**Risk Management Program Manual:**

***For The Jetson Charger Cluster-Next Gen***

# Introduction: How to Use This Manual and Why It Is Important

Cybersecurity is a critical, sometimes confusing, and complicated aspect of technology. As technology and research grows, this changes the plan and methods used to secure and provide an optimal deployment environment that must adapt to the needs of those working within this sphere. The Jetson Charger Cluster-Next Gen is not immune to such needs. It is from this need that this manual has come to fruition.

This *Risk Management Program Manual* houses critical documents, and outlines all of the major activities of the risk management process for The Jetson Charger Cluster-Next Gen and its defined project scope. From risk identification to issue-tracking and escalation, to create repeatable, iterative processes and document them in this central location in order to:

1. Standardize risk management processes.
2. Communicate processes, timelines, and results to the central risk function or stakeholders.
3. Enhance risk awareness.
4. Train Cybersecurity Engineering Students
5. Capture new knowledge through risk assessments.

**Table of Contents**

[Introduction: How to Use This Manual and Why It Is Important 1](#_Toc133259112)

[I. Introduction 4](#_Toc133259113)

[1.1 Document Version 4](#_Toc133259114)

[1.2 Document Revision History 4](#_Toc133259115)

[1.3 Executive Brief 5](#_Toc133259116)

[II. The Jetson Charger Cluster-Next Gen’s Risk Management Program 6](#_Toc133259117)

[2.1 Program Overview 6](#_Toc133259118)

[2.2 The Jetson Charger Cluster-Next Gen’s Current Risk Management Maturity 7](#_Toc133259119)

[2.3 Success Factors 8](#_Toc133259120)

[2.4 Goals and Objectives 9](#_Toc133259121)

[2.5 Metrics 11](#_Toc133259122)

[III. The JCC Cybersecurity Charter 12](#_Toc133259123)

[3.1 Cybersecurity Team Mandate 12](#_Toc133259124)

[3.2 Agenda and Responsibilities 12](#_Toc133259125)

[3.3 Meeting Schedule 13](#_Toc133259126)

[III.4 Membership 13](#_Toc133259127)

[III.5 Executive Signatures 13](#_Toc133259128)

[IV. Accountabilities and Responsibilities of Risk Management 14](#_Toc133259129)

[4.1 Accountabilities and Responsibilities of Key Stakeholders 14](#_Toc133259130)

[V. Schedule of Activities 15](#_Toc133259131)

[5.1 Identifying Risk Events 15](#_Toc133259132)

[Engage Key Stakeholders 15](#_Toc133259133)

[Review Risk Categories 15](#_Toc133259134)

[Risk Identification Processes 17](#_Toc133259135)

[Responsible Party 17](#_Toc133259136)

[Timing and Frequency 17](#_Toc133259137)

[5.2 Cataloging Risk Events 17](#_Toc133259138)

[Responsible Party 17](#_Toc133259139)

[Timing and Frequency 17](#_Toc133259140)

[5.3 Assessing Risk Severity 18](#_Toc133259141)

[Unacceptable Risk Threshold 18](#_Toc133259142)

[Probability and Impact Severity Thresholds and How to Properly Calculate Them 18](#_Toc133259143)

[Proximity Considerations 22](#_Toc133259144)

[Frequency Considerations 22](#_Toc133259145)

[Responsible Party 22](#_Toc133259146)

[Timing and Frequency 22](#_Toc133259147)

[5.4 Risk Event Accountabilities and Monitoring Responsibilities 22](#_Toc133259148)

[Responsible Party 22](#_Toc133259149)

[Timing and Frequency 22](#_Toc133259150)

[5.5 Selecting Risk Responses 23](#_Toc133259151)

[Cost-Benefit Analysis (CBA) 23](#_Toc133259152)

[Responsible Party 23](#_Toc133259153)

[Timing and Frequency 23](#_Toc133259154)

[5.6 Risk Reporting 23](#_Toc133259155)

[Appendix A: Risk and Mitigation Report 24](#_Toc133259156)

[Risk Assessment and Mitigation Report 24](#_Toc133259157)

[Appendix B: Threat Model 40](#_Toc133259158)

[Threat Model: *For The Jetson Charger Cluster-Next Gen* 40](#_Toc133259159)

[Threat Modeling Background 40](#_Toc133259160)

[Threat Modeling for The JCC 40](#_Toc133259161)

# Introduction

## 1.1 Document Version

|  |  |
| --- | --- |
| **Document Number** | JCCCT1 |
| **Revision Number** | 1 |
| **Effective Date** | April 13, 2023 |
| **Owner** | Svetlana Freeman |
| **Approver** | Dr. DJ Hovermale |

## 1.2 Document Revision History

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Revision Description** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 

## 1.3 Executive Brief

The Risk Management Program Manual serves to describe the processes, procedures, and activities that are necessary to maintain risk governance, identify IT-related or cyber risks, assess risk severity, and determine appropriate risk responses for The Jetson Charger Cluster-Next Gen (JCC). The program manual and its supporting documents (see Appendix) will be used to document detailed information regarding key risks and provide appropriate mechanisms for reporting these risks to the Lead Computer Systems Engineer, System Administrator, and Lab Manager at The University of Alabama in Huntsville (UAH) for the Engineering Building. The Risk Management Program Manual was developed with the guidance of Info-Tech’s *Build a Business Driven IT Risk Management**Program*blueprint, Ken Piddington VP and CIO at US Silica, and Dr. DJ Hovermale Clinical Assistant Professor, college of Business at The University of Alabama in Huntsville.

The *Risk Register Tool* will be used to track risks and determine appropriate risk responses, and the blueprint will walk you through how to effectively employ these tools, as well as exercises to optimize IT risk management processes. The Program Manual should be updated after completing each phase of the blueprint.

The Risk Management Program Manual will exist as a digital copy and a hard copy, located in the UAH Engineering Building with the System Administrator and any future JCC sponsor.

As part of good risk management practices, the Program Manual must be reopened during JCC maintenance and presented to any oncoming senior design team who takes on this task in the future.

Any changes to the *Risk Management Program Manual* should be documented in Section 1.2.

# The Jetson Charger Cluster-Next Gen’s Risk Management Program

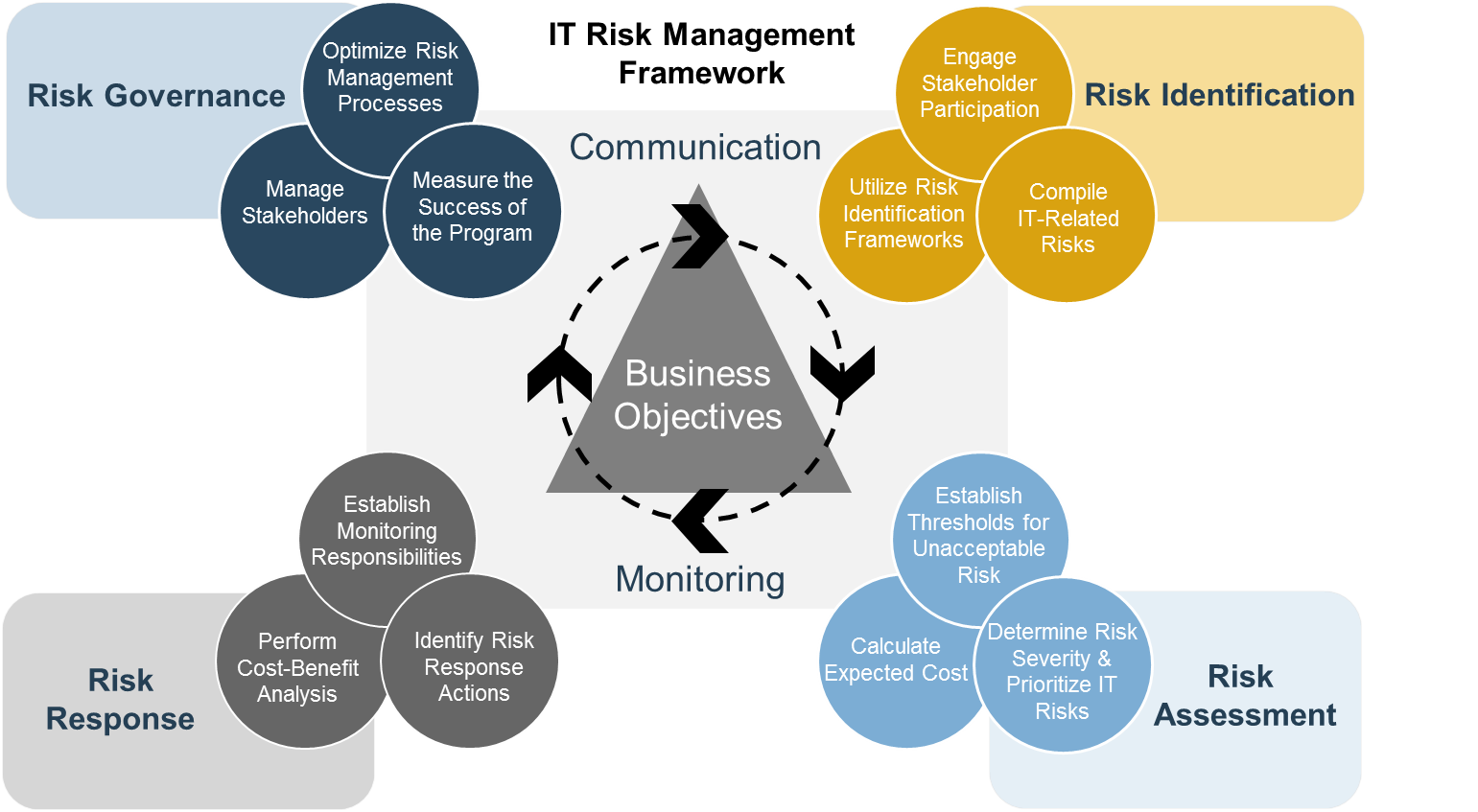
## 2.1 Program Overview

The intention of the risk management program for The Jetson Charger Cluster-Next Gen (JCC) is to instill best-practice risk management activities that allow us to proactively identify, assess, and respond to risks. The program formalizes risk management by encouraging the regular tracking of risks, assigning responsibility to individuals for monitoring and managing risks instead of leaving it to chance, and establishing risk responses to identified threats and vulnerabilities.

In addition, the risk management program for the JCC aims to foster further communication between the entire JCC team and stakeholders, and within the ECE department itself. Central to JCC’s Risk Management Framework is the continuous monitoring and communication of risk with appropriate stakeholders.

JCC’s Risk Management Framework is composed of four major pillars that govern risk management practices that have been modified to fit the scope of this project.

1. **Risk Governance** – Ensure that the JCC’s Cybersecurity Team’s risk management practices are aligned to organizational risk management standards and that stakeholders are aware of and accountable for severe risks.
2. **Risk Identification** – Ensure that all risks are identified through comprehensive stakeholder participation and the use of four risk identification methodologies combined at its core with the STRIDE Risk Assessment Model and specifically molded for the JCC’s and its scope.
3. **Risk Assessment** – Ensure that all risks are evaluated based on probability and impact using 4 different risk assessment methodologies: Standard Risk Calculation, NIST Based Risk Calculation, DREAD Based Risk Calculation, and Info Tech’s Risk Standard Risk Calculation Method to understand the severity of the JCC’s risk portfolio and prioritize risks based on their respective severity.
4. **Risk Response** – Ensure that key risks are responded to appropriately.



*Basis for the JCC’s Risk Management Framework*

## 2.2 The Jetson Charger Cluster-Next Gen’s Current Risk Management Maturity

| **Risk Management Process** | **Current Process Practices** | **Maturity Level** |
| --- | --- | --- |
| **Risk Governance** | 1. A dedicated Cybersecurity Team exists to consider risk. 2. The team meets at regular intervals and receives review and input from stakeholders. 3. Risk events are owned and monitored by specific individuals. 4. Stakeholder specific meetings are held to ensure they are always consulted. 5. Senior Cybersecurity Industry Professionals review all documents and sign off on all action plans pertaining to Cybersecurity and Risk Events. 6. Accountability for executing the risk management program is held by the JCC’s Cybersecurity Team. 7. Accountability for risk decisions is held by Dr. Wells and Dave Foreman upon the JCC’s deployment. | Current: Initial |
| **Risk Identification** | 1. The Cybersecurity and the System Administrator for UAH’s ECE department possesses a risk register that is updated to reflect the JCC’s overall risk portfolio in respect to its project scope. 2. Risk identification exercises are conducted based on the JCC’s senior design assignment cycle. 3. The risk list is developed and updated collaboratively with key stakeholders. 4. Risk events are brainstormed using high-level risk categories and then refined using Senior Cybersecurity Industry Professional’s input. | Current: Initial |
| **Risk Assessment** | 1. Formal risk assessment exercises are conducted based on the JCC’s senior design assignment cycle. 2. Unacceptable risk thresholds are dictated by the ECE departments System Administrator and appropriate stakeholders. 3. All identified risk events are assigned a severity level based on probability and impact assessments. 4. Key Senior Cybersecurity Industry Professionals and stakeholders participate in risk assessment exercise guidance and review. 5. Four customized alternative risk assessment methodologies and used to ensure risk events are appraised appropriately. | Current: Initial |
| **Risk Response** | 1. Response options are brainstormed for all risks exceeding thresholds for acceptable risk. 2. Each risk event is reassessed for residual risk. 3. Responses are selected based on the JCC Cybersecurity Team’s capabilities and resources to implement controls. 4. All risk response recommendations are presented to stakeholders for approval. | Current: Initial |
| **Risk Monitoring & Reporting** | 1. Risk owners are assigned to specific risk events or risk areas. 2. Key risk indicators (KRIs) and thresholds are developed to track changes in risk severity for specific risk event areas. 3. Protocols have been established to escalate risks when thresholds have been breached for specific risk event areas. 4. Risks are reported according to an enforced reporting schedule. 5. KRIs, thresholds, and reporting schedules have been approved by stakeholders. | Current: Initial |

## 2.3 Success Factors

The success of the Risk Management Program for The Jetson Charger Cluster-Next Gen is dependent upon not just the JCC’s Cybersecurity Team but the entirety of the JCC’s Development team’s ability to align and communicate with the stakeholder’s core risk management function, established project scope, and resources they are willing to provide. Success factors for The Jetson Charger Cluster-Next Gen’s Risk Management Program are therefore driven by the JCC Team and stakeholder’s awareness and support of the Risk Management Program developed by the JCC’s Cybersecurity Team. Beyond awareness and support, to succeed all parties need to acknowledge that risk is an organizational wide issue that needs to be addressed down to the individual level and that responsibility acknowledged by all leadership. That thought itemized out and within the scope of the JCC’s Risk Management success factors are as follows:

1. **Support and Sponsorship from our Stakeholders and UAH ECE Department IT Leadership**
   1. For the scope of this project our Stakeholders and UAH ECE Department IT Leadership can be considered, what most organizations refer to as, their senior leadership.
   2. Senior leadership sponsorship increases the likelihood that risk management is prioritized and receives the necessary resources and attention to ensure that risk accountability is shared by senior leadership.
2. **Organizational Risk Culture and Awareness**
   1. The organization embraces new policies and processes that reflect a proactive approach to risk.
   2. The organization cultivates an environment of mentorship for the exploration and development of not only cyber professionals but future industry professionals to consciously realize and equate for security in their environments and product development.
   3. Risk culture is embedded in the curriculum and project assignments and assessments to reflect risk management responsibilities essential to maintaining and innovating the JCC, the future cyber professionals involved, and the assets at stake.

## 

## 2.4 Goals and Objectives

The primary goal of The Jetson Charger Cluster-Next Gen’s Risk Management Program is to instill risk management best-practices, reduce organizational exposure to risks that may affect the continuity of The Jetson Charger Cluster-Next Gen’s value proposition in relation to UAH’s ECE Department. In addition, it must assist with the education of future cybersecurity industry professionals, because it has to handle and assess risk across modular asset scopes. The Jetson Charger Cluster-Next Gen’s Risk Management Program enables the JCC Cybersecurity Team and the ECE department’s System Administrator to make proactive decisions in conjunction with and regarding preventable risks that have the potential to impact UAH ECE Departments business and educational continuity. Through effective risk identification, assessment, response, and monitoring, risk management enables the strategic vision of The Jetson Charger Cluster-Next Gen and its implementation by reducing the reactive nature of risk management and implementing appropriate actions to minimize risk to the organization. Additionally, The Jetson Charger Cluster-Next Gen’s Risk Management Program effectively aims to:

| **Goal** | **Objectives/Initiatives** | **Additional Notes** |
| --- | --- | --- |
| Ensure that The Jetson Charger Cluster-Next Gen’s exposure to risks that affect the continuity of our stakeholder’s value proposition is minimized. | * Identify and assess all risks that expose the organization. * Mitigate severe risks. * Monitor key risks that have potential to become severe. | This is in respect to project scope and adjacent JCC team’s component completion. |
| Ensure that the JCC’s Cyber and IT managed component is compliant with external laws and regulations. | * Review IT compliance laws and regulatory rules. * Conduct audits to ensure compliance is maintained. | If the JCC is used on a larger scale, such as for a class, or is handed to another research or senior design group. Audits need to be scheduled in more frequent intervals |
| Ensure JCC’s Cyber and IT managed component provides support for organization’s compliance. | * Identify relevant organization compliance rules. * Conduct an annual review of The JCC’s Risk Management Program alignment with organizational standards. | Under the assumption The Jetson Charger Cluster is and will be an annual senior design project until completion. |
| Ensure the JCC Cybersecurity Team regularly communicates potential costs, benefits, and risks to the organization. | * Reduce the frequency of miscommunication between the JCC Cybersecurity Team, adjacent JCC Teams, stakeholders, and the organization. | Due to the potential change of project hands, the goal is to establish the framework of communication for the next JCC Cybersecurity element. |
| Ensure that information and data are secured within the organization. | * Limit frequency and severity of security breaches. | This is done in conjunction with the UAH CPE Department System Administrator. |
| Ensure that the JCC’s Cyber and IT managed component services are delivered in line with stakeholder and organization requirements. | * Identify and mitigate critical risks that may disrupt organization and project-critical IT services. |  |
| Ensure the JCC Cybersecurity projects are completed on-time and within scope. | * Limit the impact of unforeseen risks associated with project complication. | The Cybersecurity Component of the JCC is dependent on Adjacent Team’s and their workflow completions. This can lead to missed milestones and changes in project scope. |

*Cybersecurity and its management are living evolving processes so revise the above goals, objectives, and initiatives as needed.*

## 

## 2.5 Metrics

The JCC’s Cybersecurity Team has developed the following metrics to measure the success of The Jetson Charger Cluster-Next Gen’s Risk Management Program for the scope of the current project life cycle. Should this project be taken up by another senior design or research deal these metrics will be revised to fit the scope and cybersecurity necessity of their design phases. For product deployment, metrics will have to be more frequent and built around fast risk reaction and response.

| **Name** | **Method** | **Base-line** | **Target** | **Deadline** | **Check-point 1** | **Check-point 2** | **Final** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Number of risks identified** | Risk Register | 0 | ~10 | January. 25 | 6 | 8 | 8 |
| **Number of project units represented (risk identification)** | Meeting minutes | 0 | 5 | April. 25 | 2 | 6 | 8 |
| **Frequency of risk assessment** | Assessments recorded in Program Manual | 0 | 3/throughout 2022-2023 Project Life. | April. 25 | 2 | 2 | 3 |
| **Number of top risks without an identified risk response** | Risk register | 8 | 0 | February. 20 | 5 | 2 | 0 |
| **Risk Management, Mitigation, and Control Implementation** | Software scripts attached and their instructions. Command and settings instructions | 0 | 5 | April. 25 | 2 | 4 | 5 |
| **Risk Management, Mitigation, and Control Implementation Testing** | Test reports and evaluations on failures and successes | 0 | 5 | April. 25 | 0 | 3 | 5 |

# The JCC Cybersecurity Charter

The JCC Cybersecurity Team in conjunction with UAH’s ECE Department System Administrator and Lab Manager serves as a formalized task force that is responsible for ensuring that the risk management program is initiated, optimized, and maintained through regular assessment and review even after the current project lifecycle. Dr. Wells, the current project sponsor, holds the task along with associated stakeholders to ensure the risk management program and all associated documentation is passed to the next senior design or research team and encourage them to build and adapt this framework to help strengthen it and the project associated with it.

The Risk Management Program is responsible for integrating risk management into regular research and development practices. The Jetson Charger Cluster-Next Gen’s Cybersecurity Team and associated university partners and stakeholders integrate Risk Management into the project’s agenda and priorities.

## 3.1 Cybersecurity Team Mandate

The JCC Cybersecurity Team oversees the risk management processes for The Jetson Charger Cluster-Next Gen. Members of the JCC Cybersecurity Team are appointed, currently, by Svetlana Freeman and are accountable to the entire JCC team and associated stakeholders. The Cybersecurity Team will:

1. Provide risk management leadership for the JCC through the alignment of cyber-secure strategic objectives and processes with organizational and operational strategic objectives and processes.
2. Prioritize all cybersecurity risk exposures and thresholds within the project scope and resolve resource allocation issues based on risk prioritization.
3. Ensure optimal risk management through measurement of key success metrics.
4. Ensure open communication between the JCC Cybersecurity Team, their affiliated entities, other functional units of The Jetson Charger Cluster-Next Gen, and the project stakeholders so as to promote collaborative risk management and overall project success.

The JCC Cybersecurity Team is not responsible in any way for UAH’s ECE department’s operating budget, department staff, or any other aspect of day-to-day operations affiliated with the ECE department’s personnel. Nor is the JCC Senior Design Team for the 2022-2023 school year responsible for the furthering, continuation, and maintenance of this project and its Cybersecurity element after May 4th, 2023.

## 3.2 Agenda and Responsibilities

The agenda of a typical Cybersecurity meeting will include the following items:

1. Identify and review major risks prevalent in The Jetson Charger Cluster-Next Gen and associated assets.
2. Recommend an appropriate risk appetite or level of exposure for in The Jetson Charger Cluster-Next Gen
3. Review the assessment of the impact and likelihood of identified risks from the project in its research and development process.
4. Review the risk events.
5. Create a response plan to avoid, mitigate, transfer, or accept a risk event.
6. Review and communicate overall risk impact and risk management success.
7. Assign risk ownership responsibilities of key risks to ensure they are monitored, and risk responses are effectively implemented.
8. Address any concerns with regards to the risk management program, including but not limited to:
   1. Reviewing risk management duties, Risk Management Program success, Risk management resourcing.
9. Communicate risk reports to stakeholders.
10. Make any alterations as needed to the team roster and the individuals’ responsibilities as needed and document those changes.

## 3.3 Meeting Schedule

The JCC Cybersecurity Team will meet as much as it needs and if a matter requires follow-up, subsequent meetings will be planned as needed and documented until May 4th, 2023**.**

## Membership

All members of the JCC Cybersecurity Team and affiliated members should be very familiar with the stakeholder’s organization’s policies, procedures, and practices. Additionally, all members should have the authority to make decisions based on the information the stakeholder and the associated organization has provided and not provided, and take actions on behalf of the project, organization, and stakeholder unit they represent.

If any member (not applicable to adjacent members/advisors) is unable to attend the majority of the JCC Cybersecurity Team meetings, then they will be messaged independently with tasks and their absence will be recorded unless a reason for the absences is provided. The same applies to the JCC Cybersecurity Team lead.

JCC Adjacent Team Leads are required at JCC Cybersecurity Team meetings to provide project insight and help direct cybersecurity direction and scope.

Members of the JCC Cybersecurity Team include:

* Svetlana Freeman – Cybersecurity Team Lead
* Satyo Wasistho – Software Mitigation and Controls Specialist and Software Lead

Adjacent Team Advisors

* Dr. DJ Hovermale – Subject Matter Expert and Security Consultant
* Ken Piddington – Subject Matter Expert and Security Consultant
* Dave Foreman – UAH ECE Department Lead Computer Systems Engineer and System Administrator
* Chris Hardy – UAH ECE Department Lab Manager

JCC Adjacent Team Members that are Required:

* Jordan Thomas – Hardware Team Lead

## Executive Signatures

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_  
Name Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_  
Name Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_  
Name Signature Date

# Accountabilities and Responsibilities of Risk Management

## 4.1 Accountabilities and Responsibilities of Key Stakeholders

The success of the Risk Management program relies on clear articulation of risk management accountabilities and responsibilities. The JCC Cybersecurity Team will be responsible or accountable for the bulk of activities but success will also be dependent on buy-in and endorsement by external stakeholders beyond the Cybersecurity Team. These stakeholders must be aware of the Risk Management Program and are often consulted or informed about important risk management activities.

| **Stakeholder** | **Stakeholder Coordination** | **Risk Identification** | **Risk Thresholds** | **Risk Assessment** | **Identify Responses** | **Monitoring** | **Risk Decision- Making** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Dr. Wells** | C | I | C | I | I | I | C |
| **Dr. Jovanov** | C | I | I | I | I | I | I |
| **System Admin** | C | C | C | C | C | C | C |
| **Lab Manager** | I | I | I | I | I | I | I |
| **Adjacent Advisors** | C | C | C | C | C | C | C |
| **Adjacent JCC Teams** | A | A | C | C | A | I | I |
| **JCC Cyber Team** | R | R | R | R | R | R | R |

**Legend:**

R – Responsible

A – Accountable

C – Consulted

I – Informed

# Schedule of Activities

The Risk Management Program is made up of several separate but mutually reinforcing processes – some of which are to be conducted periodically, and others that are ongoing throughout the project and development lifetime. The following schedule outlines the timing and frequency for risk management processes, as well as their specific activities and tasks.

## 5.1 Identifying Risk Events

Risk identification is the most vital exercise of risk management and takes place in close tandem with and integrated into The Jetson Charger Cluster-Next Gen research and development process to ensure that all cyber-related threats and vulnerabilities are identified within the scope of the project. The JCC Cybersecurity Team uses the risk identification framework developed by Info-Tech Research Group and can be found in the *Build a Business-Driven IT Risk Management Program*blueprint.

### Engage Key Stakeholders

Comprehensive risk identification requires the engagement of key stakeholders within and outside of the perceived scope of cybersecurity. Typically, during risk identification exercises, the Cybersecurity Team will engage stakeholders that meet the following criteria:

1. Significant reliance on cybersecurity services and technologies to achieve assigned project objectives.
2. Strong relationship with The Jetson Charger Cluster-Next Gen project and willingness to engage in risk management activities.
3. Unique perspectives, skills, and experiences that the cybersecurity team may not possess.

Key stakeholders to complete the risk identification activities will include:

* Svetlana Freeman – Cybersecurity Team Lead
* Satyo Wasistho – Software Mitigation and Controls Specialist and Software Lead
* The entire Jetson Charger Cluster-Next senior design team
* Dr.Wells – Project Sponsor and Senior Design Professor
* Dr.Jovanov – Senior Design Professor
* Dave Forman – UAH ECE System Administrator
* Chris Hardy – UAH ECE Lab Manager
* UAH ECE Department and subsequent associated classes and coursework

### Review Risk Categories

By using the STRIDE threat model as a basis for threat modeling and risk identification, the JCC Cybersecurity Team is able to integrate security into the design and development of to The Jetson Charger Cluster-Next Gen allowing for an emersed cybersecurity and risk identification approach to the project. STRIDE breaks down threats into six high-level groupings that are specified for research and design project level functions where risks are frequently presented. Risk categories are complemented by risk scenarios which represent common risk groups that are more specific than each risk category. The six risk categories and their basic criteria and associated risk scenarios are as follows:

1. **Spoofing**
   1. Property Violated
      1. Authentication
   2. Threat Definition
      1. Impersonating something or someone else
   3. Examples/Risk Scenarios of Spoofing
      1. Email Spoofing: an attacker sends an email from what appears to be a legitimate address/sender, but it is forged.
      2. DNS Spoofing: this is a scenario where an attacker alters the DNS server’s response to the victim’s query.
2. **Tampering**
   1. Property Violated
      1. Integrity
   2. Threat Category Definition
      1. Modifying data or code
   3. Examples/Risk Scenarios of Tampering
      1. Code Injection: in this risk scenario, attacks inject malicious code into a software application to disrupt intended functionality in an exploitable manner.
      2. Man-in-the-Middle (MitM) Attack: this risk scenario involves an attacker intercepting communication and intercepting or modifying it typically then forwarding the communication to its intended recipient after the tampering process is complete.
3. **Repudiation**
   1. Property Violated
      1. Non-repudiation
   2. Threat Category Definition
      1. Claiming innocence or denying responsibility can be honest or fake.
   3. Examples/Risk Scenarios of Repudiation
      1. Digital Signature Spoofing: in this risk scenario an attacker spoofs a digital signature to make it appear if a legitimate user has or was the one who performed the transaction or signed a document. This allows the attacker to repudiate or deny their involvement in the transaction or document.
      2. Replay Attacks: in this risk scenario an attacker records a transaction that is legitimate and later replays it to carry out the same transaction multiple times. The attack can deny any involvement and claim the repeated transactions were not of their doing.
4. **Information Disclosure** 
   1. Property Violated
      1. Confidentiality
   2. Threat Category Definition
      1. Information is disclosed to unauthorized personnel.
   3. Examples/Risk Scenarios of Information Disclosure
      1. SQL Injection: this is a risk scenario where an attacker injects malicious SQL code into a web application’s input field. This action allows the attacker to gain unauthorized access to information the database may store.
      2. Cross-Site Scripting (XSS): in this risk scenario an attacker will malicious code into a web page that the victim visits, allowing them to steal sensitive information such as cookies or credentials.
5. **Denial of Service**
   1. Property Violated
      1. Availability
   2. Threat Category Definition
      1. Deny, degrade, or exhaust resources needed to provide a service to users.
   3. Example/Risk Scenarios of Denial of Service
      1. Distributed Denial of Service (DDoS): this risk scenario is characterized by an attacker using a network of compromised devices to flood a target system or network with traffic requests making it unavailable to legitimate users and other damages.
      2. UDP Flood: in this risk scenario an attacker sends a large number of User Datagram Protocol (UDP) packets to a target system to overwhelm it and to prevent legitimate traffic from being processed.
6. **Elevation of Privilege**
   1. Property Violated
      1. Authorization
   2. Threat Category Definition
      1. The gain of capabilities, usually of a higher order, without proper authorization.
   3. Example/Risk Scenarios of Elevation of Privilege
      1. Social Engineering: this is a risk scenario where an attack will manipulate a legitimate user into providing them with privileges access through various methods that may include posing as a work superior or even as a friend.
      2. Password Cracking: in this risk scenario an attacker will use brute force or other methods to crack a password that may lead to an elevated access to a system and its information.

### Risk Identification Processes

To complete the risk identification exercise, the JCC Cybersecurity Team frequently reviews current project processes and functionality to identify additional risk events associated with each process as the project proceeds.

### Responsible Party

Risk events will be identified by the JCC Cybersecurity Team.

### Timing and Frequency

Risk events will be identified as The Jetson Charger Cluster-Next Gen adjacent teams provide functionality and bring asset systems online to allow them to have their risk assessed and these assessments will be reviewed on a weekly basis or as needed.

## 5.2 Cataloging Risk Events

Identified risk events are documented in the *Risk Register Tool* to prepare for risk assessment. The corresponding risk category will also be tracked in the tool. An identification tag will be assigned to each risk event to perpetually track that unique risk. As risk events occur, they are tracked in the *Risk Register Tool* which assesses and logs Risk Events through four different risk assessment methodologies: Standard Risk Calculation, NIST Based Risk Calculation, DREAD Based Risk Calculation, and Info Tech’s Risk Standard Risk Calculation Method that rest atop the STRIDE Risk Identification Model.

### Responsible Party

Risk events will be documented and tracked in the *Risk Register Tool* by the JCC Cybersecurity Team.

### Timing and Frequency

Risk events will be cataloged on a weekly basis and realized risk events will be documented as they occur.

## 

## 5.3 Assessing Risk Severity

Risk Severity is calculated to help the JCC Cybersecurity Team understand which of the current risk events represent the most significant threat to the organization and are most in need of a response. Risk severity is determined via a two-level approach. First, all identified risk events are evaluated using four different risk assessment methodologies: Standard Risk Calculation, NIST Based Risk Calculation, DREAD Based Risk Calculation, and Info Tech’s Risk Standard Risk Calculation Method that rest atop the STRIDE Risk Identification Model. A Risk Severity Level Assessment is conducted by creating scales for risk probability and impact, which inform an overall severity rating.

### Unacceptable Risk Threshold

Before determining scales for probability and impact, the JCC Cybersecurity Team must adopt the UAH ECE Department’s threshold for unacceptable risk for peripheral education devices. This value is determined or approved by the stakeholders and affiliated adjacent team advisors. Any risk event severity that exceeds this threshold mustbe acted upon. This threshold should reflect UAH ECE Department’s ability to absorb financial losses and reflect its organizational appetite and tolerance for risk for peripheral education devices.

### Probability and Impact Severity Thresholds and How to Properly Calculate Them

The JCC Cybersecurity Team uses the following severity scales associated with the four risk assessment methodologies molded to accurately assess risk with respect to the JCC’s project scope to properly determine the severity of risk events:

***Standard or Simple Risk Calculation***

Simple Risk is referred to as such because the method used for calculating it comes from the most widely taught and distributed risk calculation method. Selecting the value of Impact and Likelihood from a 1-10 scale. Then using the formula of Likelihood x Impact = Risk to calculate the total risk of each risk event.

Graphical user interface, application

Description automatically generated

*Graphic Explanation of Simple Risk and its Evaluation Method*

***NIST Based Risk Calculation***

National Institute of Standards and Technology (NIST) sets security standards across numerous industries and due to this fact, the Cybersecurity team determined it was part of due diligence to assess The Jetson Charger Cluster’s risk using a tailored version of NIST’s Risk Management Framework (RMF). RMF uses a simple 1-10 likelihood scale like Simple Risk but goes a step further when it comes to assessing the impact a particular risk event can have on a team, organization, or product. The project or product scope determines the included categories for generating the combined impact assessment. For the JCC, the impact was broken into 4 sub-categories: Team Reputational Cost, Direct Business and or Monetary Costs, Reputational Costs for the University of Alabama in Huntsville (UAH), and Internal Culture Costs. Each risk event is given a 1-10 score for each impact category and then added together to generate the total impact and then added with the likelihood score to generate the total risk calculation.

|  |  |
| --- | --- |
| **NIST Impact Factors** | |
| **Noncompliance Costs:** Regulatory fines, litigation costs, remediation costs, etc. (Replaced with Team Reputational Costs) | |
| **Direct Business Costs:** Revenue or performance loss from customer abandonment or avoidance, etc. | |
| **Reputational Costs:** Brand damage, loss of customer trust, etc. | |
| **Internal Culture Costs:** Impact on capability of organization/unit to achieve vision/mission. Consider the impact on productivity/employee morale stemming from conflicts with internal cultural values or ethics. | |
| **Other:** Any other costs that an organization wants to consider. | |
| *All likelihood and Impact factors are added together for the final risk calculation and use the simple risk 1-10 scale.*  *Graphic Explanation of NIST Risk and its Evaluation Method* |  |

***DREAD Based Risk Calculation***

DREAD is a slightly different risk assessment model than the standard calculation methods. It assesses risk events based on the damage, reproducibility, exploitability, number of affected uses, and discoverability of each event. Each category gets a 1-10 score, and they are added together and divided by 5 to get the final risk score for the event. DREAD is not native to being mapped on a matrix, but the team attempted to model it in such a way for uniformity. Though it is more native to a timeline or one-dimensional approach. Both were modeled for the sake of a thorough assessment model.

|  |  |
| --- | --- |
| **DREAD Risk Individual Components Value/Calculations** | |
| **Component** | **Value Guide** |
| Damage Potential | **0** = Nothing |
| **5** = Information disclosure that could be used in combination with other vulnerabilities |
| **8** = Individual/employer non sensitive user data is compromised. |
| **9** = Administrative non sensitive data is compromised. |
| **10** = Complete system or data destruction. |
| **10** = Application unavailability. |
| Reproducible | **0** = Very hard or impossible, even for administrators of the application. |
| **5** = Complex steps are required for authorized user. |
| **7.5** = Easy steps for Authenticated user |
| **10**=Just a web browser and the address bar are sufficient, without authentication. |
| Exploitability | **2.5** = Advanced programming and networking knowledge, with custom or advanced attack tools. |
| **5**=Exploit exits in public, using available attack tools. |
| **9** = A Web Application Proxy tool |
| **10** = Just a web browser |
| Affected Users | **0** = None |
| **2.5=**individual/employer that is already compromised. |
| **6** = some users of individual or employer privileges, but not all. |
| **8** = Administrative users |
| **10** = All users |
| Discover-ability | **0** = Very hard requires source code or administrative access. |
| **5** = Can figure it out by monitoring and manipulating HTTP requests |
| **8** = Details of faults like this are already in the public domain and can be easily discovered using a search engine. |
| **10** = the information is visible in the web browser address bar or in a form. |

**DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5**

*Graphic Explanation of DREAD Risk and its Evaluation Method*

**Info-Tech Risk Calculation**

Info-Tech Research Group is an information technology research group that specializes in IT best practices research and education. They have a wide scope of influence on the cybersecurity industry and its leaders. Their methodologies have led the Cybersecurity team to evaluate the probability and impact using a nine-scale categorization scale where typically anything in the range of moderate and above falls into the category of intolerable risk.

|  |  |
| --- | --- |
| **Probability and Impact Level** | **Occurrence Criteria**  (Classification; probability of risk event within one year) |
| Level 1 – Negligible | Negligible; <5% |
| Level 2 – Very Low | Very Unlikely; 5–15% |
| Level 3 – Low | Unlikely; 15–25% |
| Level 4 – Moderately Low | Somewhat Possible; 25–40% |
| Level 5 – Moderate | Possible; 40–60% |
| Level 6 – Moderately High | Possibly Likely; 60–75% |
| Level 7 – High | Likely; 75–85% |
| Level 8 – Very High | Very Likely; 85–95% |
| Level 9 – Extreme | Extremely Likely; >95% |

*Graphic Explanation of Info-Tech Research Risk and its Evaluation Method*

Diagram

Description automatically generated

*Graphic Example of Info-Tech Research Risk and its Evaluation Method and its Implementation*

### Proximity Considerations

The severity of a risk event can fluctuate over time. This characteristic of risk is called risk proximity. These fluctuations are often unpredictable; however, when possible, information about how time will impact the risk will be documented in the *Risk Register Tool*.

### Frequency Considerations

A risk event may be expected to occur more than once within the specified time frame. Frequency is reflected in the impact and updated in the likelihood of the risk event. By adjusting the numeric value associated with the likelihood and impact up a magnitude to reflect current risk.

### Responsible Party

The organization’s threshold for (un)acceptable risk is determined or approved by the stakeholders and adjacent team advisors. Probability and impact scales are determined by the JCC Cybersecurity Team with approval and guidance from the adjacent team advisors, and then transferred to the *Risk Register Tool.*

### Timing and Frequency

Risk-related thresholds and risk-severity scales for each risk event will be reviewed on a weekly basis and as needed. A comprehensive assessment of the risk portfolio will be conducted on a bi-semesterly basis based on the assignment cycle of The Jetson Charger Cluster senior design project.

## 5.4 Risk Event Accountabilities and Monitoring Responsibilities

Every risk event in the *Risk Register Tool* must be assigned to a Risk Owner and the Risk Owners will be the acting JCC Cybersecurity team and associated stakeholders who are and will be responsible for monitoring the risk event’s severity and reporting changes at JCC Cybersecurity meetings and or informing the JCC Cybersecurity Team of the scope and acceptance of the risk and assets associated with the Charger Jetson Cluster senior design project.

**Risk Owner Responsibilities**

The responsibilities of the risk owner are:

* Monitor the risk event for changes in probability of occurrence and/or probable impact.
* Monitor changes in the market and external environment that may alter the severity of the risk event.
* Monitor changes of closely related risks that may have interdependencies.
* Develop and use KRIsto measure changes in risk severity.
* Regularly report changes in risk severity to the IT risk council
* If necessary, escalate the risk to other stakeholders or advisors for reassessment.
* Monitor risk severity levels for risk events after a risk response project is implemented.

Severe risk events that exceed the (un)acceptable risk threshold must be closely monitored and regularly reported on. Continuous monitoring, industry best practices, and oversight from senior industry cybersecurity processional will be used to ensure that changes in risk severity are detected and reported.

### Responsible Party

Risk Accountability will be assigned by associated stakeholders and the JCC Cybersecurity team.

### Timing and Frequency

Risk Accountability will be assigned at the beginning of each senior design cycle if and when a team has selected The Jetson Charger Cluster.

## 5.5 Selecting Risk Responses

All risk responses fall under one of the following categories:

1. **Avoidance** – Risk avoidance involves taking evasive maneuvers away from the risk event. Risk avoidance targets risk probability, decreasing the likelihood of the risk event occurring.
2. **Mitigation** – Risk mitigation actions are risk responses that reduce the probability and impact of the risk event. Risk mitigation actions can either be to implement new controls or enhance existing ones.
3. **Transfer –** Risk transfer is the exchange of uncertain future costs for fixed present costs. Often, the uncertain future cost of a risk event can be transferred to a third-party insurer who assumes the risk in exchange for some sort of insurance premiums.
4. **Acceptance** –Accepting a risk means absorbing the expected cost of a risk event. It is a conscious and deliberate decision to retain the threat.

### Cost-Benefit Analysis (CBA)

When selecting a risk mitigation action, the JCC Cybersecurity team should and will use a modified cost-benefit analysis to guide that fits the scope of the project assigned and the assets that pertain to it and its execution. This enables the JCC Cybersecurity Team to assess numerous risk mitigation actions and make risk-conscious investment decisions that fall within the range of acceptable tolerance.

### Responsible Party

Risk responses will be generated and assessed by the JCC Cybersecurity team and associated adjacent advisors and presented to the stakeholders for further review.

### Timing and Frequency

Risk responses will be determined once risk severities are finalized during the initial risk assessment phase.

## 5.6 Risk Reporting

Reporting requirements for risk events, including escalation protocols, are to be established and clarified by stakeholders and best practices for each risk event based on the project scope and the needs of the stakeholders. High-level summaries of the risk portfolio are communicated to the stakeholders using the Risk and Mitigation Report located in Appendix A.

**Responsible Party**The risk report will be completed by the JCC Cybersecurity Team. Specific reports on key risks will be completed upon request by the JCC Cybersecurity Team using personal knowledge and information as well as the guidance of best practices and industry professionals.

**Timing and Frequency**Risk reports will be completed on an as needed basis, at the discretion of the JCC Cybersecurity Team and when mandated by the senior leadership team.

# Appendix A: Risk and Mitigation Report

# Risk Assessment and Mitigation Report

***For The Jetson Charger Cluster-Next Gen***

**Executive Brief**

Between January 6th and February 20th of 2023, the Cybersecurity division of The Jetson Charger Cluster-Next Gen team undertook its initial risk assessment. The Cybersecurity team completed risk identification and risk assessment exercises and built risk responses for key risks that were above the organizational unacceptable risk threshold. This Risk Report documents the results of the initial review as well as numerous risk response mitigation actions for each risk event, and the Cybersecurity team’s recommendations to mitigate key risk events. The Risk Report was developed through the completion of Info-Tech’s *Build a Business-Driven IT Risk Management Program* blueprint.

The *Risk Register Tool* was used to track risks and determine appropriate risk responses.

**Results of Risk Management Activities**

**Risk Identification**

The Cybersecurity team used Info-Tech’s risk categories outlines to comprehensively identify 8 risk events that were above the organizational unacceptable risk threshold. The portfolio of risk events is documented in Info-Tech’s *Risk Register Tool*. Risk events were categorized several ways but can be best broken down using a combination of the STRIDE Risk Assessment Model:

|  |  |
| --- | --- |
| **STRIDE Risk/Threat Category** | **Number of Risk Events** |
| **S**poofing | 3 |
| **T**ampering | 1 |
| **R**epudiation | 1 |
| **I**nformation Disclosure | 1 |
| **D**enial of Service | 1 |
| **E**levation of Privilege | 1 |

**Risk Assessment**

The Cybersecurity team evaluated the severity of each risk event by assessing the probability of occurrence and impact using 4 different risk assessment methodologies: Standard Risk Calculation, NIST Based Risk Calculation, DREAD Based Risk Calculation, and Info Tech’s Risk Standard Risk Calculation Method. For the heat maps used to display the visual representation of all 4 risk assessment methodologies, green represents minimal to negligible risk, yellow is moderate, and red is high to critical risk.

|  |  |  |
| --- | --- | --- |
| **Problem Prioritization/Risk Severity Distribution Heat Map Legend** | | |
| **Threat** | **Threat Identifier** | **Point Label** |
| Spoofing | S1 | A |
| S2 | B |
| S3 | C(R) |
| Tampering | T1 | D |
| Reputation | R1 | E |
| Information Disclosure | I1 | F |
| Denial of Service | D1 | G |
| Elevation of Privilege | E1 | H |

**Simple Risk**

Simple Risk is referred to as such because the method used for calculating it comes from the most widely taught and distributed risk calculation method. Selecting the value of Impact and Likelihood from a 1-10 scale. Then using the formula of Likelihood x Impact = Risk to calculate the total risk of each risk event.

**NIST Based Risk Calculation**

National Institute of Standards and Technology (NIST) sets security standards across numerous industries and due to this fact, the Cybersecurity team determined it was in due diligence to assess The Jetson Charger Cluster’s risk using a tailored version of NIST’s Risk Management Framework (RMF). RMF uses a simple 1-10 likelihood scale like Simple Risk but goes a step further when it comes to assessing the impact a particular risk event can have on a team, organization or product. The project or product scope determines the included categories for generating the combined impact assessment. For the JCC, impact was broken into 4 sub-categories: Team Reputational Cost, Direct Business and or Monetary Costs, Reputational Costs for the University of Alabama in Huntsville (UAH), and Internal Culture Costs. Each risk event is given a 1-10 score for each impact category and then added together to generate the total impact and then added with the likelihood score to generate the total risk calculation.

**DREAD Based Risk Calculation**

DREAD is a slightly different risk assessment model than the standard calculation methods. It assesses risk events based on the damage, reproducibility, exploitability, number of affected uses, and discoverability of each event. Each category gets a 1-10 score, and they are added together and divided by 5 to get the final risk score for the event. DREAD is not native to being mapped on a matrix but the team attempted to model it in such a way for uniformity. Though it is more native to a timeline or one-dimensional approach. Both were modeled for the sake of a thorough assessment model.

**Info-Tech Risk Calculation**

Info-Tech Research Group is an information technology research group that specializes in IT best practices research and education. They have a wide scope of influence on the cybersecurity industry and its leaders. Their methodologies have led the Cybersecurity team to evaluate the probability and impact using a nine-scale categorization scale where typically anything in the range of moderate and above falls into the category of intolerable risk.

**Risk Responses**

The Cybersecurity team determined the necessary risk response for each identified risk event. There were four courses of action to describe the most appropriate risk response:

Numerouskey risksrequire additional risk response analysis by stakeholders. These risk events and their subsequent individual risk response analyses will be presented in the following section. However, key risk events under consideration for further analysis are as follows:

|  |  |
| --- | --- |
| **Risk Number** | **Risk Events** |
| R001 | An attacker can impersonate a legitimate user, student, or UAH staff, to gain access to the JCC and potentially the Blackhawk Server or Engineering Network. |
| R002 | An attacker could socially engineer their way into physical access to the JCC. |
| R003 | An attacker could use a phishing attack to get users information on access to the JCC, Blackhawk or school network. |
| R004 | An attacker could modify or corrupt data on the JCC through vulnerabilities on the software running on it, potentially in the Blackhawk server. Maybe even parts of the Engineering Building's network. |
| R005 | An attacker could deny their actions on or misuse the JCC and due to the remote capabilities also be out of punishable jurisdiction making it difficult to seek justice and for the attacker to be held accountable. |
| R006 | An attacker could gain access to sensitive or personal information on the JCC, Blackhawk, or Network without proper authorization. Possibly network vulnerabilities from improper connection to the JCC. |
| R007 | An attacker could launch a DDoS attack on the JCC, BLACKHAWK, or schools’ network. It can affect or be directed to any of the network infrastructure |
| R008 | Should the attacker gain access to the JCC they have the potential to gain access to Blackhawk and or the school’s network and escalate their privileges to gain more information or control over the system. |

**Subsequent Risk Response and Mitigation Analysis**

**Mitigation Recommendations**

|  |  |  |
| --- | --- | --- |
| **Risk Number** | **Risk Event** | **Recommended Mitigation Controls** |
| R001 | An attacker can impersonate a legitimate user, student, or UAH staff, to gain access to the JCC and potentially the Blackhawk Server or Engineering Network. | Add group policy and admin controls onto the JCC to help prevent damage even if an unauthorized user gets attacked. Hand management and control over to an experienced Cyber professional to monitor and refine controls at the end of the semester. Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. Users have a limited access to the internet when logged into the JCC environment eliminating some of potential exploitations that can be implemented on the system. |
| R002 | An attacker could socially engineer their way into physical access to the JCC. | Keep the JCC in a locked room in front of the department chair's office. If someone knows it is in there. It will have to be an inside job. |
| R003 | An attacker could use a phishing attack to get users information on access to the JCC, Blackhawk or school network. | UAH's filters are good. But ensuring users take a small refresher on the dangers of fishing before use of the JCC. This will be done by the admin. Spear fishing is unlikely because it is a very specific device. Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. |
| R004 | An attacker could modify or corrupt data on the JCC through vulnerabilities on the software running on it, potentially in the Blackhawk server. Maybe even parts of the Engineering Building's network. | Implementing Karslurm controls and maxes. Locking away potentially dangerous commands through methods like specific command interfacing. Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. Users have a limited access to the internet when logged into the JCC environment eliminating some of potential exploitations that can be implemented on the system. |
| R005 | An attacker could deny their actions on or misuse the JCC and due to the remote capabilities also be out of punishable jurisdiction making it difficult to seek justice and for the attacker to be held accountable. | Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. |
| R006 | An attacker could gain access to sensitive or personal information on the JCC, Blackhawk, or Network without proper authorization. Possibly network vulnerabilities from improper connection to the JCC. | Follows in compliance with Dave Foreman's network connection instructions so it is in proper shielding with UAH's firewall. This is hard to deal with. Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. Users have a limited access to the internet when logged into the JCC environment eliminating some of potential exploitations that can be implemented on the system. |
| R007 | An attacker could launch a DDoS attack on the JCC, BLACKHAWK, or schools' network. It can affect or be directed to any of the network infrastructure | Dave walked us through his mitigation strategy in a way to not disclose secure information but to ease out worries. But how we can mitigate it on our side is to make there be node timeout so someone can't waste or take out the JCC by node control. |
| R008 | Should the attacker gain access to the JCC they have the potential to gain access to Blackhawk and or the school’s network and escalate their privileges to gain more information or control over the system. | Add group policy and admin controls onto the JCC to help prevent damage even if an unauthorized user gets attacked. Hand management and control over to an experienced Cyber professional to monitor and refine controls at the end of the semester. Have logging of all activity and activity of interest is saved. Logged and sent to the admin for an alert. (Every couple of months logs with non-flagged information will be cleared.). So, this will give as much data as humanly possible so we can catch who/what it is while it is happening or before it gets out. Users have a limited access to the internet when logged into the JCC environment eliminating some of potential exploitations that can be implemented on the system. |

**Risk Reassessment: Estimated Change to Likelihood and Impact of Risk Event/Threat**

**Simple Risk**

**Side by Side of Simple Risk Before and After Proposed Mitigations**

***In purple is the updated Risk***

Chart

Description automatically generated

**NIST Based Risk Calculation**

**Side by Side of NIST Based Risk Before and After Proposed Mitigations**

***In purple is the updated Risk***

Chart, scatter chart

Description automatically generated

**DREAD Based Risk Calculation**

**Side by Side of DREAD Based Risk Before and After Proposed Mitigations**

***In purple is the updated Risk***

Chart, scatter chart

Description automatically generated

**Info-Tech Risk Calculation**

**Recommendations**

The above graphs represent the expected risk of each event after the recommended mitigation controls have been put in place. Although implementing some of these controls may seem tedious, they reduce the probability of occurrence to almost nothing. Therefore, the JCC’s Cybersecurity team strongly recommends the utilization of the **JCC Risk Management Manual,** and its occupying deliverablesfor the risk management and control of the JCC but leaves any further mitigation up to the discretion of UAH’s system administrators and project stakeholders.

**Executive Signatures**

**Selected Risk Response:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

By signing below, you indicate that you:

1. Are aware of the above risk and its potential impact on business objectives.
2. Support the risk assessment conducted by the JCC Cybersecurity Team.
3. Support the plan of action and monitoring responsibilities proposed by the JCC Cybersecurity Team.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_  
Name Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_  
Name Signature Date

# Appendix B: Threat Model

# Threat Model: *For The Jetson Charger Cluster-Next Gen*

## Threat Modeling Background

A threat model is used to help cybersecurity professionals identify possible risk vectors by allowing them to put assets into perspective through visual and or interactive means. A threat model allows for perspective and can manage scope when performing a risk assessment of a system. It is commonly used in conjunction with a formal risk assessment to ensure a thorough review of attack surfaces.

## Threat Modeling for The JCC

The JCC’s cybersecurity with the aid of UAH’s ECE Department’s System Administrator and Adjacent Cybersecurity Advisors constructed a threat model to ensure the completeness of the JCC’s risk assessment and in turn the success of the JCC’s risk mitigation strategies.

Diagram

Description automatically generated

*The Visual Representation of The JCC’s Threat Model*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Special thanks to Info-Tech for their blueprints and Ken Piddington who provided them. These documents are intended to supply general information only and are not intended to be used as a substitute for any kind of professional advice.