Cybersecurity is included in human resources practices.

Internal and external threats to the organization are identified and recorded.

Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.

Secure software development practices are integrated and their performance is monitored throughout the software development life cycle.

Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Assets are prioritized based on classification, criticality, resources, and impact on the mission.

Risk management objectives are established and agreed to by organizational stakeholders.

Inventories of software, services, and systems managed by the organization are maintained.

Incident data and metadata are collected, and their integrity and provenance are preserved.

Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.

Incidents are declared when adverse events meet the defined incident criteria.

Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.

The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.

The incident response plan is executed once an incident is declared in coordination with relevant third parties.

Recoverability and transition to normal operations are conducted within the scope of incident response.

The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.

Analysis is performed to determine what has taken place during an incident and the root cause of the incident.

Potentially adverse events are analyzed to better understand associated activities.

Continuous evaluation is applied to identify improvements.

Information is correlated from multiple sources.

Log records are generated and made available for continuous monitoring.

Incidents are categorized and prioritized.

Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements.

Inventories of software, services, and systems managed by the organization are maintained.

Software is maintained, replaced, and removed commensurate with risk.

Continuous evaluation is applied to identify improvements.

Cybersecurity is included in human resources practices.

Internal and external threats to the organization are identified and recorded.

Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.

Secure software development practices are integrated and their performance is monitored throughout the software development life cycle.

Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Assets are prioritized based on classification, criticality, resources, and impact on the mission.

Risk management objectives are established and agreed to by organizational stakeholders.

Inventories of software, services, and systems managed by the organization are maintained.

Incident data and metadata are collected, and their integrity and provenance are preserved.

Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.

Incidents are declared when adverse events meet the defined incident criteria.

Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.

The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.

The incident response plan is executed once an incident is declared in coordination with relevant third parties.

Recoverability and transition to normal operations are conducted within the scope of incident response.

The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.

Analysis is performed to determine what has taken place during an incident and the root cause of the incident.

Potentially adverse events are analyzed to better understand associated activities.

Continuous evaluation is applied to identify improvements.
<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
<th>Sub-Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Govern GV</td>
<td>58.6%</td>
<td>Organizational Content GV.OC</td>
<td>30.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Management Strategy GV.RM</td>
<td>34.3%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cybersecurity Supply Chain Risk Management GV.SC</td>
<td>67.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Roles, Responsibilities, and Authorities GV.RR</td>
<td>68.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policies, Processes, and Procedures GV.PO</td>
<td>62.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oversight GV.OV</td>
<td>38.3%</td>
</tr>
<tr>
<td>Identify ID</td>
<td>54.0%</td>
<td>Asset Management ID.AM</td>
<td>28.6%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Assessment ID.RA</td>
<td>36.3%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improvement ID.IM</td>
<td>75.0%</td>
</tr>
<tr>
<td>Protect PR</td>
<td>67.6%</td>
<td>Identity Management, Authentication, and Access Control PR.AA</td>
<td>70.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Awareness and Training PR.AT</td>
<td>62.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Security PR.DS</td>
<td>65.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform Security PR.PS</td>
<td>70.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technology Infrastructure Resilience PR.IR</td>
<td>68.8%</td>
</tr>
<tr>
<td>Detect DE</td>
<td>63.8%</td>
<td>Continuous Monitoring DE.CM</td>
<td>65.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adverse Event Analysis DE.AE</td>
<td>62.5%</td>
</tr>
<tr>
<td>Respond RS</td>
<td>60.6%</td>
<td>Incident Management RS.MA</td>
<td>30.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Analysis RS.AN</td>
<td>62.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Response Reporting and Communication RS.CO</td>
<td>75.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Mitigation RS.MI</td>
<td>75.0%</td>
</tr>
<tr>
<td>Recover RC</td>
<td>68.8%</td>
<td>Incident Recovery Plan Execution RC.RP</td>
<td>62.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Recovery Communication RC.CO</td>
<td>75.0%</td>
</tr>
</tbody>
</table>
NIST CSF 2.0

Public Draft: The NIST Cybersecurity Framework 2.0

6 Functional Areas
22 Categories
106 Subcategories

SCALE
5.0 "World class, setting the standard"
4.5 "Standard Operating Procedure, aligned with the business, aligned with best practices"
4.0 "Standard Operating Procedure, Business as Usual (BAU)"
3.5 "Occurs, consistently, aligned with ERM business risk and adversarial threat"
3.0 "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"
2.5 "Occurs, not consistently, structured"
2.0 "Occurs, not consistently, unstructured"
1.5 "Initial process and documentation in place"
1.0 "ADHOC or only when necessary"
0.5 "Awareness and acceptance of the need exists"
0.0 "Not doing this at all"

COST PROJECTIONS
1 Labor Hour $ cost per each 106 Subcategories = 106 Labor Hours to fill out ATO Attestation Form/Questions
Knowledge Management/Intelligence = 14 Labor Hours to convert ATO data to KM Repo & Executive Dashboard
TOTAL = 120 Labor Hours using Microsoft Suite (Excel, Sharepoint, PowerBI) x 37.5hr average FTE = $8640 COST

*AI (GPT, LLMs) could increase efficiency (ex. ChatBots) & improve cost savings
The organizational mission is understood and informs cybersecurity risk management.

Level 5.0: "Multidisciplinary, setting the tone"

- Understand what your organization's cybersecurity risk management (CRM) landscape looks like and how it interacts with the organizational mission.
- Ensure that your organization's CRM activities are fully aligned with and integrated into the organizational mission to support the organizational mission.
- Ensure that your organization's CRM activities are fully aligned with and integrated into the organizational mission to support the organizational mission.
- Ensure that your organization's CRM activities are fully aligned with and integrated into the organizational mission to support the organizational mission.
- Ensure that your organization's CRM activities are fully aligned with and integrated into the organizational mission to support the organizational mission.

Level 4.5: "Organized Operating Procedure, aligned with the business, aligned with best practices"

- Align cybersecurity risk management with the business goals and objectives to ensure that the CRM strategy aligns with the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 4.0: "Organized Operating Procedure, Business as usual" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 3.5: "Organized Operating Procedure, aligned with ERM business risk and adversarial threat" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 3.0: "Organized Operating Procedure, aligned with business and risk considerations" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 2.5: "Awareness and acceptance of the need exists" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 2.0: "ADHOC or only when necessary" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 1.5: "Consistent, not consistently, unstructured" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 1.0: "Consistent, not consistently, structured" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 0.5: "Awareness and acceptance of the need exists" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.

Level 0.0: "Not doing this at all" (B4U)

- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
- Ensure that cybersecurity risk management processes are integrated into business processes and decision-making to support the organizational mission.
Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood.

1. Are your organization’s approach to engaging with stakeholders in cybersecurity risk management been recognized as a best practice by industry peers or standards bodies?
2. Does your organization leverage stakeholder feedback to develop cybersecurity strategies and innovations for risk management solutions that incorporate business workflows?
3. Is stakeholder feedback managed through a consistent system that ensures needs and expectations are identified, prioritized, tracked, and aligned with cybersecurity objectives?
4. Is there continuous feedback loop with stakeholders that contributes to the evolution of cybersecurity practices, which in turn influence global standards?

Level 0.0: "Not doing this at all"
Level 1.5: "Initial processes and documentation in place"
Level 2.0: "Occurs, not consistently, unstructured"
Level 2.5: "Occurs, not consistently, structured"
Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"
Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"
Level 4.5: "Standard operating procedure, aligned with the business, aligned with best practices"

Level 1.0: "Gains, sensitively, aligned with IBRM business- risk- and adversarial threat"

1. Are there no established processes or plans in place to engage with stakeholders on cybersecurity matters?
2. Does your organization completely disregard stakeholder needs and expectations in the context of cybersecurity risk management?
3. Are there informal discussions about stakeholder needs in cybersecurity that are not yet part of an official engagement strategy?
4. Does your organization lack a routine mechanism for capturing and addressing stakeholder needs, leading to ad-hoc engagement practices?
5. Are engagements with stakeholders regarding cybersecurity performed sporadically and without a predefined process?

Level 2.0: "Gains, sensitively, aligned with IBRM technical vulnerabilities and the attack surface"

1. Are initial processes for stakeholder engagement in place that are not fully developed or regularly utilized?
2. Are your organization’s processes for involving stakeholders in understanding and managing the technical aspects of cybersecurity risk management the same as those for engaging with business- risk- and adversarial threat?

Level 3.0: "Gains, sensoritively, monitored"

1. Are stakeholder concerns regarding cybersecurity risks occasionally discussed but not formally documented or consistently acted upon?
2. Does your organization view stakeholder feedback as a critical input in developing and updating cybersecurity strategies?
3. Do stakeholder engagements happen in an ad-hoc manner, influenced by individual initiative rather than organizational policy?
4. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?
5. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?

Level 4.0: "Gains, sensoritively, measured"

1. Do leaders recognize the value of stakeholder input for cybersecurity risk management without it being reflected in business practices?
2. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?
3. Are there recognized stakeholders whose cybersecurity concerns are only occasionally considered in risk management?
4. Is the understanding of stakeholder expectations in cybersecurity sporadic and dependent on the occurrence of incidents or specific demands?
5. Are stakeholder engagement activities in cybersecurity risk management included in the routine responsibilities of relevant staff?

Level 5.0: "Not doing this at all"
Level 1.0: "Gains, sensitively, aligned with IBRM business- risk- and adversarial threat"

1. Are there no established processes or plans in place to engage with stakeholders on cybersecurity matters?
2. Does your organization completely disregard stakeholder needs and expectations in the context of cybersecurity risk management?
3. Are there informal discussions about stakeholder needs in cybersecurity that are not yet part of an official engagement strategy?
4. Does your organization lack a routine mechanism for capturing and addressing stakeholder needs, leading to ad-hoc engagement practices?
5. Are engagements with stakeholders regarding cybersecurity performed sporadically and without a predefined process?

Level 2.0: "Gains, sensitively, aligned with IBRM technical vulnerabilities and the attack surface"

1. Are initial processes for stakeholder engagement in place that are not fully developed or regularly utilized?
2. Are your organization’s processes for involving stakeholders in understanding and managing the technical aspects of cybersecurity risk management the same as those for engaging with business- risk- and adversarial threat?

Level 3.0: "Gains, sensoritively, monitored"

1. Are stakeholder concerns regarding cybersecurity risks occasionally discussed but not formally documented or consistently acted upon?
2. Does your organization view stakeholder feedback as a critical input in developing and updating cybersecurity strategies?
3. Do stakeholder engagements happen in an ad-hoc manner, influenced by individual initiative rather than organizational policy?
4. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?
5. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?

Level 4.0: "Gains, sensoritively, measured"

1. Do leaders recognize the value of stakeholder input for cybersecurity risk management without it being reflected in business practices?
2. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM?
3. Are there recognized stakeholders whose cybersecurity concerns are only occasionally considered in risk management?
4. Is the understanding of stakeholder expectations in cybersecurity sporadic and dependent on the occurrence of incidents or specific demands?
5. Are stakeholder engagement activities in cybersecurity risk management included in the routine responsibilities of relevant staff?

Level 5.0: "Not doing this at all"
Level 1.0: "Gains, sensitively, aligned with IBRM business- risk- and adversarial threat"

1. Are there no established processes or plans in place to engage with stakeholders on cybersecurity matters?
2. Does your organization completely disregard stakeholder needs and expectations in the context of cybersecurity risk management?
3. Are there informal discussions about stakeholder needs in cybersecurity that are not yet part of an official engagement strategy?
4. Does your organization lack a routine mechanism for capturing and addressing stakeholder needs, leading to ad-hoc engagement practices?
5. Are engagements with stakeholders regarding cybersecurity performed sporadically and without a predefined process?
Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Level 2.0: "Occurs, not consistently, unstructured"

Level 2.5: "Occurs, not consistently, structured"

Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

Level 5.0: "World class, setting the standard"
Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated.

Level 5.0: "World class, setting the standard"

Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

Level 3.0: "Occurs, consistently, aligned with CRMM technical vulnerabilities and the attack surface"

Level 2.5: "Occurs, not consistently, structured"

Level 2.0: "Occurs, not consistently, unstructured"

Level 1.5: "Initial process and documentation in place"

Level 1.0: "ADHOC or only when necessary"

Level 0.5: "Awareness and acceptance of the need exists"

Level 0.0: "Not doing this at all"
Outcomes, capabilities, and services that the organization depends on are determined and communicated.