# Autymate
# Cyber Security Risk Assessment

## December 29, 2019

*Confidential*

**Report Type: Tier 3**
**Date of Assessment: 12/30/2019**
**Report Version: 0.9.7**

**Prepared by CyberGRX**

# Table of Contents

## Legal Disclaimer

CyberGRX has prepared this Tier 3 assessment at the request of the client to whom it is furnished. The client agrees that reports and information received from CyberGRX, including this report, are strictly confidential and are intended solely for the private and exclusive use of client. The opinions and findings contained in this report are based upon information sources provided by the company being assessed and our experience in the field of third party security assessment. This is not an audit, but moreover provides a detailed account of the organization's security maturity and capabilities.

This risk assessment report was developed by CyberGRX under the authorization of the assessed company. The findings in this report are intended only for the client to whom this report is furnished, and any other parties that the assessed company grants approval through the CyberGRX platform. CyberGRX assumes no direct, indirect, or consequential liability to any third party or any other person who is not the intended addressee of this report for the information contained herein, its interpretation or applications, or for omissions, or for reliance by any such third party or other person thereon. Statements herein concerning financial, regulatory, or legal matters should be understood to be general observations based solely on CyberGRX's experience in third party security assessment, and may not be relied upon as financial, regulatory, or legal advice, which CyberGRX is not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas.

The findings in this report cannot be disclosed or shared with any additional parties without approval from the assessed company through the CyberGRX platform. No information can be reproduced in part or its entirety without expressed written consent from both the assessed company and CyberGRX. CyberGRX may use these findings in aggregate for the development of cyber risk insights and trends.

THIS REPORT DOES NOT CONSTITUTE A RECOMMENDATION, ENDORSEMENT, OPINION, OR APPROVAL OF ANY KIND WITH RESPECT TO ANY TRANSACTION OR DECISION, AND SHOULD NOT BE RELIED UPON AS SUCH UNDER ANY CIRCUMSTANCES.

## Assessment Scope

CyberGRX has performed this Tier 3 assessment on Autymate. The CyberGRX risk assessment is focused on measuring the overall maturity of a third party's enterprise security program and the existence of controls, not an assessment of a specific third party system or application.

The scope of this assessment includes Autymate's enterprise cyber security program, unless otherwise stated in the title of this assessment. CyberGRX assessments evaluate five control groups: Strategic, Operational, Core, Management, and GDPR to determine risk over a broad set of controls.

CyberGRX prepared the accompanying cyber security risk assessment of Autymate. The identification of inherent risk, residual risk, and control gaps are based on the potential risk present in Autymate's operating industry and the implementation of security controls by Autymate.

The questionnaire focuses on two dimensions: control family maturity and control completeness. The maturity models gauge the overall maturity (on a scale of 0-5) of people, process and technology employed by the organization across 25 different control families. The control completeness contains questions to determine the existence of each control. Together, this assessment will provide a detailed account of the organizational security maturity and completeness of control implementation.

**Please refer to the Assessor Statement for further details.**

## Section 1. Third Party Risk Assessment "At a Glance"

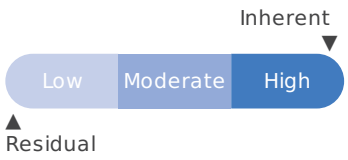
This section provides high level results of the risk assessment for Autymate controls assessment based on a maturity model and completeness of control implementation.

### Controls Assessment

| Control Group | Maturity | Trend | Group Coverage % | Trend | Family Coverage % | | Trend |
|---|---|---|---|---|---|---|---|
| 1.0 Strategic<br>- 4 Control Families<br>- 16 Controls | 4.79 Adaptive | ↔ 0% Constant | 100% Complete — 16 of 16 Controls | ↔ 0% Constant | 1.1 Cyber Security Risk Management | 100% | ↔ |
| | | | | | 1.2 Cyber Security Organization and Governance | 100% | ↔ |
| | | | | | 1.3 Cyber Security Policy and Standards | 100% | ↔ |
| | | | | | 1.4 Cyber Security Audit and Compliance | 100% | ↔ |
| 2.0 Operational<br>- 6 Control Families<br>- 24 Controls | 4.78 Adaptive | ↔ 0% Constant | 100% Complete — 24 of 24 Controls | ↔ 0% Constant | 2.1 Prepare - Threat Management | 100% | ↔ |
| | | | | | 2.2 Prevent - Vulnerability Management | 100% | ↔ |
| | | | | | 2.3 Detect - Security Operations | 100% | ↔ |
| | | | | | 2.4 Respond - Security Incident Response | 100% | ↔ |
| | | | | | 2.5 Recover - Service Restoration | 100% | ↔ |
| | | | | | 2.6 Business Resiliency | 100% | ↔ |
| 3.0 Core<br>- 8 Control Families<br>- 31 Controls | 4.80 Adaptive | ↔ 0% Constant | 100% Complete — 30 of 31 Controls | ↔ 0% Constant | 3.1 Business Process Protection | 100% | ↔ |
| | | | | | 3.2 End User Protection | 100% | ↔ |
| | | | | | 3.3 Identity and Access Management | 100% | ↔ |
| | | | | | 3.4 Application and Services Security | 100% | ↔ |
| | | | | | 3.5 Data Protection | 100% | ↔ |
| | | | | | 3.6 Endpoint Security | 100% | ↔ |
| | | | | | 3.7 Network and Boundary Security | 100% | ↔ |
| | | | | | 3.8 Facility Security | 100% | ↔ |
| 4.0 Management<br>- 8 Control Families<br>- 33 Controls | 4.43 Adaptive | ↔ 0% Constant | 97% Complete — 32 of 33 Controls | ↔ 0% Constant | 4.1 Asset Management | 100% | ↔ |
| | | | | | 4.2 Change and Configuration Management | 100% | ↔ |
| | | | | | 4.3 Enterprise Security Architecture Management | 100% | ↔ |
| | | | | | 4.4 Security Controls Management | 100% | ↔ |
| | | | | | 4.5 Security Controls Performance Management | 100% | ↔ |
| | | | | | 4.6 Third Party Risk Management | 100% | ↔ |
| | | | | | 4.7 Human Capital Management | 100% | ↔ |
| | | | | | 4.8 Information Sharing and Partnerships | 75% | ↔ |

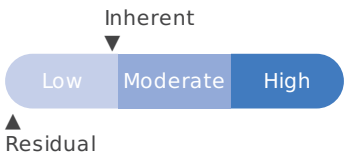
### Residual Risk Assessment

**Data Loss**



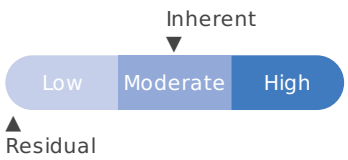

↔ 0% Constant

**Disruptive Attack**



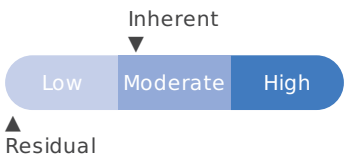

↔ 0% Constant

**Destructive Attack**




↔ 0% Constant

**Fraud**




↔ 0% Constant

## Section 2. Company Background

### Autymate

**Name:** Autymate

**Address:** 3221 Ruckriegel Pkwy, B, Louisville, KY, 40299

**Number of Full Time Employees:** 5

**Business Classification:**

- **Economic Sector(s):** Industrials
- **Business Sector(s):** Industrial & Commercial Services
- **Industry Group(s):** Professional & Commercial Services
- **Industry(ies):** Business Support Services
- **Activity(ies):** Data Processing Services

**Website:** autymate.com

## Section 3. Assessment Results

The following sections explore the results of the CyberGRX assessment on Autymate.

Section 3A explores the potential or inherent risk of an organization based on the likelihood and impact of various attack scenarios using industry and threat intelligence data.

Section 3B explores the maturity of an organization's cyber security program and the effectiveness of their control implementation as a means to mitigate inherent risk.

Section 3C explores the remaining or residual risk of an organization based on those inherent risks that have weak or non-existent controls as mitigating factors.

| Section 3A<br>Inherent Risk | Section 3B<br>Controls Assessment | Section 3C<br>Residual Risk |
|---|---|---|
| **The potential risk of a third party based on the likelihood and impact of potential threats and attack scenarios based on the current threat environment** | **A measure of cyber security program maturity and controls existence** | **The remaining risk of a third party based on control gaps identified during the assessment** |

## Section 3A. Inherent Risk

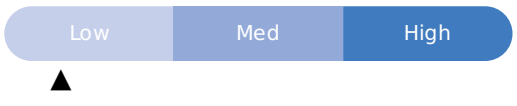
Understand the potential or inherent risks - in terms of likelihood and impact - that a third party presents in the absence of controls or other mitigating factors. The likelihood of an attack is addressed by assessing an organization's surface area (size, complexity, and interdependence) and identifying any recent cyber incidents experienced by your organization or other incidents within the industry; impact is assessed by considering the typical connectivity between a third party and a typical customer based on the third party's industry and services provided.

### Inherent Risk Likelihood: Attack Surface

Attack surface is a critical factor in determining the likelihood of an attack on the third party and is based on three dimensions: size, complexity, and interdependence over the full asset stack. The larger, more complex, and more reliant on external parties, the larger the exposure to potential threats.

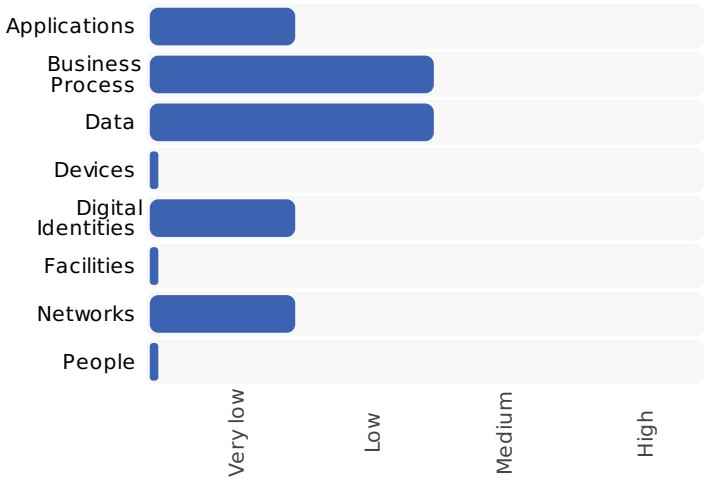
### Overall Exposure

Overall exposure due to third party size, complexity, and interdependence:



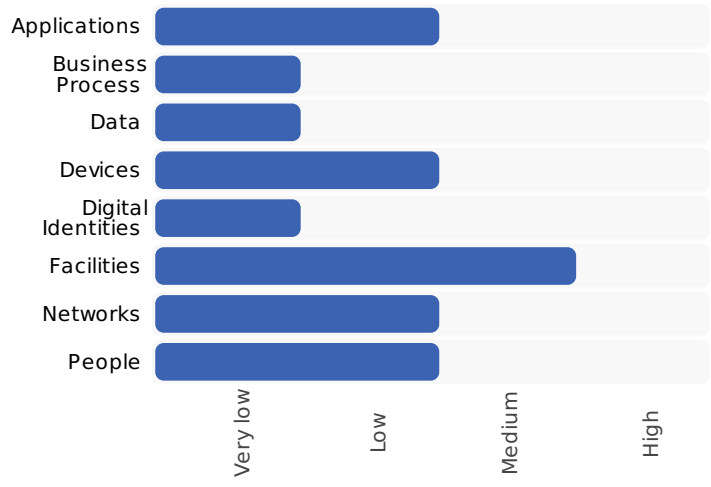

**Size**

**The number and scale of organizational activities.**



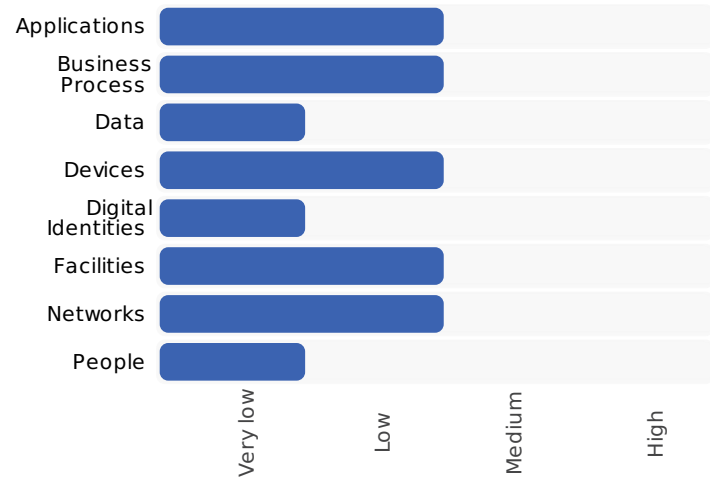

**Complexity**

**The level and variety of interconnection, distribution, and integration of organizaitonal activities.**




**Interdependence**

**The degree of reliance on third parties to manage organizational activities.**



## Inherent Risk Likelihood: Cyber Incidents in the Business Support Services Industry

Cybersecurity incidents experienced in the last 12 months, with quarterly trending, by the Business Support Services Industry through Dec 29, 2019

### Data Loss

Attacks or inadvertent usage that results in exposure or loss of sensitive information.

**Examples:** Unauthorized access, disclosure of personally identifiable information, theft of intellectual property; accidental disclosure of personal health information.

**36463** dataloss Incidents

↓ **-78.5%** Decrease

### Disruptive Attack

Attacks that degrade performance or interrupt the flow of information, reducing the overall system effectiveness.

**Examples:** Denial of service attacks, domain name system hijacking, and website defacement.

**103** disruptive Incidents

↓ **-96.6%** Decrease

### Destructive Attack

Attacks that render a device or application unusable without complete rebuild, or that deny access to a system.

**Examples:** Ransomware, logic bombs, source code destruction, destructive malware.

**811** destructive Incidents

↓ **-90.7%** Decrease

### Fraud

Attacks that use deception or target the integrity of business process, leading to non-compliance, asset loss or financial manipulation and misrepresentation.

**Examples:** Social media disinformation campaigns, CEO fraud (“Business E-mail Compromise”), wire transfer compromise, financial statement manipulation.

**910** fraud Incidents

↓ **-92.3%** Decrease

## Inherent Risk: Reported Cyber Incidents

The third party has self-reported the following cyber and data incident information for the last 12 months or since the last CyberGRX assessment. Incident classification is based on the severity of the incident experienced by the third party as follows:

**N/A:** Incident type does not apply to the organization or no incidents shared.

**Very Low:** Operational cost fully absorbed by existing business as usual allocations; limited (short-term) negative local or social media coverage; may result in additional legal regulatory scrutiny, but fines are unlikely; negligible impact on enterprise value.

**Low:** Significant cost experienced by the third party in excess of business as usual allocations, but not material to earnings; negative national or social media coverage; regulatory action likely to result in fines; impact to enterprise value.

**Medium:** Cost experienced has an impact on earnings in a single quarter; sustained or substantive negative national or social media coverage; regulatory action or civil suit with material impact to earnings in a single quarter; impact to the ability to raise capital and fund planned acquisitions.

**High:** Cost experienced has an impact on full-year earnings affecting balance sheet or threatening liquidity; substantial negative shift in public/partner perceptions; regulatory action forces significant change to business model, regulatory fine or civil suit with material impact to balance sheet; impact to enterprise value threatens ability to fund operations.

### Data Loss

N/A | Very Low | Low | Medium | **High** ▲

### Disruptive Attack

N/A | Very Low | Low | Medium | **High** ▲

### Destructive Attack

N/A | Very Low | Low | Medium | **High** ▲

### Fraud

N/A | Very Low | Low | Medium | **High** ▲

## Inherent Risk: Overall Risk

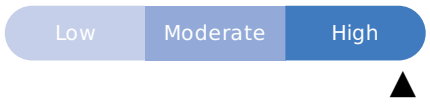
The overall inherent risk is determined by analyzing responses for surface area, identified recent cyber incidents against your organization or industry, and the asset criticality typical to a third party operating in a particular industry and providing a particular service.

### Data Loss Risk

Risk associated with the theft of inadvertent disclosure of sensitive information.

**Primary Use Case Drivers**

An internal user steals third party IP residing on internal servers
An outsider steals customer data from an internal database
An internal user copies and steals physical documents containing third party IP



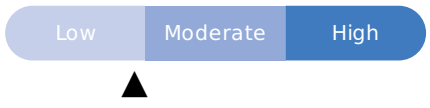

↔ 0%
Constant

### Disruptive Attack Risk

Risk associated with attacks intended to disrupt the flow of information or business processes and risk associated with attacks intended to degrade critical applications, data or systems.

**Primary Use Case Drivers**

A network-level DDoS attack causes disruption
A DNS reflection DDoS attack causes disruption
An NTP reflection DDoS attack causes disruption




↔ 0%
Constant

### Destructive Attack Risk

Risk associated with attacks intended to destroy a critical asset so it cannot perform its intended function and risk associated with attacks intended to deny users from accessing critical assets.

**Primary Use Case Drivers**

Ransomware encrypts critical data
An outsider uses malware to delete critical data
An outsider deletes critical data


↔ 0%
Constant

### Fraud Risk

Risk associated with deception intended to manipulate a person or system by targeting the integrity of and corrupting processes, data or systems and risk associate with influence intended to cause others to behave in a manner favorable to the actor.

**Primary Use Case Drivers**

An outsider executes fraudulent wire transfers
An outsider tricks a company official into transferring funds to an outside account
An outsider steals payroll through altered payee data


↔ 0%
Constant

## Section 3B. Detailed Control Assessment Review

This section provides the output of the control assessment at the control family level.

| | Maturity | Coverage |
|---|---|---|
| **High Risk** | 0.00 to 2.00 | 0% to 50% |
| **Med Risk** | 2.01 to 3.50 | 51% to 75% |
| **Low Risk** | 3.51 to 5.00 | 76% to 100% |

### Maturity Scores and Control Coverage Percentage (Framework View)

This view, organized by the CyberGRX integrated cyber security controls framework,shows the control group maturity scores as well as maturity and coverage scores of the associated control families.

| | Maturity | Coverage | Validity |
|---|---|---|---|
| **1: Strategic Controls**<br>Risk Management, Accountability, Codification, and Compliance. | 4.8 | 100% | |
| 1.1 Cyber Security Risk Management | 4.9 | 100% | |
| 1.2 Cyber Security Organization and Governance | 4.7 | 100% | |
| 1.3 Cyber Security Policy and Standards | 4.8 | 100% | |
| 1.4 Cyber Security Audit and Compliance | 4.8 | 100% | |
| **2: Operational Controls**<br>Focus on Day-to-Day Information Protection. | 4.8 | 100% | |
| 2.1 Prepare - Threat Management | 4.8 | 100% | |
| 2.2 Prevent - Vulnerability Management | 4.8 | 100% | |
| 2.3 Detect - Security Operations | 4.8 | 100% | |
| 2.4 Respond - Security Incident Response | 4.8 | 100% | |
| 2.5 Recover - Service Restoration | 4.8 | 100% | |
| 2.6 Business Resiliency | 4.8 | 100% | |
| **3: Core Controls**<br>Full spectrum of controls - preventive, detective, and responsive - to protect all asset layers (stack) of the organization. | 4.8 | 100% | |
| 3.1 Business Process Protection | 4.8 | 100% | |
| 3.2 End User Protection | 4.8 | 100% | |
| 3.3 Identity and Access Management | 5.0 | 100% | |
| 3.4 Application and Services Security | 5.0 | 100% | |
| 3.5 Data Protection | 5.0 | 100% | |
| 3.6 Endpoint Security | 4.8 | 100% | |
| 3.7 Network and Boundary Security | 4.8 | 100% | |
| 3.8 Facility Security | 4.3 | 100% | |
| **4: Management Controls**<br>Foundational capabilities necessary to provide a well-managed security program. | 4.4 | 97% | |
| 4.1 Asset Management | 4.4 | 100% | |
| 4.2 Change and Configuration Management | 4.4 | 100% | |
| 4.3 Enterprise Security Architecture Management | 5.0 | 100% | |
| 4.4 Security Controls Management | 4.4 | 100% | |
| 4.5 Security Controls Performance Management | 4.8 | 100% | |
| 4.6 Third Party Risk Management | 4.3 | 100% | |
| 4.7 Human Capital Management | 4.3 | 100% | |
| 4.8 Information Sharing and Partnerships | 3.8 | 75% | |

## Control Family Maturity (List View)

This view shows the control family maturity scores organized from lowest maturity to highest maturity.

| | |
|---|---|
| **High Risk** | 0.00 to 2.00 |
| **Med Risk** | 2.01 to 3.50 |
| **Low Risk** | 3.51 to 5.00 |

| Control Family | Score | Validity |
|---|---|---|
| 4.8 Information Sharing and Partnerships | 3.8 | |
| 3.8 Facility Security | 4.3 | |
| 4.6 Third Party Risk Management | 4.3 | |
| 4.7 Human Capital Management | 4.3 | |
| 4.1 Asset Management | 4.4 | |
| 4.2 Change and Configuration Management | 4.4 | |
| 4.4 Security Controls Management | 4.4 | |
| 1.2 Cyber Security Organization and Governance | 4.7 | |
| 1.3 Cyber Security Policy and Standards | 4.8 | |
| 1.4 Cyber Security Audit and Compliance | 4.8 | |
| 2.1 Prepare - Threat Management | 4.8 | |
| 2.2 Prevent - Vulnerability Management | 4.8 | |
| 2.3 Detect - Security Operations | 4.8 | |
| 2.4 Respond - Security Incident Response | 4.8 | |
| 2.5 Recover - Service Restoration | 4.8 | |
| 2.6 Business Resiliency | 4.8 | |
| 3.1 Business Process Protection | 4.8 | |
| 3.2 End User Protection | 4.8 | |
| 3.6 Endpoint Security | 4.8 | |
| 3.7 Network and Boundary Security | 4.8 | |
| 4.5 Security Controls Performance Management | 4.8 | |
| 1.1 Cyber Security Risk Management | 4.9 | |
| 3.3 Identity and Access Management | 5 | |
| 3.4 Application and Services Security | 5 | |
| 3.5 Data Protection | 5 | |
| 4.3 Enterprise Security Architecture Management | 5 | |

## Control Family Coverage Percentage (List View)

This view shows the control family coverage organized from lowest to highest control coverage percentage.

| | |
|---|---|
| **High Risk** | 0% to 50% |
| **Med Risk** | 51% to 75% |
| **Low Risk** | 76% to 100% |

| Control Family | Coverage | Validity |
|---|---|---|
| 4.8 Information Sharing and Partnerships | 75% | |
| 1.1 Cyber Security Risk Management | 100% | |
| 1.2 Cyber Security Organization and Governance | 100% | |
| 1.3 Cyber Security Policy and Standards | 100% | |
| 1.4 Cyber Security Audit and Compliance | 100% | |
| 2.1 Prepare - Threat Management | 100% | |
| 2.2 Prevent - Vulnerability Management | 100% | |
| 2.3 Detect - Security Operations | 100% | |
| 2.4 Respond - Security Incident Response | 100% | |
| 2.5 Recover - Service Restoration | 100% | |
| 2.6 Business Resiliency | 100% | |
| 3.1 Business Process Protection | 100% | |
| 3.2 End User Protection | 100% | |
| 3.3 Identity and Access Management | 100% | |
| 3.4 Application and Services Security | 100% | |
| 3.5 Data Protection | 100% | |
| 3.6 Endpoint Security | 100% | |
| 3.7 Network and Boundary Security | 100% | |
| 3.8 Facility Security | 100% | |
| 4.1 Asset Management | 100% | |
| 4.2 Change and Configuration Management | 100% | |
| 4.3 Enterprise Security Architecture Management | 100% | |
| 4.4 Security Controls Management | 100% | |
| 4.5 Security Controls Performance Management | 100% | |
| 4.6 Third Party Risk Management | 100% | |
| 4.7 Human Capital Management | 100% | |

## Section 3C. Residual Risk

Residual risk is the portion of inherent risk that has not or cannot be reduced through effective control implementation and remain a threat to the organization.

### Residual Risk: Top Risks

The top risks that are more likely to impact a company are identified by using data about an organization's operating industry and asset exposure. Residual risk can be identified by evaluating the highest risk use cases associated with operating in a particular industry, mapping key controls to those use cases, and evaluating control performance.

Control gaps are derived by analyzing available organizational and asset exposure data to determine the highest impact use cases to an organization. By aligning controls to the use cases and threat models, inherent risk can be identified. Lastly, through the control assessment, security gaps represent residual risk.

| 1. Risk Identification | 2. Inherent Risk | 3. Control Assessment | | 4. Residual Risks | | |
|---|---|---|---|---|---|---|
| **Attack Scenarios** | **Risk Rating** | **Associated Control Families** | **Control Coverage** | **Control Gaps** | **Residual Risk Rating** | **Mitigation Strategy** |
| An internal user steals third party IP residing on internal servers | High | 2.4: Respond - Security Incident Response | 100 | 2.4.3: Incident Containment | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 2.4.4: Threat Removal | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.2: End User Protection | 100 | 3.2.1: Employee and Contractor Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.3: Identity and Access Management | 100 | 3.3.1: Identity Authorization | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.3.2: Identity Authentication | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.6: Endpoint Security | 100 | 3.6.1: Desktop and Laptop Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.6.2: Server Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.6.3: Virtualization Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |

## Third Party-Driven Risk: Top Risks (Continued)

| 1. Risk Identification | 2. Inherent Risk | 3. Control Assessment | | 4. Residual Risks | | |
|---|---|---|---|---|---|---|
| **Attack Scenarios** | **Risk Rating** | **Associated Control Families** | **Control Coverage** | **Control Gaps** | **Residual Risk Rating** | **Mitigation Strategy** |
| An internal user steals third party IP residing on internal servers | High | 3.7: Network and Boundary Security | 100 | 3.7.2: Network Security Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| An outsider steals customer data from an internal database | High | 2.4: Respond - Security Incident Response | 100 | 2.4.3: Incident Containment | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 2.4.4: Threat Removal | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.2: End User Protection | 100 | 3.2.1: Employee and Contractor Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.3: Identity and Access Management | 100 | 3.3.1: Identity Authorization | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.3.2: Identity Authentication | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.4: Application and Services Security | 100 | 3.4.3: Application and Services Security - Production | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.5: Data Protection | 100 | 3.5.2: Data at Rest Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.6: Endpoint Security | 100 | 3.6.1: Desktop and Laptop Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.6.2: Server Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.6.3: Virtualization Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |

## Third Party-Driven Risk: Top Risks (Continued)

| 1. Risk Identification | 2. Inherent Risk | 3. Control Assessment | | 4. Residual Risks | | |
|---|---|---|---|---|---|---|
| **Attack Scenarios** | **Risk Rating** | **Associated Control Families** | **Control Coverage** | **Control Gaps** | **Residual Risk Rating** | **Mitigation Strategy** |
| An outsider steals customer data from an internal database | High | 3.7: Network and Boundary Security | 100 | 3.7.2: Network Security Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| An internal user copies and steals physical documents containing third party IP | High | 2.4: Respond - Security Incident Response | 100 | 2.4.3: Incident Containment | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 2.4.4: Threat Removal | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.2: End User Protection | 100 | 3.2.1: Employee and Contractor Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.3: Identity and Access Management | 100 | 3.3.1: Identity Authorization | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.5: Data Protection | 100 | 3.5.2: Data at Rest Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| An outsider executes fraudulent wire transfers | Medium | 2.4: Respond - Security Incident Response | 100 | 2.4.3: Incident Containment | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 2.4.4: Threat Removal | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.2: End User Protection | 100 | 3.2.1: Employee and Contractor Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.3: Identity and Access Management | 100 | 3.3.2: Identity Authentication | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.6: Endpoint Security | 100 | 3.6.1: Desktop and Laptop Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |

## Third Party-Driven Risk: Top Risks (Continued)

| 1. Risk Identification | 2. Inherent Risk | 3. Control Assessment | | 4. Residual Risks | | |
|---|---|---|---|---|---|---|
| **Attack Scenarios** | **Risk Rating** | **Associated Control Families** | **Control Coverage** | **Control Gaps** | **Residual Risk Rating** | **Mitigation Strategy** |
| An outsider executes fraudulent wire transfers | Medium | 3.7: Network and Boundary Security | 100 | 3.7.2: Network Security Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 3.7.3: Network Content Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| An internal user steals physical documents containing third party customer data | Medium | 2.4: Respond - Security Incident Response | 100 | 2.4.3: Incident Containment | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | | | 2.4.4: Threat Removal | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |
| | | 3.2: End User Protection | 100 | 3.2.1: Employee and Contractor Protection | Low | No remediations recommended, but this remains a low risk due to the current threat environment. |

## Section 4. Detailed Control Assessment

This section provides a deep dive into each control family scoring in terms of maturity and completeness.

### Family 1.1: Cyber Security Risk Management

Establish a cyber security risk management program that effectively evaluates, mitigates, and monitors cyber security risk across the enterprise.

#### Control Family Maturity


↔ 0%
Constant

#### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

#### Control Completeness

1.1 Cyber Security Risk Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **1.1.1 Risk Planning**<br>Implemented: Yes |
| **1.1.2 Risk Assessment**<br>Implemented: Yes |
| **1.1.3 Risk Mitigation**<br>Implemented: Yes |
| **1.1.4 Risk Monitoring**<br>Implemented: Yes |

## Family 1.2: Cyber Security Organization and Governance

Establish a comprehensive cyber security program with clear leadership structure, a budget, and executive oversight to create a culture of accountability and awareness for cyber security.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

1.2 Cyber Security Organization and Governance
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **1.2.1 Cyber Security Organization and Leadership**<br>Implemented: Yes |
| **1.2.2 Cyber Security Plan and Budget**<br>Implemented: Yes |
| **1.2.3 Cyber Security Governance**<br>Implemented: Yes |
| **1.2.4 Cyber Security Communications**<br>Implemented: Yes |

## Family 1.3: Cyber Security Policy and Standards

Establish a cyber security policy and standards program that effectively creates, implements, and continuously measures the effectiveness of cyber security policy and standards.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

1.3 Cyber Security Policy and Standards
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **1.3.1 Cyber Security Policy and Standards Framework**<br>Implemented: Yes |
| **1.3.2 Cyber Security Policy and Standards Development**<br>Implemented: Yes |
| **1.3.3 Cyber Security Policy and Standards Approval and Dissemination**<br>Implemented: Yes |
| **1.3.4 Cyber Security Policy and Standards Effectiveness**<br>Implemented: Yes |

## Family 1.4: Cyber Security Audit and Compliance

Establish an independent audit and compliance function that routinely audits your cyber security controls based on enterprise policy and standards, to quickly and effectively identify cyber security gaps and ensures regulatory compliance.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

1.4 Cyber Security Audit and Compliance
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **1.4.1 Cyber Security Audit and Compliance Design**<br>Implemented: Yes |
| **1.4.2 Cyber Security Audit and Compliance Communications**<br>Implemented: Yes |
| **1.4.3 Cyber Security Audit and Compliance Assessments**<br>Implemented: Yes |
| **1.4.4 Cyber Security Audit and Compliance Remediation**<br>Implemented: Yes |

## Family 2.1: Prepare - Threat Management

Create a threat management program that leverages threat analysis and performs threat assessments to proactively identify, prioritize, and respond to current and emerging threats in the environment.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.1 Prepare - Threat Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **2.1.1 Threat Management Planning**<br>Implemented: Yes |
| **2.1.2 Threat Analysis**<br>Implemented: Yes |
| **2.1.3 Threat Assessment**<br>Implemented: Yes |
| **2.1.4 Threat Management Enhancements**<br>Implemented: Yes |

## Family 2.2: Prevent - Vulnerability Management

Establish a vulnerability management framework that identifies, prioritizes, and effectively remediates vulnerabilities in the environment.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.2 Prevent - Vulnerability Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **2.2.1 Vulnerability Management Planning**<br>Implemented: Yes |
| **2.2.2 Vulnerability Assessment**<br>Implemented: Yes |
| **2.2.3 Vulnerability Remediation and Patch Management**<br>Implemented: Yes |
| **2.2.4 Vulnerability Remediation Verification**<br>Implemented: Yes |

## Family 2.3: Detect - Security Operations

Ensure threats are effectively detected and addressed through the collection, correlation, and alerting of known signatures, unknown attacks, and abnormal behavior.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.3 Detect - Security Operations
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **2.3.1 Collect - Data Ingestion and Management**<br>Implemented: Yes |
| **2.3.2 Assess - Security Alerting and Analytics**<br>Implemented: Yes |
| **2.3.3 Decide - Visualization and Decision Support**<br>Implemented: Yes |
| **2.3.4 Act - Event Management and Incident Escalation**<br>Implemented: Yes |

## Family 2.4: Respond - Security Incident Response

Establish a cyber security incident response framework that effectively validates, contains, and removes a security incident from the environment.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.4 Respond - Security Incident Response
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **2.4.1 Incident Validation**<br>Implemented: Yes |
| **2.4.2 Incident Classification**<br>Implemented: Yes |
| **2.4.3 Incident Containment**<br>Implemented: Yes |
| **2.4.4 Threat Removal**<br>Implemented: Yes |

## Family 2.5: Recover - Service Restoration

Establish cyber security incident recovery procedures to effectively mitigate, remediate, and investigate security incidents while ensuring systems are restored and key stakeholders are notified.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.5 Recover - Service Restoration
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **2.5.1 Restore Normal Operations**<br>Implemented: Yes |
| **2.5.2 Incident Investigations and Forensics**<br>Implemented: Yes |
| **2.5.3 Mitigation and Reporting**<br>Implemented: Yes |
| **2.5.4 Lessons Learned and Sharing**<br>Implemented: Yes |

## Family 2.6: Business Resiliency

Leverage a business impact analysis (BIA) to establish a business continuity plan (BCP)  that drives contingency plans with recovery objectives, regular testing and updates.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

2.6 Business Resiliency
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
|---|
| **2.6.1 Business Resiliency Requirements**<br>Implemented: Yes |
| **2.6.2 Business Continuity Plan**<br>Implemented: Yes |
| **2.6.3 Business Continuity Plan (BCP) Testing**<br>Implemented: Yes |
| **2.6.4 Business Continuity Plan Updates**<br>Implemented: Yes |

## Family 3.1: Business Process Protection

Ensure business processes are effectively protected through the monitoring of enterprise and regulatory policy and standards adherence, asset misappropriation fraud protection capabilities, and financial statement fraud protection.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.1 Business Process Protection
Number of Controls: 3

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **3.1.1 Compliance Management**<br>Implemented: Yes |
| **3.1.2 Asset Misappropriation Fraud Protection**<br>Implemented: Yes |
| **3.1.3 Financial Statement Fraud Protection**<br>Implemented: Yes |

## Family 3.2: End User Protection

Protect company personnel and customer information through background checks, cyber security awareness training, continuous monitoring of potentially malicious activity, and effective response capabilities.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.2 End User Protection
Number of Controls: 3

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **3.2.1 Employee and Contractor Protection**<br>Implemented: Yes |
| **3.2.2 Customer Protection**<br>Implemented: Yes |
| **3.2.3 Secure Traveler Protection**<br>Implemented: Yes |

## Family 3.3: Identity and Access Management

Ensure the protection of user, device, and system identities and credentials from compromise through established identity authorization, authentication, access management, directory services, and certificate management capabilities.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.3 Identity and Access Management
Number of Controls: 5

100% Coverage

↔ 0% Constant

| Control |
|---|
| **3.3.1 Identity Authorization**<br>Implemented: Yes |
| **3.3.2 Identity Authentication**<br>Implemented: Yes |
| **3.3.3 Access Management**<br>Implemented: Yes |
| **3.3.4 Directory Services**<br>Implemented: Yes |
| **3.3.5 Certificate Management**<br>Implemented: Yes |

## Family 3.4: Application and Services Security

Protect applications and services from compromise through the use of application and services security measures that secure the development and production of all applications and services.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.4 Application and Services Security
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **3.4.1 Application and Services Security Planning**<br>Implemented: Yes |
| **3.4.2 Application and Services Security - Development**<br>Implemented: Yes |
| **3.4.3 Application and Services Security - Production**<br>Implemented: Yes |
| **3.4.4 Software-as-a-Service (Saas) Protection**<br>Implemented: Yes |

## Family 3.5: Data Protection

Protect sensitive information from being stolen, altered, destroyed or disrupted through the use of data and key management best practices, and data at rest, data in use, and data in motion protection capabilities.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.5 Data Protection
Number of Controls: 6

100% Coverage

↔ 0% Constant

| Control |
|---|
| **3.5.1 Data Management**<br>Implemented: Yes |
| **3.5.2 Data at Rest Protection**<br>Implemented: Yes |
| **3.5.3 Data in Use Protection**<br>Implemented: Yes |
| **3.5.4 Data in Motion Protection**<br>Implemented: Yes |
| **3.5.5 Key Management**<br>Implemented: Yes |
| **3.5.6 Cloud Data Protection**<br>Implemented: Yes |

## Family 3.6: Endpoint Security

Protect desktops and laptops, servers, virtualized endpoints and mobile devices from compromise through secure hardening, malware protection, endpoint application control, intrusion detection and prevention, host-based firewalls, and continuous monitoring.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.6 Endpoint Security
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **3.6.1 Desktop and Laptop Protection**<br>Implemented: Yes |
| **3.6.2 Server Protection**<br>Implemented: Yes |
| **3.6.3 Virtualization Protection**<br>Implemented: Yes |
| **3.6.4 Mobile Device Protection**<br>Implemented: Yes |

## Family 3.7: Network and Boundary Security

Protect the network through the use of network device hardening, firewall capabilities, intrusion detection and prevention systems (IDPS), denial of service protection, segmentation, rogue device detection, e-mail filtering and web filtering.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.7 Network and Boundary Security
Number of Controls: 3

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **3.7.1 Network Routing Protection**<br>Implemented: Yes |
| **3.7.2 Network Security Protection**<br>Implemented: Yes |
| **3.7.3 Network Content Protection**<br>Implemented: Yes |

## Family 3.8: Facility Security

Protect the facility perimeter, interior, and physical property from compromise by using external and internal access controls, delivery screening areas, video surveillance, perimeter guards, and robust response capabilities.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

3.8 Facility Security
Number of Controls: 3

100%
Coverage

↔ 0%
Constant

| Control |
| --- |
| **3.8.1 Facility Perimeter Protection**<br>Implemented: Yes |
| **3.8.2 Facility Interior Protection**<br>Implemented: Yes |
| **3.8.3 Physical Property Protection**<br>Implemented: NA |

## Family 4.1: Asset Management

Effectively manage assets through asset planning, acquisition, inventory, and retirement.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.1 Asset Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.1.1 Asset Management Planning**<br>Implemented: Yes |
| **4.1.2 Asset Acquisition**<br>Implemented: Yes |
| **4.1.3 Asset Inventory and Use**<br>Implemented: Yes |
| **4.1.4 Asset Retirement**<br>Implemented: Yes |

## Family 4.2: Change and Configuration Management

Ensure configuration changes are securely managed through the identification and implementation of change and the effective remediation of deviations.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.2 Change and Configuration Management
Number of Controls: 5

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.2.1 Configuration Management Planning**<br>Implemented: Yes |
| **4.2.2 Configuration Management Design and Implementation**<br>Implemented: Yes |
| **4.2.3 Configuration Change Detection and Alerting**<br>Implemented: Yes |
| **4.2.4 Configuration Change Response and Remediation**<br>Implemented: Yes |
| **4.2.5 Change Management**<br>Implemented: Yes |

## Family 4.3: Enterprise Security Architecture Management

Establish an enterprise security architecture that leverages a standardized enterprise security architecture framework, evaluates risk when developed and implemented, and is routinely measured to evaluate effectiveness.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.3 Enterprise Security Architecture Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.3.1 Security Architecture Standard**<br>Implemented: Yes |
| **4.3.2 Security Architecture Design**<br>Implemented: Yes |
| **4.3.3 Security Architecture Use**<br>Implemented: Yes |
| **4.3.4 Security Architecture Effectiveness**<br>Implemented: Yes |

## Family 4.4: Security Controls Management

Establish a security controls framework that includes methods to stay abreast of new control capabilities and monitors the effectiveness of current controls in the environment.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.4 Security Controls Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.4.1 Security Controls Planning**<br>Implemented: Yes |
| **4.4.2 Security Controls Development**<br>Implemented: Yes |
| **4.4.3 Security Controls Selection**<br>Implemented: Yes |
| **4.4.4 Security Controls Effectiveness**<br>Implemented: Yes |

## Family 4.5: Security Controls Performance Management

Effectively design, develop, report, and evaluate security controls performance to ensure continuous improvement in the cyber security program.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.5 Security Controls Performance Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.5.1 Security Performance Management**<br>Implemented: Yes |
| **4.5.2 Security Performance Measures**<br>Implemented: Yes |
| **4.5.3 Security Performance Operational Effectiveness**<br>Implemented: Yes |
| **4.5.4 Evaluation of Security Performance Measures**<br>Implemented: Yes |

## Family 4.6: Third Party Risk Management

Establish a third party risk management program that effectively evaluates, mitigates, and routinely monitors the risk of all third party engagements across the enterprise.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.6 Third Party Risk Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.6.1 Third Party Risk Planning**<br>Implemented: Yes |
| **4.6.2 Third Party Risk Assessments**<br>Implemented: Yes |
| **4.6.3 Third Party Risk Mitigation**<br>Implemented: Yes |
| **4.6.4 Third Party Risk Monitoring**<br>Implemented: Yes |

## Family 4.7: Human Capital Management

Understand your organization's cyber security staffing needs and establish plans to recruit, develop, and retain the necessary talent.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.7 Human Capital Management
Number of Controls: 4

100% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.7.1 Security Staffing Framework**<br>Implemented: Yes |
| **4.7.2 Security Staffing Role Criteria**<br>Implemented: Yes |
| **4.7.3 Security Staff Training**<br>Implemented: Yes |
| **4.7.4 Security Staff Stability**<br>Implemented: Yes |

## Family 4.8: Information Sharing and Partnerships

Establish an information sharing program that shares and receives cyber threat information to promote threat-informed decision making aligned to defensive capabilities, threat detection techniques, and mitigation strategies.

### Control Family Maturity


↔ 0%
Constant

### Maturity Components


↔ 0%
Constant


↔ 0%
Constant


↔ 0%
Constant

### Control Completeness

4.8 Information Sharing and Partnerships
Number of Controls: 4

75% Coverage

↔ 0% Constant

| Control |
| --- |
| **4.8.1 Information Sharing Planning**<br>Implemented: Yes |
| **4.8.2 Information Sharing Integration**<br>Implemented: Yes |
| **4.8.3 Information Sharing Use**<br>Implemented: Yes |
| **4.8.4 Information Sharing Program Measurement**<br>Implemented: No |

## Section 5. Assessor Statement

CyberGRX prepared the accompanying third party risk assessment of Autymate. The CyberGRX platform utilizes proprietary methodology that incorporates current threat intelligence, multiple industry standards, and best practices to identify risks that may be applicable to Autymate.

## Section 6. Assessment Methodology

CyberGRX provides a third-party risk management platform for supporting enterprises and their partners and vendors measure, rank, mitigate, and monitor cyber risk. A significant aspect to the platform is the ability to perform a security controls assessment and score the maturity and effectiveness of an organization's internal security controls and obtain evidence to verify those scores. Our assessment conforms to the following standard methodology:


### 1. Distribute Assessment Questionnaire

Upon receipt of an order for an assessment, CyberGRX will engage with the organization to establish appropriate accounts and permissions to the platform, and distribute and assign a CyberGRX controls assessment. CyberGRX will also assign an independent assessor to support the attestation of the internal security controls from either the CyberGRX assessment team or partner assessor.

### 2. Perform Self Assessment

The organization point of contact for performing and managing the risk assessment identifies the appropriate responsible parties to complete the various sections of the assessment questionnaire. Each section is accompanied by an assertion statement that the responsible party is the correct person and the answers are truthful to the best of their knowledge. These sections are compiled, asserted, and submitted by the primary point of contact as being complete, truthful, and accurate.

### 3. Prioritize Controls

CyberGRX uses data about the enterprise-partner relationship including services provided, operating industry, and asset exposure coupled with the current threat environment to identify the inherent risk and uniquely prioritize controls creating the greatest inherent risk exposure for that unique relationship.

### 4. Perform Verification Review

CyberGRX, or assigned partner, performs a targeted attestation examination of the self assessment. Using control prioritization, validation rules, and judgement, the assessor will request sufficient evidence to confirm the organization's assertion of their internal controls. In the event the evidence does not support the answers the assessor will indicate the discrepancy for inclusion in the scoring algorithm. Evidence will take the form of examination of documents and business processes, inspection of compliance, and/or review of personnel through interviews. This validation is indicated throughout the assessment as a control validity indicator with the following values:

1 - Very low: Self attestation only
2 - Low: Self attestation with external scan
3 - Moderate: Interview validation
4 - High: Evidence examination
5 - Very High: Internal validation testing

### 5. Assess and Score Controls

CyberGRX measures both maturity (how advanced an organization is performing across process, people, and technology as it relates to cyber risk controls) and control effectiveness (how well you've implemented your control in terms of strength, coverage, and timeliness) in accordance with CyberGRX's integrated cyber security controls framework.

#### Identify Control Gaps

Based on the scoring, a residual risk analysis is performed to identify those controls/subcontrols that persist from the inherent risk analysis. These controls/subcontrols are prioritized to provide actionable information to decrease an organization's cyber security risk.

#### Generate Report

The final state is for the assessor to attest to the scores and generate an assessment report summarizing the findings.