fast-paced environment with frequent organizational changes and new factories. If policies are not updated promptly in response to these changes, Tesla risks regulatory non-compliance, potentially leading to fines or loss of credibility.

PE-2 Physical Access Authorizations (L)(M)(H)

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals **at least annually** and

d. Remove individuals from the facility access list when access is no longer required.

PE-2 Control Summary Information
Responsible Role: Facility Security Manager
Parameter PE-2(c): at least annually
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-2 Implementation Risks
Part a: Maintaining an accurate list of individuals with authorized access can be challenging in a dynamic environment like Tesla, where employees frequently change roles. Miscommunication about role changes can disrupt operations, as seen when an employee who should not have accessed a critical facility was granted access.

Part b: If credentials are issued to the wrong person or misused, it can lead to serious consequences, including unauthorized access from misplaced or stolen items like ID cards and key fobs. Accurate identification is essential to prevent risks, as human error can compromise the process.

Part c: When the review process is rushed or lacks proper resources, critical discrepancies can be easily overlooked, resulting in unauthorized access rights being maintained far longer than needed.

Part d: Retaining orphan access accounts poses a significant risk, as it could permit unauthorized personnel to enter the facility without detection.

PE-3 Physical Access Control (L)(M)(H)

a. Enforce physical access authorizations at **organization-defined entry and exit points** to the facility where the system resides by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using **biometric scanners (fingerprint and facial recognition) at entry and exit points, RFID badge readers for employees, secure turnstiles, and automated gates linked to Tesla's access control network. Security personnel monitor critical Tesla facilities, such as Gigafactories and data centers, while live CCTV monitoring by Tesla's Security Operations Center (SOC) ensures real-time oversight**;

b. Maintain physical access audit logs for **organization-defined entry and exit points at critical facilities, including data centers, battery production units, and robotics labs**;

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: **utilizing turnstiles, visitor check-in kiosks, and visible ID badges. Additionally, ensure 24/7 surveillance cameras are in place to effectively manage and monitor public access areas, including visitor lobbies and presentation rooms**;

d. Escort visitors and control visitor activity **in all circumstances within restricted access area where the information system resides like the data centers and cutting-edge robotics facilities, including those with Optimus Gen 3 systems**;

e. Secure keys, combinations, and other physical access devices;

f. Inventory **all physical access devices—employee badges, biometric devices, and master keys** every **quarter**; and

g. Change combinations and keys **quarterly or right after security breaches** and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

PE-3 Control Summary Information
Responsible Role: Chief Information Security Officer & Facility Security Manager
Parameter PE-3(a): organization-defined entry and exit points
Parameter PE-3(a)(2): biometric scanners (fingerprint and facial recognition) at entry and exit points, RFID badge readers for employees, secure turnstiles, and automated gates linked to Tesla's access control network. Security personnel monitor critical Tesla facilities, such as Gigafactories and data centers, while live CCTV monitoring by Tesla's Security Operations Center (SOC) ensures real-time oversight
Parameter PE-3(b): organization-defined entry and exit points at critical facilities, including data centers, battery production units, and robotics labs
Parameter PE-3(c): utilizing turnstiles, visitor check-in kiosks, and visible ID badges. Additionally, ensure 24/7 surveillance cameras are in place to effectively manage and monitor public access areas, including visitor lobbies and presentation rooms
Parameter PE-3(d): in all circumstances within restricted access area where the information system resides like the data centers and cutting-edge robotics facilities, including those with Optimus Gen 3 systems
Parameter PE-3(f)-1: all physical access devices—employee badges, biometric devices, and master keys
Parameter PE-3(f)-2: quarter
Parameter PE-3(g): quarterly or right after security breaches
Implementation Status: ☐ Partially Implemented

Control Origination: ☐ Service Provider Corporate

PE-3 Implementation Risks
Part a: Tailgating is a real risk if enforcement is not strict, as it is ultimately dependent on people's behavior.
Part b: If the logging system is not properly updated or patched upon discovering a vulnerability, it poses a potential threat due to the possibility of altering the logs through remote access.
Part c: Public areas pose a tangible risk of unauthorized surveillance or tampering if they are not properly monitored. Physical access controls might be bypassed if not consistently monitored.
Part d: Unsupervised visitors present a significant risk to restricted systems and areas. Even a momentary lapse in oversight can allow unauthorized access to critical facilities.
Part e: Improper storage of physical access devices, such as keys and master codes, poses a serious risk of unauthorized access.
Part f: Missed inventory updates can lead to unaccounted or outdated access devices, increasing vulnerability to attacks in a constantly evolving threat landscape, similar to the pager attack.
Part g: Not changing combinations/keys promptly after personnel changes can expose security risks if former employees still have access.

PE-4 Access Control for Transmission (M)(H)

Control physical access to **Solar Roofs, Powerwall, Powerpack, Megapack solutions, high-voltage transmission lines, substations, smart grid technology, and EV Supercharger Stations, enabling efficient energy generation, storage, and delivery** within organizational facilities **using security controls, such as restricted access zones, biometric locks, surveillance systems, and physical barriers.**

PE-4 Control Summary Information
Responsible Role: Facility Security Manager

Parameter PE-4-1: Solar Roofs, Powerwall, Powerpack, Megapack solutions, high-voltage transmission lines, substations, smart grid technology, and EV Supercharger Stations, enabling efficient energy generation, storage, and delivery
Parameter PE-4-2: security controls, such as restricted access zones, biometric locks, surveillance systems, and physical barriers.
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-4 Implementation Risks
Dependence on technology like surveillance cameras and biometric locks poses risks of equipment failure. Malfunctions can create blind spots or access points that adversaries may exploit, leading to unauthorized access during critical operations.

PE-5 Access Control for Output Devices (M)(H)

Control physical access to output from **printers, KPI dashboards, and energy output systems for Powerwall, Powerpack, Megapack, and Optimus Gen 3 robot report screens** to prevent unauthorized individuals from obtaining the output.

PE-5 Control Summary Information
Responsible Role: Chief Information Security Officer (CISO)
Parameter PE-5: printers, KPI dashboards, and energy output systems for Powerwall, Powerpack, Megapack, and Optimus Gen 3 robot report screens
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-5 Implementation Risks
Insider threats can occur when employees or contractors misuse their access to output devices, retrieving confidential data for personal or competitive gain

PE-6 Monitoring Physical Access (L)(M)(H)

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs **at least once every month** and upon occurrence of a **potential security threats or anomalies**; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

PE-6 Control Summary Information
Responsible Role: Facility Security Manager
Parameter PE-6(b)-1: at least once every month
Parameter PE-6(b)-2: potential security threats or anomalies
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-6 Implementation Risks
Part a: Blind spots may occur due to poor camera installation or equipment failures, risking unauthorized access going undetected. Adverse weather conditions can also impact security measures, compromising camera functionality and monitoring capabilities, which leaves the facility vulnerable during critical times.

Part b: The overwhelming volume of generated data can cause important incidents to be lost among numerous log entries, leading to overlooked anomalies and undetected security violations.
Part c: If the review team doesn't communicate findings to the incident response team quickly, it could lead to significant losses.

PE-6(1) Intrusion Alarms and Surveillance Equipment (M)(H)

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

PE-6(1) Control Summary Information
Responsible Role: Facility Security Manager & Security Operations Center (SOC) Team
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-6(1) Implementation Risks
Intrusion alarms and surveillance equipment can be vulnerable to tampering by determined adversaries. Without protective measures like secure mounting or tamper-evident seals, criminals may disable alarms or recording capabilities undetected, compromising facility security.

PE-8 Visitor Access Records (L)(M)(H)

a. Maintain visitor access records to the facility where the system resides **for a minimum of one (1) year**;

b. Review visitor access records **monthly once**; and

c. Report anomalies in visitor access records to **Facility Security Manager and Security Operations Center (SOC)**.

PE-8 Control Summary Information

Responsible Role: Chief Information Security Officer (CISO)
Parameter PE-8(a): for a minimum of one (1) year
Parameter PE-8(b): monthly once
Parameter PE-8(c): Facility Security Manager and Security Operations Center (SOC)
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-8 Implementation Risks
Part a: Losing out on data due to a cyber attack resulting in not being able to maintain visitor access records for at least one year can result in regulatory non-compliance and potential fines.
Part b: If reviewers of the logs are not properly trained, they may miss anomalies or significant patterns, undermining the effectiveness of the control.
Part c: A vague reporting structure for anomalies can leave personnel uncertain about whom to report to, causing confusion and delays that may result in unresolved issues and heightened security risks.

PE-9 Power Equipment and Cabling (M)(H)

Protect power equipment and power cabling for the system from damage and destruction.

PE-9 Control Summary Information
Responsible Role: Energy Infrastructure Lead
Implementation Status: ☐ Partially Implemented
Control Origination:

☐ Service Provider Corporate

PE-9 Implementation Risks
Maintenance activities around power equipment and cabling can lead to damage if personnel are not adequately trained in safe handling practices. Failing to secure cables and equipment during and after maintenance can increase the risk of power outages and equipment failures, affecting operations.

PE-10 Emergency Shutoff (M)(H)

a. Provide the capability of shutting off power **to all critical Tesla systems, including Powerwall, Powerpack, Megapack units, Supercharger Stations, Gigafactory production lines, and data center operations** in emergency situations;

b. Place emergency shutoff switches or devices in **multiple egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off** to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

PE-10 Control Summary Information
Responsible Role: Facility Security Manager
Parameter PE-10(a): to all critical Tesla systems, including Powerwall, Powerpack, Megapack units, Supercharger Stations, Gigafactory production lines, and data center operations
Parameter PE-10(b): multiple egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-10 Implementation Risks

Part a: Emergency shutoff mechanisms are prone to failure if they are not properly maintained or if they experience wear and tear.
Part b: Inconsistent labeling of shutoff devices can cause confusion in urgent situations, leading authorized personnel to misidentify switches and respond ineffectively.
Part c: Malicious actors could access and disable critical systems. Without alarms or alerts for unauthorized access, risks persist. Personnel must be informed of anomalies to respond quickly to threats against emergency capabilities.

PE-11 Emergency Power (M)(H)

Provide an uninterruptible power supply to facilitate an orderly shutdown of the system **for critical Gigafactories, research and development centers, and Tesla Energy sites ; transition of the system to long-term alternate power to Tesla's Powerwall-based long-term alternate power solutions** in the event of a primary power source loss.

PE-11 Control Summary Information
Responsible Role: Facility Security Manager
Parameter PE-11: for critical Gigafactories, research and development centers, and Tesla Energy sites ; transition of the system to long-term alternate power to Tesla's Powerwall-based long-term alternate power solutions
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-11 Implementation Risks
UPS implementation can be costly, especially for large operations like Tesla’s Gigafactories. Additionally, the energy stored in Powerwall may not sustain the facilities for long durations.

PE-12 Emergency Lighting (L)(M)(H)

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-12 Control Summary Information
Responsible Role: Facility Security Manager
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-12 Implementation Risks
If the emergency lighting system relies on a Powerwall or alternative power sources, any malfunction in the dependent system can lead to complete system failure. Additionally, if integrated with IoT, it may be vulnerable to cyberattacks. Lastly, untrained personnel will render it ineffective.

PE-13 Fire Protection (L)(M)(H)

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13 Control Summary Information
Responsible Role: Facility Security Manager
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-13 Implementation Risks
Tesla's factories, which use Lithium-ion batteries and other volatile materials, face heightened fire risks. Any malfunction in fire detection or suppression systems could lead to disastrous outcomes, especially if these systems can be disabled remotely.

PE-13(1) Detection Systems — Automatic Activation and Notification (M)(H)

Employ fire detection systems that activate automatically and notify **Tesla's on-site physical security and building maintenance teams who monitor automated fire detection alerts through Tesla's centralized systems** and **service provider emergency responders like local fire departments & Tesla's internal emergency response teams with incident response responsibilities** in the event of a fire.

PE-13(1) Control Summary Information
Responsible Role: Facility Security Manager & Emergency Response Coordinator
Parameter PE-13(1)-1: Tesla's on-site physical security and building maintenance teams who monitor automated fire detection alerts through Tesla's centralized systems
Parameter PE-13(1)-2: service provider emergency responders like local fire departments & Tesla's internal emergency response teams with incident response responsibilities
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-13(1) Implementation Risks
Delays in emergency responder arrival may occur due to notification gaps or lack of facility familiarity. Additionally, IoT-integrated automated systems could be vulnerable to cyberattacks, disrupting their functionality.

PE-13(2) Suppression Systems — Automatic Activation and Notification (M)(H)

(a) Employ fire suppression systems that activate automatically and notify **Facility Security Manager & Emergency Response Coordinator** and **local fire departments & Tesla's internal emergency response teams**; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

PE-13(2) Control Summary Information
Responsible Role: Facility Security Manager & Emergency Response Coordinator
Parameter PE-13(2)(a)-1: Facility Security Manager & Emergency Response Coordinator
Parameter PE-13(2)(a)-2: local fire departments & Tesla's internal emergency response teams
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-13(2) Implementation Risks
Part a: The notification system is vulnerable to remote tampering, which can cause delays leading to major incidents. Employee credentials can be obtained through social engineering.
Part b: If the automatic system fails and there aren't enough trained personnel, a manageable incident could escalate into a significant crisis for the organization.

PE-14 Environmental Controls (L)(M)(H)

a. Maintain consistent with **American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments levels within the facility** where the system resides at **organization-defined acceptable levels**; and

b. Monitor environmental control levels **continuously**.

PE-14 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

PE-14 Control Summary Information
Responsible Role: Environmental Monitoring Systems Manager
Parameter PE-14(a)-1: American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments levels within the facility
Parameter PE-14(a)-2: organization-defined acceptable levels
Parameter PE-14(b): continuously
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-14 Implementation Risks
Part a: Excessive temperatures at server inlets from HVAC failures due to cyberattacks can cause overheating and equipment failures. Also, improper humidity levels may lead to moisture-related damage to electronics.
Part b: Failure of monitoring systems can impede accurate tracking of temperature and humidity. Delays in responding to environmental alerts may result in equipment damage

PE-15 Water Damage Protection (L)(M)(H)

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-15 Control Summary Information

Responsible Role: Facilities Operations Manager
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-15 Implementation Risks
A key risk is that master shutoff or isolation valves may not be easily accessible during water emergencies. Also, if personnel are not trained on the location and operation of these valves, delays in shutting off water flow can occur.

PE-16 Delivery and Removal (L)(M)(H)

a. Authorize and control **all information system components, including servers, storage devices, and networking equipment** entering and exiting the facility; and

b. Maintain records of the system components.

PE-16 Control Summary Information
Responsible Role: Facilities Security Manager
Parameter PE-16(a): all information system components, including servers, storage devices, and networking equipment
Implementation Status: ☐ Partially Implemented
Control Origination: ☐ Service Provider Corporate

PE-16 Implementation Risks

Part a: Unauthorized personnel may access critical information systems, risking data breaches or compromises. Discarded systems or electronics that aren't properly formatted or tracked can also lead to data breaches.
Part b: Historical records may be lost or mismanaged, hindering audits and tracking sensitive components over time.

PE-17 Alternate Work Site (M)(H)

a. Determine and document the **organization-defined alternate work sites which include remote offices, co-working spaces, and certain home office setups that meet security compliance standards** allowed for use by employees;

b. Employ the following controls at alternate work sites: **organization-defined controls which include secure access to company systems through virtual private networks (VPNs), data encryption protocols, and guidelines for handling sensitive information in non-corporate environments. In addition, employees are trained on how to use these controls effectively to safeguard corporate data** ;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PE-17 Control Summary Information
Responsible Role: Chief Information Security Officer & Human Resources (HR) Manager
Parameter PE-17(a): organization-defined alternate work sites which include remote offices, co-working spaces, and certain home office setups that meet security compliance standards
Parameter PE-17(b): organization-defined controls which include secure access to company systems through virtual private networks (VPNs), data encryption protocols, and guidelines for handling sensitive information in non-corporate environments. In addition, employees are trained on how to use these controls effectively to safeguard corporate data
Implementation Status: ☐ Partially Implemented
Control Origination:

☐ Service Provider Corporate

PE-17 Implementation Risks
Part a: A potential risk is poor documentation of approved alternate work sites. Without clear guidelines, employees may work from insecure locations, putting organizational data at risk.
Part b: If employees don't follow the controls, it exposes the organization to significant risks. The enforcement of these controls is an important consideration.
Part c: The organization risks not regularly assessing control effectiveness at alternate work sites to save costs, potentially overlooking weaknesses in Tesla's security.
Part d: Unawareness of communication channels for reporting incidents can hinder operations.

Risk Assessment

RA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to **Chief Risk Officer (CRO)**:

1. **Organization-level and mission/business process-level** risk assessment policy that:

   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an **Chief Risk Officer (CRO)** to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy **at least every three (3) years** and following **major data breaches and regulatory changes**; and

2. Procedures **at least annually** and following **significant changes**.

RA-1 Control Summary Information
Responsible Role: **Chief Information Security Officer**
Parameter RA-1(a): **Chief Risk Officer (CRO)**
Parameter RA-1(a)(1): **Organization-level and mission/business process-level**
Parameter RA-1(b): **Chief Risk Officer (CRO)**
Parameter RA-1(c)(1)-1: **at least every three (3) years**
Parameter RA-1(c)(1)-2: **major data breaches and regulatory changes**
Parameter RA-1(c)(2)-1: **at least annually**
Parameter RA-1(c)(2)-2: **significant changes**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-1 Implementation Risks
Part a: Failure to involve all relevant personnel in the development process may result in incomplete policies and procedures.
Part b: Appointing a person without adequate expertise or resources may undermine the effectiveness of policy and procedure management.
Part c: Significant changes in the environment might not be reflected in a timely manner, leaving gaps in the risk assessment framework.

RA-2 Security Categorization (L)(M)(H)

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2 Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-2 Implementation Risks
Part a: Undermining the criticality of system information could result in insufficient or excessive security measures.
Part b: Poorly documented results may lead to challenges during audits or disagreements among stakeholders.
Part c: Delays in the review and approval process by the authorizing official could hold up the implementation of security measures.

RA-3 Risk Assessment (L)(M)(H)

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in **security assessment report**;

d. Review risk assessment results **at least every three (3) years and when a significant change occurs**;

e. Disseminate risk assessment results to **risk management team**; and

f. Update the risk assessment **at least every three (3) years** or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

(e) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-3 Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-3(c): **security assessment report**
Parameter RA-3(d): **at least every three (3) years and when a significant change occurs**
Parameter RA-3(e): **risk management team**
Parameter RA-3(f): **at least every three (3) years**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-3 Implementation Risks
Part a: Failure to identify all potential threats or vulnerabilities may result in incomplete risk assessment and inadequate security measures.
Part b: Misalignment between organizational, business process, and system-level assessments can lead to gaps in risk management.
Part c: Poorly documented assessments can hinder the understanding of risks and impede future reviews or audits.
Part d: Missing scheduled reviews or failing to respond to changes can result in outdated risk assessments.
Part e: Sharing risk assessment results with the wrong personnel could expose sensitive information.
Part f: Risk assessments might not reflect changes in the threat environment, new regulations, or system modifications.

RA-3(1) Supply Chain Risk Assessment (L)(M)(H)

(a) Assess supply chain risks associated with **IT systems**; and

(b) Update the supply chain risk assessment **annually**, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in supply chain.

RA-3(1) Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-3(1)(a): **IT systems**
Parameter RA-3(1)(b): **annually**

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-3(1) Implementation Risks
Part a: The risk assessment may fail to identify all relevant risks, such as geographic vulnerabilities, or third-party cybersecurity weaknesses.
Part b: Significant updates to suppliers, geopolitical conditions, or system dependencies may not be reflected in the risk assessment.

RA-5 Vulnerability Monitoring and Scanning (L)(M)(H)

a. Monitor and scan for vulnerabilities in the system and hosted applications **monthly operating system/infrastructure; monthly web applications (including APIs) and databases** and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities **high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery** in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with **Risk Management Team** to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page > Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/

Guidance: Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity and for FedRAMP does not require an entry onto the POA&M or entry onto the RET during any assessment phase.

Warning findings, on the other hand, are given a risk rating (low, moderate, high or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.

Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a “warning” as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on “Tracking of Compliance Scans” in FAQs.

(a) Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

(d) Requirement: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) the KEV remediation date supersedes the FedRAMP parameter requirement.

(e) Requirement: to include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-5 Control Summary Information

Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-5(a): **monthly operating system/infrastructure; monthly web applications (including APIs) and databases**
Parameter RA-5(d): **high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery**
Parameter RA-5(e): **Risk Management Team**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-5 Implementation Risks
Part a: Failure to perform timely scans may leave critical vulnerabilities undetected, exposing the system to threats.
Part b: Lack of interoperability between tools may lead to gaps in the vulnerability management process.
Part c: Complex reports may result in critical vulnerabilities being missed or improperly prioritized.
Part d: Limited resources or poor tracking may lead to delays, increasing exposure.
Part e: Sharing sensitive vulnerability information could expose the organization to additional risks.
Part f: Tools that are not regularly updated may miss new vulnerabilities, rendering scans ineffective.

RA-5(2) Update Vulnerabilities to Be Scanned (L)(M)(H)

Update the system vulnerabilities to be scanned **within twenty-four (24) hours prior to running scans**.

RA-5(2) Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-5(2): **within twenty-four (24) hours prior to running scans**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-5(2) Implementation Risks
Running scans with outdated vulnerability definitions may lead to missed detections of newly identified risks.

RA-5(3) Breadth and Depth of Coverage (M)(H)

Define the breadth and depth of vulnerability scanning coverage.

RA-5(3) Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

RA-5(3) Implementation Risks
Defining an overly narrow scope for scans may miss critical vulnerabilities.

RA-5(5) Privileged Access (M)(H)

Implement privileged access authorization to **all components that support authentication** for **all scans**.

RA-5(5) Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-5(5)-1: **all components that support authentication**
Parameter RA-5(5)-2: **all scans**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

RA-5(5) Implementation Risks
Misconfigurations in access controls may allow unauthorized users to manipulate or bypass scans, compromising their integrity.

RA-5(11) Public Disclosure Program (L)(M)(H)

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-5(11) Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

RA-5(11) Implementation Risks
A poorly managed reporting channel could result in disclosure of sensitive vulnerabilities before they are resolved.

RA-7 Risk Response (L)(M)(H)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-7 Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-7 Implementation Risks
Failure to address findings from assessments promptly can leave the organization exposed to known risks.

RA-9 Criticality Analysis (M)(H)

Identify critical system components and functions by performing a criticality analysis for **databases, application servers, network infrastructure, storage devices** at **deployment phase.**

RA-9 Control Summary Information
Responsible Role: **Chief Risk Officer (CRO)**
Parameter RA-9-1: **databases, application servers, network infrastructure, storage devices**
Parameter RA-9-2: **deployment phase**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

RA-9 Implementation Risks
Overlooking critical components that are not mentioned can result in insufficient security measures

Supply Chain Risk Management

SR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate **to include Chief Privacy Officer (CPO) and Information System Security Officer (ISSO)**:

1. **Organization-level and system-level** supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an **Chief Supply Chain Manager** to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy **at least every three (3) years** and following **cyber-attacks affecting critical suppliers and counterfeiting incidents**; and

2. Procedures **at least annually** and following **significant changes**.

SR-1 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-1(a): **Chief Privacy Officer (CPO) and Information System Security Officer (ISSO)**
Parameter SR-1(a)(1): **Organization-level and system-level**
Parameter SR-1(b): **Chief Supply Chain Manager**
Parameter SR-1(c)(1)-1: **at least every three (3) years**
Parameter SR-1(c)(1)-2: **cyber-attacks affecting critical suppliers and counterfeiting incidents**
Parameter SR-1(c)(2)-1: **at least annually**
Parameter SR-1(c)(2)-2: **significant changes**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-1 Implementation Risks

Part a: ● The SCRM policy might not fully address critical areas, or may fail to comply with applicable laws and standards. ● Poor coordination between departments may lead to inconsistent application of SCRM policy.
Part b: ● Over-reliance on the Chief Supply Chain Manager could result in bottlenecks or continuity risks if they leave the position.
Part c: ● Failure to regularly review and update policies can lead to outdated policies that don't address current risks.

SR-2 Supply Chain Risk Management Plan (L)(M)(H)

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services such as **data storage and processing systems**.

b. Review and update the supply chain risk management plan **at least annually** or as required, to address threat, organizational or environmental changes; and

c. Protect the **supply chain risk management plan** from unauthorized disclosure and modification.

SR-2 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-2(a): **data storage and processing systems**
Parameter SR-2(b): **at least annually**
Parameter SR-2(c): **supply chain risk management plan**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Hybrid (Corporate and System Specific)

SR-2 Implementation Risks
Part a: Delays in identifying secure suppliers and partners who comply with security and risk management requirements could cause operational delays.
Part b: Risk of overlooking emerging technologies or evolving threats that may affect the supply chain.
Part c: Exposure to data breach risks if the plan is not encrypted or stored securely within the organization.

SR-2(1) Establish SCRM Team (L)(M)(H)

Establish a supply chain risk management team consisting of **Chief Supply Chain Manager, Information Security Manager, Configuration Management Officer and Supply Chain Manager** to lead and support the following SCRM activities: **Supply Chain Risk Identification and Assessment, Risk Mitigation Planning, Supplier Evaluation and Monitoring, Incident Response Planning**.

SR-2(1) Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-2(1)-1: **Chief Supply Chain Manager, Information Security Manager, Configuration Management Officer and Supply Chain Manager**
Parameter SR-2(1)-2: **Supply Chain Risk Identification and Assessment, Risk Mitigation Planning, Supplier Evaluation and Monitoring, Incident Response Planning**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-2(1) Implementation Risks
- Team members may lack specialized skills or experience needed for specific SCRM tasks, particularly in complex areas like cybersecurity and supplier risk assessment. - In the event of a supply chain disruption, delays in coordinating a response can escalate risks and costs.

SR-3 Supply Chain Controls and Processes (L)(M)(H)

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of **vehicle control system, battery and energy system, manufacturing equipment and robotics** in coordination with **Chief Supply Chain Manager, Information Security Manager, Configuration Management Officer and Supply Chain Manager**;

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: **Supply Chain Risk Management Plan (SCRM Plan)**; and

c. Document the selected and implemented supply chain processes and controls in **supply chain risk management plan, Supply Chain Risk Management Plan**.

SR-3 Additional FedRAMP Requirements and Guidance:

Requirement: CSO must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary.

SR-3 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-3(a)-1: **vehicle control system, battery and energy system, manufacturing equipment and robotics**
Parameter SR-3(a)-2: **Chief Supply Chain Manager, Information Security Manager, Configuration Management Officer and Supply Chain Manager**
Parameter SR-3(b): **Supply Chain Risk Management Plan (SCRM Plan)**
Parameter SR-3(c): **supply chain risk management plan, Supply Chain Risk Management Plan**.

Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-3 Implementation Risks
Part a: Each of these systems has distinct requirements and risks, making it challenging to establish a standardized process for identifying weaknesses.
Part b: Different departments may interpret or implement processes differently, leading to inconsistent identification and handling of weaknesses.
Part c: The supply chain risk landscape can change rapidly, rendering some controls ineffective if they are not regularly updated.

SR-5 Acquisition Strategies, Tools, and Methods (L)(M)(H)

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: **risk-based supplier selection criteria, digital contracts, ongoing supplier audits and compliance assessments**.

SR-5 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-5: **risk-based supplier selection criteria, digital contracts, ongoing supplier audits and compliance assessments**.
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-5 Implementation Risks
● Regular audits can require a lot of resources, particularly for a company with a large number of suppliers or global supply chains like Tesla. ● Digital platforms may require significant upfront investment in technology and staff training.

SR-6 Supplier Assessments and Reviews (M)(H)

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide **at least annually**.

SR-6 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure that their supply chain vendors build and test their systems in alignment with NIST SP 800-171 or a commensurate security and compliance framework. CSOs must ensure that vendors are compliant with physical facility access and logical access controls to supplied products.

SR-6 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-6: **at least annually.**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-6 Implementation Risks
Suppliers may lack the expertise or commitment to fully implement and maintain compliance with the NIST framework or similar standards.

SR-8 Notification Agreements (L)(M)(H)

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the **notification of supply chain compromises and results of assessment or audits**.

SR-8 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.

SR-8 Control Summary Information
Responsible Role: Quality Assurance Coordinator
Parameter SR-8: **notification of supply chain compromises and results of assessment or audits**.
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-8 Implementation Risks
● With numerous vendors in the supply chain, tracking vulnerability notifications from all suppliers becomes complex and may lead to missed or delayed responses to high-level vulnerabilities. ● An excessive volume of vulnerability notifications, especially if suppliers over-report to avoid non-compliance, can make it challenging to prioritize genuine high-risk vulnerabilities.

SR-10 Inspection of Systems or Components (L)(M)(H)

Inspect the following systems or system components **at random**, upon **detection of unusual behavior in a system or component** to detect tampering: **vehicle control system, battery and energy system, manufacturing equipment and robotics**.

SR-10 Control Summary Information
Responsible Role: Quality Assurance Coordinator
Parameter SR-10-1: **at random**
Parameter SR-10-2: **detection of unusual behavior in a system or component**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-10 Implementation Risks
● Tampering can be subtle, especially for cybersecurity attacks or hardware backdoors, which may be challenging to detect without advanced tools or methods.

SR-11 Component Authenticity (L)(M)(H)

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to **source of counterfeit component**; **Federal Trade Commission (FTC); Chief Supply Chain Manager.**

SR-11 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline.

SR-11 Control Summary Information
Responsible Role: Chief Supply Chain Manager
Parameter SR-11(b): **source of counterfeit component**; **Federal Trade Commission (FTC); Chief Supply Chain Manager.**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-11 Implementation Risks
Part a: Policies may not comprehensively cover all potential sources or types of counterfeit components.
Part b: If external reporting requirements are unclear or misinterpreted, counterfeit issues may not be properly reported.

SR-11(1) Anti-counterfeit Training (L)(M)(H)

Train **Quality Assurance Specialists** to detect counterfeit system components (including hardware, software, and firmware).

SR-11(1) Control Summary Information
Responsible Role: Quality Assurance (QA) Training Coordinator
Parameter SR-11(1): **Quality Assurance Specialists**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply):

☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-11(1) Implementation Risks
Inadequate training resources or ineffective training programs may fail to adequately prepare QA specialists to identify counterfeit components.

SR-11(2) Configuration Control for Component Service and Repair (L)(M)(H)

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: **all**.

SR-11(2) Control Summary Information
Responsible Role: Configuration Management Officer
Parameter SR-11(2): **all**
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

SR-11(2) Implementation Risks
Possibility of data loss or corruption if configuration backups are not maintained or are altered during repair.

SR-12 Component Disposal (L)(M)(H)

Dispose of **sensitive data, hardware, software components, documentation** using the following techniques and methods: **physical data destruction and digital wiping**.

SR-12 Control Summary Information
Responsible Role: Information Security Manager and personnel
Parameter SR-12-1: **sensitive data, hardware, software components, documentation**
Parameter SR-12-2: **physical data destruction and digital wiping**.
Implementation Status (check all that apply): ☐ Partially Implemented
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

SR-12 Implementation Risks
Inadequate data sanitization could lead to data breaches.

Works Cited

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector

https://www.sec.gov/Archives/edgar/data/1318605/000162828024002390/tsla-20231231.htm

https://www.tesla.com/giga-nevada

https://www.bbc.com/news/world-us-canada-56469475