Cybersecurity Rubric 2.0

The Cybersecurity Rubric (CR 2.0) is a tool for assessing a school's cyber-readiness, aligned with NIST Cybersecurity Framework (NIST CSF 2.0). It includes 6 Functions and 22 Categories, each rated from Initial (Level 1) to Optimized (Level 5). The overall maturity level is based on Function maturity levels, detailed in the Results tab.

Before starting the rubric, you are encouraged to take the **FREE** course, "Learn How to Use the Cybersecurity Rubric." This course provides a solid grasp of the NIST evaluation criteria, insights, and tools that will guide you in accurately gauging your school's cybersecurity posture across the NIST categories.

Instructions:

Evaluate the school system's cybersecurity Maturity Level for every category in the function tabs.

Results

The Results tab is next, but data is not entered here. This tab auto-populates ratings, including the overall maturity level. The data comes from the ratings in each of the function tabs after all categories have been assigned a level.

Function Tabs (Govern, Identify, Protect, Detect, Respond, & Recover)

The six (6) tabs at the bottom are National Institute of Standards and Technology (NIST) functions. Each tab has a set of categories that are to be evaluated and assigned a maturity level. Ensure ALL categories are rated to get an accurate maturity level for the school system. Review "NIST Function and Category Descriptions" for an overview of each function and its supporting categories.

This Cybersecurity Rubric is regularly reviewed and updated to reflect current trends. For easy access to the latest version, download the CR from https://www.cybersecurityrubric.org/ . Be sure to download a new file copy of the Cybersecurity Rubric each time you conduct a system-wide cybersecurity evaluation.

December 2025

Cybersecurity Rubric for Education

CYBERSECURITY RUBRIC: GOVERN (GV)

GV1: ORGANIZATIONAL CONTEXT

LEVEL 1: INITIAL

Risk mitigation defenses are not clearly defined. **Third-party data-sharing** agreements are not formal. Sensitive data processes need improvement. **Risk management** decisions are not included in cybersecurity initiative planning.

LEVEL 2: REPEATABLE

Operational processes and **responsibilities** are consistent but mostly ad hoc or reactive. Some contractual **data-sharing agreements** with third parties are formalized. **Sensitive data** processes are not routinely measured or enforced.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND risk mitigation operations are documented. **Third-party data-sharing agreements** are formalized and meet legal, contractual, and regulatory requirements. **Sensitive data** processes are measured and enforced and include privacy and security requirements. Controls are in place to prevent loss, damage, or theft. Strategic plans address cybersecurity roles and responsibilities. Risk management decisions are understood through the mission, expectations, and contracts.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND performance controls are in place at department levels to measure and evaluate system-wide risk. **Resiliency measures** to anticipate, prepare for, and recover from cyber events are in place and are a priority. Regular **cybersecurity assessments** are conducted to verify optimal performance levels. **Strategic planning** and budget allocations are fueled by needs assessment data.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND strategic plans inform cybersecurity roles, responsibilities, and risk management decisions. **Controls** in place are effective, systematic, and responsive. Fact-based, **cybersecurity assessments** are optimized based on an organization-wide analysis.

ENTER SCORE

NOTES

GV2: RISK MANAGEMENT STRATEGY

LEVEL 1: INITIAL

The organization's risk **priorities, constraints**, risk **tolerances**, and **assumptions** are not clearly defined. A comprehensive **risk management strategy** is lacking or nonexistent. Processes are not documented or aligned to support the **architecture** and strategic **roadmap.**

LEVEL 2: REPEATABLE

The organization's risk **priorities, constraints,** risk **tolerances,** and assumptions are being developed. Processes to develop a comprehensive **risk management strategy** are being established and used to support operational risk decisions. Risk management is transitioning from **reactive** to **proactive.**

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND risk management **processes** are documented and agreed to by organizational stakeholders. **Risk management** processes include cybersecurity risk objectives, activities, and outcomes. **Supply chain** risk management processes are defined. Tracked **action plans** include disseminating cybersecurity risks to stakeholders. The risk management strategy includes a documented **communication plan.**

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND the shared risk management **strategy** and desired **response patterns** are culturally embedded and well understood. All **stakeholders** are committed to detecting and responding to changing tactics and techniques of cybersecurity threats and vulnerabilities.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND the risk management **strategy** is fully deployed without significant weaknesses or gaps across the school system. **Processes** and **lessons learned** are regularly shared with the **education market sector** community.

ENTER SCORE

NOTES

GV3: ROLES, RESPONSIBILITIES, AND AUTHORITIES

LEVEL 1: INITIAL

Roles and Responsibilities for the development and implementation of data privacy and cybersecurity policies and practices need to be defined. **Resources** and budgets need to be allocated to meet cybersecurity and data privacy needs of the school system.

LEVEL 2: REPEATABLE

Cybersecurity processes are developing with **roles and responsibilities** for internal and external stakeholders being defined. A school system **executive leader** is identified as the person responsible for the development and implementation of cybersecurity policies and practices. **Resources** and budgets are being allocated, with basic needs identified to meet the cybersecurity and data privacy needs of the school system.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND processes that demonstrate cybersecurity **roles and responsibilities** for the internal and external stakeholders are defined, understood and documented. **Designated staff** maintain data privacy and cybersecurity policies. **Resources** are aligned and allocated system-wide to meet cybersecurity current and future needs. **Human resource** processes include onboard cyber training and regular training.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND system-wide **cybersecurity governance** includes cybersecurity awareness programs to influence behavior among the workforce to be security conscious and properly skilled to reduce risks to the school system. The **TLE practice** areas are reviewed annually and improvement initiatives are based on evaluation results.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND roles and responsibilities for detection are well-defined to ensure accountability. Governance **processes** are audited annually to assess federal, state, and local regulatory compliance. The school system is working toward or has obtained the **TLE seal** mark of distinction.

ENTER SCORE

NOTES

GV4: POLICY

LEVEL 1: INITIAL	LEVEL 2: REPEATABLE	LEVEL 3: DEFINED	LEVEL 4: MANAGED	LEVEL 5: OPTIMIZED
The school's **policies** for managing cybersecurity risks are lacking. Policies are not documented, communicated, or enforced.	The school's **policies** for managing cybersecurity risks are being developed. **Governance practice** includes the approval of strategic direction and policy creation to support operational risk decisions. **Risk management** is transitioning from reactive to proactive.	Meets **REPEATABLE** Maturity Level **AND cybersecurity policies** are documented and agreed to by organizational stakeholders. **Risk assessment policies** include identifying new threats, vulnerabilities, and conditions that may impact the system's security.	Meets **DEFINED** Maturity Level **AND policies** for managing cyber risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and the school's mission. All **stakeholders** are committed to detecting and responding to changing tactics and techniques of cybersecurity threats and vulnerabilities.	Meets **MANAGED** Maturity Level **AND** policies for risk management strategy are fully deployed without significant weaknesses or gaps across the school. **Policy updates** and lessons learned are regularly shared with the education market sector community.

ENTER SCORE

NOTES

GV5: OVERSIGHT

LEVEL 1: INITIAL

Lack of **oversight** in the review of cybersecurity guidelines, processes, or policy by executive leadership is evident. Cybersecurity risk management **outcomes** are not reviewed or adjusted to ensure coverage of school system requirements and risks.

LEVEL 2: REPEATABLE

Cybersecurity guidelines, processes, and policies are **approved** by executive leadership. Cybersecurity documentation undergoes review, evaluation, and improvement at a minimum annually. Cybersecurity risk management outcomes are reviewed and adjusted to ensure coverage of school system requirements and risks.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND organizational cybersecurity risk management performance is measured and reviewed to adjust strategic direction. Cybersecurity documentation undergoes review, evaluation, and improvement quarterly.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND governance practices adhere to all federal, state, and local regulations.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND governance includes cybersecurity reviews conducted by an outside independent party on an annual basis.

ENTER SCORE

NOTES

GV6: CYBERSECURITY SUPPLY CHAIN MANAGEMENT

LEVEL 1: INITIAL

Processes to manage **supplier** risks are not documented and are ad hoc, inconsistent, or reactive. A comprehensive **inventory** of suppliers and third-party partners and the identification of the information systems, components, and services provided is lacking or nonexistent.

LEVEL 2: REPEATABLE

An **inventory** of suppliers and third-party partners with processes to identify, assess, and manage supply chain risks is being developed. A systematic approach to evaluating third-party **key processes** is evident. Improvement initiatives with suppliers to ensure compliance are being developed.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND risk **management processes** include suppliers and third-party partners of information systems, components, and services. All processes are **identified, documented, prioritized,** and routinely assessed using audits, test results, or other forms of evaluations to confirm suppliers and partners are meeting their contractual obligations.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND suppliers and third-party partners conduct routine tests to evaluate **compliance** and the **adequacy** and **effectiveness** of all implementations. **Results** from tests ensure all policies, processes, and controls are managed as expected by ensuring the appropriate cybersecurity levels of control. Effective corrective **actions** are taken to address any weaknesses. Independent **audits** and valid **certifications** of proven performance are required.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND supply chain **risk processes** are advancing, optimizing, and progressive. Cyber **defenses** are maximized as evidenced by a comprehensive supply chain security program. Suppliers and partners are chosen based on risk and mission **impact.** Response and recovery **planning** and **testing** are conducted with suppliers and third-party providers at least annually. Results are evaluated and used for **continuous improvement.**

ENTER SCORE

NOTES

CYBERSECURITY RUBRIC: IDENTIFY (ID)

ID1: ASSET MANAGEMENT

LEVEL 1: INITIAL	LEVEL 2: REPEATABLE	LEVEL 3: DEFINED	LEVEL 4: MANAGED	LEVEL 5: OPTIMIZED
Asset inventory processes are ad hoc, inconsistent, and/or reactive and may be out of date. **Controls** for asset protection are lacking or need improvement.	**Asset inventories** are current and processes are consistent. **Protection controls** for asset protection are transitioning from being reactionary. **Improvement initiatives** are underway.	Meets **REPEATABLE** Maturity Level **AND asset inventories** are current and document an asset's full life cycle. **Data classifications** are defined per state standards, regulations, and legal requirements. **Protection controls** are maintained and off-site asset security measures are in place, including software installs and asset transfers.	Meets **DEFINED** Maturity Level **AND asset inventory** processes are highly managed with defined metrics. Effectiveness and accuracy are statistically analyzed. Asset **compliance** is evaluated regularly, and noncompliance is identified through root-cause analysis. **Protection controls** are tested, and results influence improvements.	Meets **MANAGED** Maturity Level **AND** efficient, effective, and innovative **asset inventories** are in place system-wide with best practice process improvements. Inventory management is well integrated with the current and future needs aligned with system-wide objectives and risk strategy.

ENTER SCORE

NOTES

ID2: RISK ASSESSMENT

LEVEL 1: INITIAL

Risk management capacity is lacking. **Processes** are not documented and are ad hoc, inconsistent, or reactive. **Vulnerabilities** are exposed and impacts are unknown. **Collaborative approaches** to risk identification and management are lacking or not evident.

LEVEL 2: REPEATABLE

Leadership demonstrates awareness of the importance of cybersecurity risk to organizational operations, assets, and individuals. The transition from a **reactive** to a **proactive** approach to risk management is evident. Processes to **identify** vulnerabilities and **mitigate** risks are being developed. Collaborative problem-solving and information gathering from **information-sharing** forums are being prioritized.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND processes to **identify** vulnerabilities, **mitigate** and **minimize** threats, and determine potential instructional and business operations **impacts** are documented and built into daily operations. Threat intelligence from **information-sharing** forums and sources is collected. Information processing facilities are **secure.** Processes for **backup** and **recovery** systems are documented, tested, and evaluated at least annually.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND established **risk management strategy** is in place with integrated improvements beyond compliance regulation requirements Priority is given to building **knowledge** about the risk management process and raising **awareness** about the needed capabilities to effectively conduct risk assessments and manage risk.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND risk assessment includes a focus on **disciplined optimization** and continual **process improvement.** Qualified cybersecurity **practitioners** are employed to measure and assess every aspect of the school system for possible cybersecurity issues and improvement opportunities. A fact-based evaluation **cycle of improvement** is optimized.

ENTER SCORE

NOTES

ID3: IMPROVEMENT

LEVEL 1: INITIAL

An improvement **posture** is not evident or is lacking. Improvement is primarily **reactive.** The overall capacity for **detection, response,** and **recovery** is lacking or limited. Recovery planning **alignment** and **coordination** need improvement.

LEVEL 2: REPEATABLE

Improvement is beginning to transition from **reactive** to **proactive.** The overall **capacity** for recovery is limited but growing. **Leaders** demonstrate commitment to improvement. **Budgets** are being allocated to align the school system's enterprise architecture and strategic roadmap to improve a comprehensive cyber recovery plan.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND actions taken to **restore** business continuity and **protect** assets after an incident are routinely analyzed. Improvement **actions** are identified as lessons learned for continuous improvement. Recovery plans incorporate **retrospective** (lessons learned) sessions and initiatives. Response and recovery strategies are updated.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND all stakeholders acknowledge the value of managing a pristine **response and recovery plan.** The **school system** evaluates incident response performance, identifies challenges, and improves incident response capabilities in strategic plans. Lessons learned and continuous improvement efforts result in an improved cybersecurity **posture** and **readiness** to face future security incidents.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND the school system continuously **evaluates** and **improves** response and recovery processes. **Metrics** are captured and used to evaluate processes and drive improvement. Advanced technology solutions are used to assist in all phases of incident recovery. Overall cybersecurity **maturity** and school system **resilience** improve through optimized incident response, business continuity, and disaster recovery planning initiatives.

ENTER SCORE

NOTES

CYBERSECURITY RUBRIC: PROTECT (PR)

PR1: IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL

LEVEL 1: INITIAL

Access control processes and protocols for physical and remote access are not established and documented. **Multi-factor authentication** has not been implemented. **Data protection** measures are inconsistent. **Network integrity** processes are not defined. **Account review** processes for user, supplier, and system accounts are not defined. Conditions for **group** and **role membership** are not defined.

LEVEL 2: REPEATABLE

Access control processes and protocols for physical and remote access are documented but not routinely managed. At least one **multi-factor authentication** method is in place. **Data protection** measures are documented. **Network integrity** processes are defined. **Account review** processes for user, supplier, and system accounts are defined but not routinely enforced. Conditions for **group** and **role membership** are defined.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND compliant **data protection measures** are maintained. **Network integrity** processes, protections, and controls are routinely enforced. **Account review** processes are routinely conducted. **Account managers** are assigned. Conditions for **group** and **role membership** are routinely met.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND access control processes, protocols, and protection measures are systematic and well deployed. **Multi-factor authentication** methods are routinely evaluated for efficacy. **Network integrity** and **account review** processes are routinely evaluated for state and federal compliance. **Evaluation** processes include access control risk mitigation.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND data-driven decisions to mitigate and avert risk in alignment with best practices are routinely made. The **overall approach** to cybersecurity awareness, training, and implementation is fully deployed without significant weaknesses or gaps.

ENTER SCORE

NOTES

PR2: AWARENESS AND TRAINING

LEVEL 1: INITIAL

Processes to ensure all staff and students with **user ID** accounts are undocumented and are ad hoc, inconsistent, or reactive. Cybersecurity awareness training is not mandatory or scheduled for new or existing users. Specific **role-based** security training to designated personnel is inconsistent or nonexistent. **Personnel** to document and monitor information system security training activities are not defined or designated. A **records retention policy** is not defined.

LEVEL 2: REPEATABLE

Processes are being developed to ensure all staff and students with **user ID** accounts are adequately trained. Cybersecurity awareness **training** improvement initiatives are being developed. Specific **role-based** security training for personnel with assigned security roles and responsibilities is defined. **Personnel** to document and monitor information system security training activities are identified. A **records retention policy** is defined.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND role-based security training is provided before authorizing access to the information system or performing assigned duties. **Personnel** to document and monitor information system **security training** activities are active in their designated roles. Training records are retained based on the **records retention policy.**

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND regular cybersecurity **alerts,** training **campaigns,** and **simulated attacks** are issued. Staff and student **training progress** is routinely tracked and updated as needed based on available data. Leadership is involved in continuous process and training monitoring. Designated staff continually monitors, measures, and enforces training **adherence.**

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND cybersecurity **awareness** and **training** methods are focused on continually improving performance through incremental and innovative optimization. **Metrics** to measure training performance objectives are established. A data-based **evaluation cycle** of improvement is optimized. Leadership is instrumental in designing, implementing, revising, and monitoring **training initiatives** and **progress.**

ENTER SCORE

NOTES

PR3: DATA SECURITY

LEVEL 1: INITIAL

Processes to manage and protect **stored** and **transmitted data** are not documented or are ad hoc, inconsistent, or reactive. Processes and policies to **protect** the **confidentiality, integrity,** and **availability** of information and records are nonexistent or lacking. **Leadership** demonstrates an incomplete understanding of data protection and risk management.

LEVEL 2: REPEATABLE

Stored and **transmitted data** is managed and monitored consistently. Processes **are defined, repeatable,** and **scalable.** Leadership demonstrates sufficient understanding of data protection and risk management. Formal process definitions and protocol for managing and monitoring data and information are being developed and documented.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND data includes mitigating controls, protections, and innovative technologies. **Data management** and **protection** processes are routinely enforced. **Data records** are formally managed and are consistent with implemented risk management strategies. **Exceptions** for non-encryption are routinely evaluated. Dedicated **technology staff** monitors and investigates alerts.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND risk evaluation processes and measures extend beyond compliance requirements and regulations. **Risks** are routinely identified, analyzed, monitored, and controlled. **Results** from evaluation and monitoring processes and activities are used to drive improvements. T**echnology staff** demonstrates a high degree of skill and knowledge in managing and monitoring **stored** and **transmitted data.**

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND state-of-the-art **data security solutions** are used to provide enhanced visibility into system vulnerabilities. Innovative **integrity-checking mechanisms** are used to secure all information systems. Cybersecurity **controls** are adapted to meet the challenges of a dynamic information technology (IT) security environment. **Technology staff** demonstrates consistent ownership of proactive risk assessment and mitigation measures.

ENTER SCORE

NOTES

PR4: PLATFORM SECURITY

LEVEL 1: INITIAL

Processes to **maintain** and **repair** information systems and applications in accordance with vendor specifications and requirements are lacking. Maintenance **systems** and **tools** are not controlled. Maintenance **activities** are primarily reactive and are sporadic and/or inconsistent. **Security controls** to verify functionality after maintenance lack definition. **Records** of maintenance activities are ad hoc, inconsistent, or incomplete. Processes to prevent **unauthorized access** need definition and/or improvement.

LEVEL 2: REPEATABLE

Systems and tools used to **maintain** and **repair** information systems and applications are routinely and consistently implemented per vendor specifications and requirements. **Security controls** are identified, documented, and implemented. Maintenance activity **records** are consistently kept. Processes are **repeatable** as the school system employs qualified "go-to" staff members for organizational knowledge. Formal definition and documentation of **proactive** and **preventative** maintenance activities are underway.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND documented processes to **maintain** and **repair** information systems and applications are implemented in accordance with **vendor specifications** and **requirements.** Maintenance **systems, tools, and activities** are approved, controlled, tested, and monitored. Post-maintenance **security controls** are routinely tested. Detailed **records** of maintenance activities are logged and retained. **Remote maintenance** of system assets is routinely approved, logged, and performed.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND maintenance of organizational information systems and applications is managed with acute care by designated, highly qualified staff. Regular maintenance is performed and verified to ensure all **systems** and **components** are effectively protected. Designated staff routinely monitors, measures, and enforces **adherence** to maintenance requirements and refresh cycles. The leadership chain of command is flexible to ensure **resources** are made available if there is a risk of noncompliance or poor performance.

LEVEL 5: OPTIMIZED

Meets MANAGED Maturity Level

AND information systems and **applications** are implemented in a proactive life cycle of maintenance and repair. **Continuous improvement** focused on efficiency and effectiveness is optimized and flexible. **Change management** is strategically planned and consistently prioritized. Designated technology staff is thoroughly trained in cybersecurity and prioritizes routine, proactive **system maintenance** to meet and exceed security objectives.

ENTER SCORE

NOTES

PR5: TECHNOLOGY INFRASTRUCTURE RESILIENCE

LEVEL 1: INITIAL

Processes to protect student and staff **devices** are lacking, or are ad hoc, inconsistent, or reactive. Advanced **protective technologies** to shield devices from identified and potential threats are lacking or nonexistent. **Security updates** are not conducted in a timely, scheduled manner. **Time** for information technology (IT) staff to capture and review audit logs needs is sparsely allocated or nonexistent. Additional protection measures for **removable media** and **network infrastructure components** are needed.

LEVEL 2: REPEATABLE

Processes to protect student and staff **devices** are being defined. Advanced **protective technologies** to shield devices from identified and potential threats are being researched and identified. **Resources** and **budgets** are being allocated. Qualified information technology (IT) staff are designated to maintain protection measures and **security updates** focused on ensuring the security and resilience of systems and assets. Protection measures for **removable media** and **network infrastructure** components are being determined.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND processes to protect student and staff **devices** are documented and implemented. Advanced **protective technologies** to protect devices are in place. Timely **installation** of security updates is applied. **Audit log records** are determined, documented, implemented, and reviewed in accordance with defined practices and policies. **Removable media** is protected, and use is restricted according to documented and implemented practices and policies. **Communications and control networks** are protected.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND the approach for implementing **protective technologies** is well deployed, with no significant gaps. Best practices drive performance levels, resulting in successful cybersecurity **sustainability.** Enhanced practices to protect changing tactics, techniques, and vulnerabilities of advanced persistent threats are reviewed and evaluated. **Corrective actions** are routinely taken to address identified weaknesses. Communications and control networks are routinely monitored. **Automated checks** are in place to avert cyber-attacks.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND the effects of deployed protective technologies are measured using **key indicators. Evaluation results** are used to guide improvement activities. **Protective technologies** are standardized across the organization. Processes are enhanced by using sophisticated protective technologies to detect and respond to advanced threats and vulnerabilities. Protective technologies aided by **automated checks** are **resilient** with an end goal in mind to ensure system availability and cyber protection is sustained at 100%.

ENTER SCORE

NOTES

CYBERSECURITY RUBRIC: DETECT (DE)

DE1: CONTINUOUS MONITORING

LEVEL 1: INITIAL

Processes to actively manage all **assets** are nonexistent or incomplete. Processes to detect, remove, and/or remediate **unauthorized** and **unmanaged assets** are ad hoc, incomplete, or reactive. **Reviews** of accounts, firewall rules, and penetration tests of external-facing systems are not consistently conducted. External **vulnerability scans** are not performed at least quarterly.

LEVEL 2: REPEATABLE

Processes to actively manage **assets** are documented but are primarily reactive. A systematic approach to evaluation and improvement of **key processes** for detecting, removing, and/or remediating **unauthorized** and **unmanaged assets** is being formulated. Schedules for regular external **vulnerability scans** are being developed.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND processes to actively manage **assets** and to detect, remove, and/or remediate **unauthorized** and **unmanaged assets** are routinely implemented. Quarterly vulnerability scans are regularly conducted. Annual penetration **tests** are regularly conducted. Systematic **account reviews** are routinely performed.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND continuous **monitoring processes** to rapidly detect cybersecurity risks in real time are embedded in daily operations. **Monitored performance** of critical security processes using forensics, root cause analysis, threat intelligence, and incident response is prioritized. Effective **correction actions** are taken to address identified weaknesses or vulnerabilities.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND continuous **security monitoring** uses data to verify the effectiveness of proactive measures and optimizes real-time threat detection to aid timely mitigation, improve cybersecurity maturity, and reduce risk. **Gap analyses** via multiple technologies are conducted to identify vulnerabilities, develop failsafe measures, and drive process improvement.

ENTER SCORE

NOTES

DE2: ADVERSE EVENT ANALYSIS

LEVEL 1: INITIAL

Processes to collect, review, and correlate **event data** from a cybersecurity attack are not documented or are ad hoc, inconsistent, or reactive. A **baseline** of network operations and expected data flows for staff, students, and systems is nonexistent or lacking. Technology staff assigned to analyzing the **impact** of events are needed. The capacity to detect **anomalies** is lacking.

LEVEL 2: REPEATABLE

Anomalous activity is detected consistently but the approach is mostly reactive. Processes to collect, review, and correlate **event data** from a cybersecurity attack are being developed and improvement initiatives are being addressed. Technology staff are assigned to analyze the **impact** of events and the school system is transitioning from being reactionary. Staff are developing their skills in learning about **pattern recognition** and attack targets and methods.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND documented processes to collect, review, and correlate **event data** from multiple sources and technology systems are in place. A **baseline** of network operations and expected data flows is established and managed. Processes for **collecting evidence** and **conducting forensic analysis** are documented and in place. Designated technology staff routinely analyze the **impact** of events. Detected anomalies are analyzed via a formalized process. **Pattern recognition** technologies are used.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND rigorous **analytics** generated from anomalies and trends at the subprocess level of the school system's applications, systems, and databases are used. Formal analysis is conducted of **patterns** of information technology activities outside of normal behavior. Underlying causes of **vulnerabilities** are identified through root-cause analysis. Issues related to **vulnerability identification** are tracked and reported to relevant managers.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND advanced processes generating immediate results are used to identify and detect **anomalies** and **events** and trigger rapid response. Cybersecurity technologies are based on **threat intelligence** combined with **data analytics** to segregate normal behavior from abnormal activity. **Proactive technologies** alert unauthorized access or suspicious behavior in real time.

ENTER SCORE

NOTES

CYBERSECURITY RUBRIC: RESPOND (RS)

RS1: INCIDENT MANAGEMENT

LEVEL 1: INITIAL

Approved processes to maintain a comprehensive cybersecurity **incident response plan** are lacking or nonexistent. Designated **staff** responsible for developing and implementing of the incident response plan have not been identified and/or trained.

LEVEL 2: REPEATABLE

An **incident response** plan is documented. **Improvement** is a priority as evidenced in strategic plans. The beginnings of a **systematic approach** to the evaluation and improvement of key processes are evident. Appropriate **staff** are designated and trained to ensure a timely response to detected cybersecurity events.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND a comprehensive, formal cybersecurity **incident response** plan is documented and annually reviewed. Designated **staff** are responsible for participating in the development and implementation of the practices outlined in the plan. In-house and third-party scenario-based plan **testing** is routinely conducted. **Results** are systematically evaluated.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND a customized, scenario-based cyber event **playbook** is used to measure and evaluate risk. **Business continuity, resilience**, and **agility** are prioritized and incorporated in scenarios. Planning time is allocated to evaluate **impact, response,** and **recovery**. **Practice** is incorporated to strengthen recovery plans. Findings through practice are instrumental in generating **action plans**.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND the documented, reflective, flexible response **planning process** pervades organizational culture and undergoes continuous improvement on an annual basis, or more frequently where possible. Results from feedback drive change and aid **retrospective** (lessons learned) sessions and initiatives.

ENTER SCORE

NOTES

RS2: INCIDENT ANALYSIS

LEVEL 1: INITIAL

Processes to **analyze** incidents are insufficient. Adequate response and support for **recovery activities** are ad hoc, inconsistent, or reactive.

LEVEL 2: REPEATABLE

A **cross-functional process** is employed to examine incidents. Systematic response and **support** for recovery activities are being developed. **Proactive** evaluation and improvement of key processes are being prioritized.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND incidents are analyzed and categorized consistently with **response plans**. **Measures** used in the analysis include compliance with federal and state regulations. Analysis **findings** and **results** are systematically evaluated. Additional **third-party** analysis is conducted.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND response **analysis** is culturally embedded and drives design, implementation, and evaluation. Detailed analysis is managed at the subprocess level to understand **causation** and **correlation**. Analysis drives **processes identification** and **inventories** for effectively mitigating risks and determining response levels.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND broad **incident analysis** is employed to identify shortfalls and performance gaps and drive process improvement. A team of knowledgeable information technology (IT) staff measures and assesses the full **cybersecurity landscape**, analyzing possible issues and identifying improvement opportunities.

ENTER SCORE

NOTES

RS3: INCIDENT RESPONSE REPORTING AND COMMUNICATION

LEVEL 1: INITIAL

Processes to define orderly **response activities** are lacking or nonexistent. Criteria for **incident reporting** are not clearly defined or are primarily reactive. Communication processes for **incident reporting** are unclear or nonexistent.

LEVEL 2: REPEATABLE

Processes to define orderly **response activities** are being developed. Proactive **coordination** with internal and external stakeholders is improving. Consistent **criteria** for incident reporting is being determined. A **systematic approach** to evaluation and improvement of key processes is being designed.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND processes to ensure orderly **response activities** are defined and shared. **Coordination** with stakeholders is in line with response plans. Information is shared with leadership and internal and external stakeholders to achieve transparent **situational awareness.**

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND processes are documented in a managed cybersecurity **incident communication plan.** Incident **responsibilities** are assigned to designated staff members. Defined criteria are used to measure the success of communications. **Evaluation** of the communication process is periodically conducted. Evaluation **results** drive tracked improvement initiatives.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND communications are **optimized** through collaboration with external cybersecurity and privacy groups, associations, and solution providers. Cybersecurity **alerts** and **recommendations** are obtained from and shared with external sources. **Response activities** are optimized using best practices, innovative processes, and technological aids.

ENTER SCORE

NOTES

RS4: INCIDENT MITIGATION

LEVEL 1: INITIAL

A systematic approach to prevent the **expansion** of an event is lacking or nonexistent. Processes or technologies to **mitigate** the effects of and **eradicate** an incident are not defined, and practices are ad hoc, inconsistent, and reactive.

LEVEL 2: REPEATABLE

Processes for preventing the **expansion** of an event, **mitigate** its effects, and **eradicate** the incident are defined. The overall **approach** for cyber defense is consistent. **Collaborative** problem solving is used to prevent the expansion of an event.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND activities are routinely performed to prevent event **expansion**. Processes and technologies to **mitigate** the effects of and **eradicate** an incident are available and practiced. Incidents are **contained**. Identified **vulnerabilities** are mitigated and/or documented as accepted risks.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND sophisticated **response mitigation** during a cybersecurity incident is routinely managed using best practices, tools, and techniques. Effective mitigation is used to isolate and block threats in near real time. Processes are universally **deployed** and **maintained** to manage mitigation and generate data.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND risk **mitigation activities** and **technical mechanisms** are proactively and interactively improved. **Roadmap** development is prioritized. Leadership understands the importance of building **resilience**. Resources are made available when **gaps** in capabilities are identified. **Vulnerabilities** are cataloged and **best practices** are collaboratively established.

ENTER SCORE

NOTES

CYBERSECURITY RUBRIC: RECOVER (RC)

RC1: Incident Recovery Plan Execution

LEVEL 1: INITIAL	LEVEL 2: REPEATABLE	LEVEL 3: DEFINED	LEVEL 4: MANAGED	LEVEL 5: OPTIMIZED
Incident plans are nonexistent or lacking. **Recovery** action steps for educational continuity are not determined. If a plan is present, it does not align with **strategic roadmaps** or cybersecurity **objectives.**	**Incident plans** are documented. **Recovery** action steps describe restoration **procedures** with clearly defined **roles and responsibilities. Plan execution** is detailed in depth for during and after cyber incidents.	Meets **REPEATABLE** Maturity Level **AND asset protection**, direct and indirect processes affecting normal **operations.** Evidence of plans being **executed** during or after cyber events is documented	Meets **DEFINED** Maturity Level **AND incident plans** are well managed. **Pre-incident asset protection and recovery** processes are routinely successful. **Business continuity** is tested. Leadership and information technology (IT) teams regularly **review** recovery processes. **Gap analyses** are completed with identified weaknesses translating to actionable improvement plans.	Meets **MANAGED** Maturity Level **AND** fully integrated **incident plans** are embedded into daily decision-making. **Recovery planning** is optimized using innovative techniques. **Post-recovery** (staged recovery planning or real-time cyber event recovery) includes addressing lessons learned and making improvements to the recovery plan. Leadership is committed to evolving **strategic plans** based on education market sector trends.

ENTER SCORE

NOTES

RC2: Incident Recovery Communication

LEVEL 1: INITIAL

A systematic approach for communicating **restoration activities** is lacking or nonexistent. **Conditions** and **responsibilities** under which the recovery plan is to be invoked are not defined or documented.

LEVEL 2: REPEATABLE

Processes are being developed to manage **media interactions**, handle and 'triage' **communication** requests, and ensure staff are apprised of **public relations** and **privacy** policies. **Action steps** to reduce damage inflicted by an event are defined. **Communications** include steps for handling data breaches and recovery activities.

LEVEL 3: DEFINED

Meets **REPEATABLE** Maturity Level

AND conditions and responsibilities under which the recovery plan is to be invok ed are documented. Communication about **restoration** activities and responsibilities is documented. **Public relations,** including reputation restoration after an event, are managed. Recovery **activities** are communicated to internal and external stakeholders, law enforcement agencies, and leadership teams.

LEVEL 4: MANAGED

Meets **DEFINED** Maturity Level

AND a coordinated **communication response** to achieve a balance between the cybersecurity investigation and recovery is managed with concern. Communication **channels** are identified in advance. Communication **templates** derived from a playbook or tabletop exercises are described. Improvement **initiatives** are set forth based on the evaluation results from communication exercises.

LEVEL 5: OPTIMIZED

Meets **MANAGED** Maturity Level

AND recovery **communications** undergo a continuous, cyclical improvement process and include a documented feedback and communication strategy. Feedback **analysis** identifies shortfalls or gaps in performance and drives measurable process improvement. **Transparent** communication is an integrated practice. A **playbook** with predefined communication topics helps to restore order and optimize the communication strategy.

ENTER SCORE

NOTES