TECHNOLOGY COMMITTEE

NOVEMBER 3, 2025

AGENDA

INFRASTRUCTURE

CYBER SECURITY

DEPARTMENT
NO UPDATES

WEBSITE
NO UPDATES

YOUTUBE UPDATE

AI CIRCLE UPDATE

NEW YORK STATE ASSOCIATION FOR COMPUTERS AND TECHNOLOGY IN EDUCATION CONFERENCE (NYSCATE)

INFRASTRUCTURE

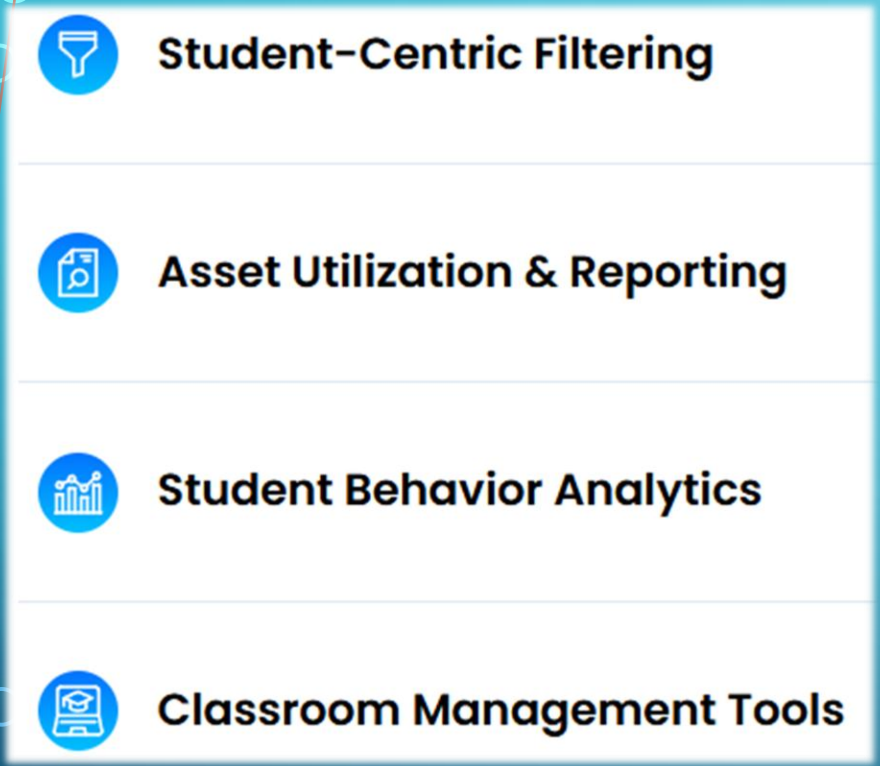
Previous meeting:

- The SSBA amendment to allocate funds for Interactive Displays has been approved.
- Majority of devices have been upgraded to Windows 11; a few still require replacement.
- Desktop replacements were acquired during the summer.

Updates:

- Field technicians finishing up the Windows upgrades.

ARISTOTLEK12



Student-Centric Filtering

Asset Utilization & Reporting

Student Behavior Analytics

Classroom Management Tools

- Aristotle K12 offers an educational platform that includes content filtering, classroom management, and resources for self-harm support.
- Replaced GoGuardian.
- Aristotle K12 is compatible with various devices including Chromebooks, iPads, and Windows systems.
- Its classroom management features provide detailed reporting and allow teachers to manage internet access comprehensively.
- Deployed on July 7, 2025.

SERGEANT LABORATORIES | 25 YEAR ANNIVERSARY

CYBER SECURITY

NATIONAL INSTITUTE OF STANDARDS CYBERSECURITY FRAMEWORK 2.0

The NIST Cybersecurity Framework 2.0 is an updated version of the original framework, providing organizations with guidance on managing and reducing cybersecurity risks.

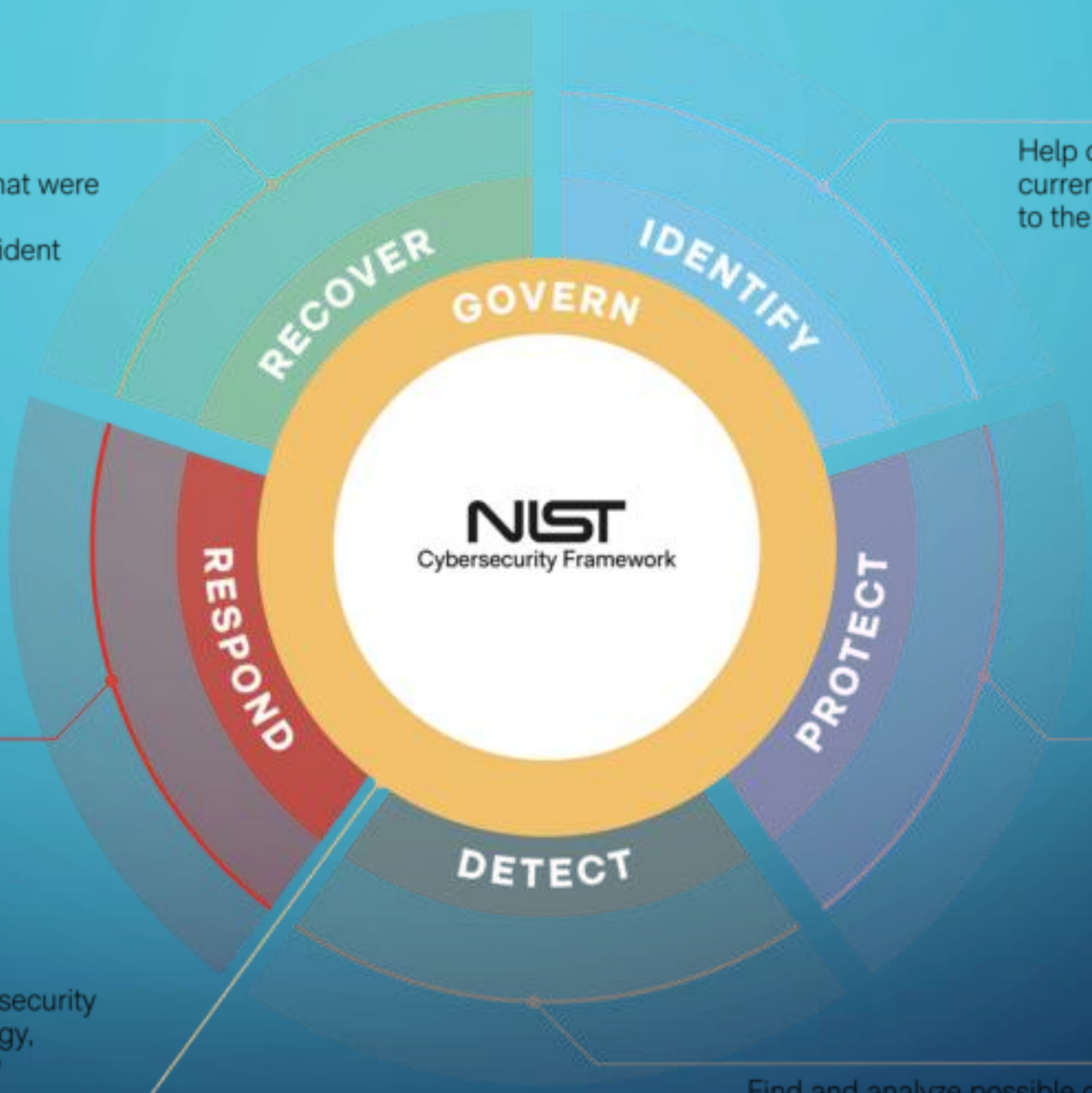
NIST 2.0 introduces a new **GOVERN (GV)** function alongside the existing Identify, Protect, Detect, Respond, and Recover functions, emphasizing the role of governance and risk management.

This framework is flexible and scalable, making it applicable to organizations of various sizes and sectors, including education, healthcare, and critical infrastructure.

NIST 2.0 helps align cybersecurity practices with business objectives and regulatory requirements, supporting organizations in enhancing their resilience to new and evolving threats.

*As per PBOR, Schools are required to implement the NIST Cybersecurity Framework.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



Restore assets and operations that were impacted by a cybersecurity incident

Help determine the current cybersecurity risk to the organization

Take action regarding a detected cybersecurity incident

Use safeguards to prevent or reduce cybersecurity risk

Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

Find and analyze possible cybersecurity attacks and compromises

Expanded Framework Functions

NIST CSF 2.0 adds a new GOVERN function alongside Identify, Protect, Detect, Respond, and Recover.

Comprehensive Structure

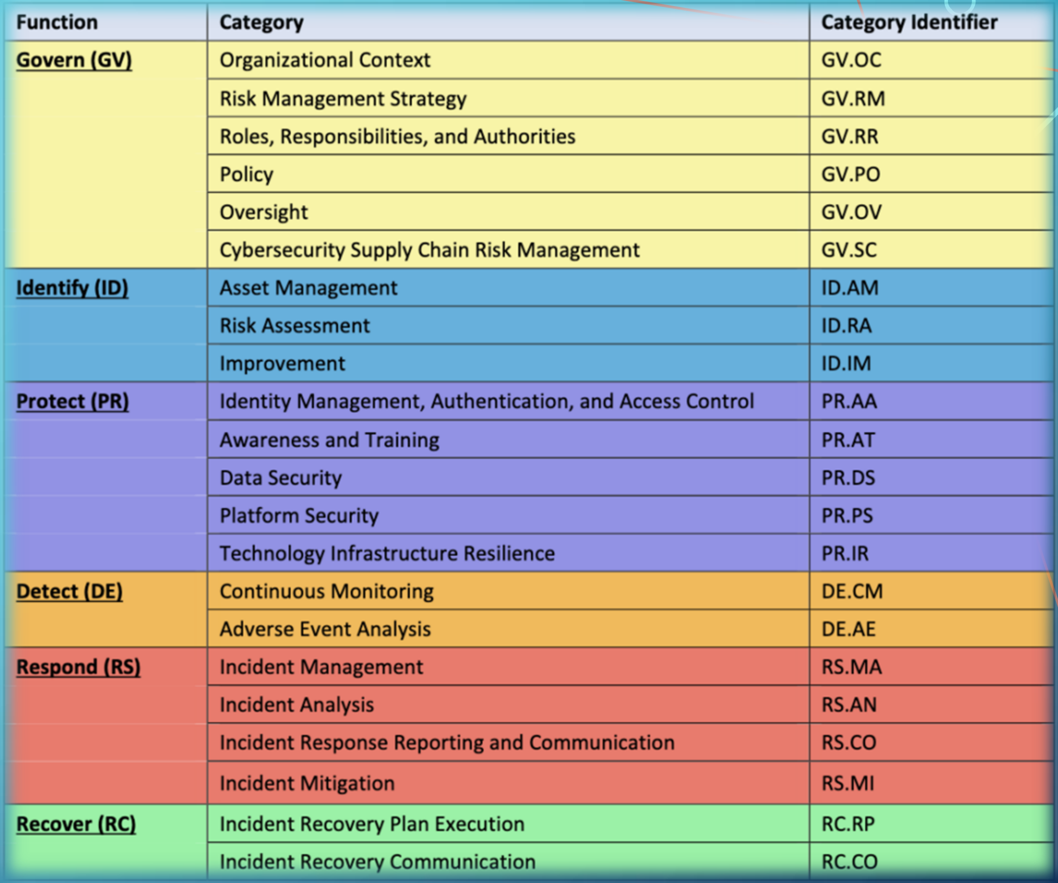
The framework includes six functions, 22 categories, and 106 subcategories for scalability.

Organizational Profiles and Tiers

Profiles and Tiers help organizations assess cybersecurity posture and plan improvements.

Applicability Across Sectors

Designed for organizations of all sizes and sectors, including K-12 school districts.



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

PURPOSE AND IMPORTANCE OF GOVERN

Strategic Cybersecurity Risk

GOVERN treats cybersecurity as a strategic business risk, not just technical. It aligns risk management with organizational goals effectively.

Defined Roles and Policies

Establishes clear expectations for staff, vendors, and stakeholders with guiding cybersecurity policies.

K-12 Data Protection

Critical for protecting sensitive student and staff data and ensuring compliance with regulations like FERPA and COPPA.

Building Resilience

Helps build resilience against threats like ransomware and phishing, maintaining trust with community stakeholders.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CATEGORIES WITHIN THE GOVERN FUNCTION

Organizational Context

Focuses on understanding mission, stakeholder needs, and regulatory requirements to guide governance.

Risk Management Strategy

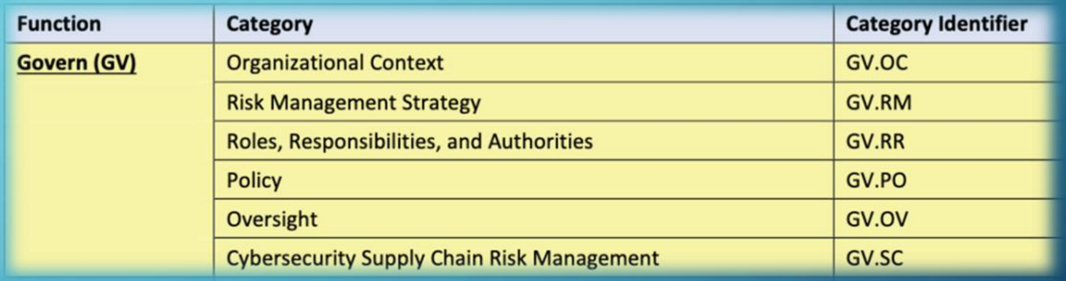
Defines risk appetite and integrates cybersecurity into enterprise risk management practices.

Roles, Responsibilities, Authorities

Ensures clear assignment of roles, responsibilities, and escalation paths within governance.

Policy Development

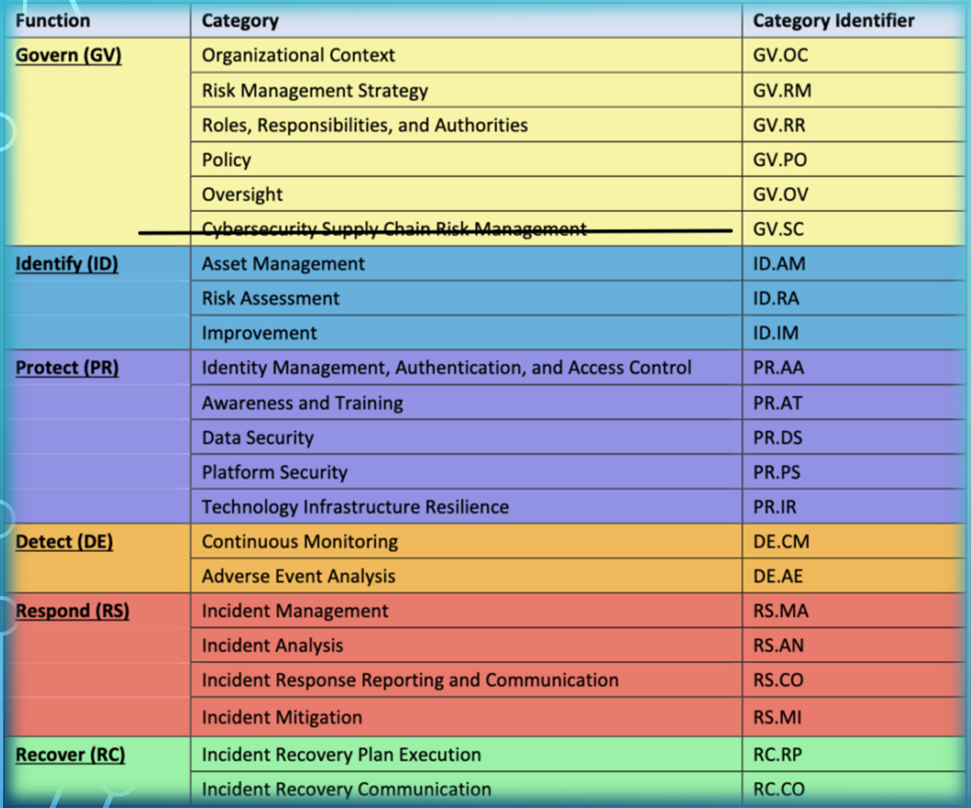
Covers creation and maintenance of cybersecurity policies to support governance objectives.



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

ACTION PLAN FOR GOVERN IMPLEMENTATION



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Document Mission and Compliance

Record district mission, stakeholder expectations, and compliance with laws like FERPA and COPPA.

Define Risk Appetite and Register

Establish cybersecurity risk tolerance and maintain a risk register to prioritize threats.

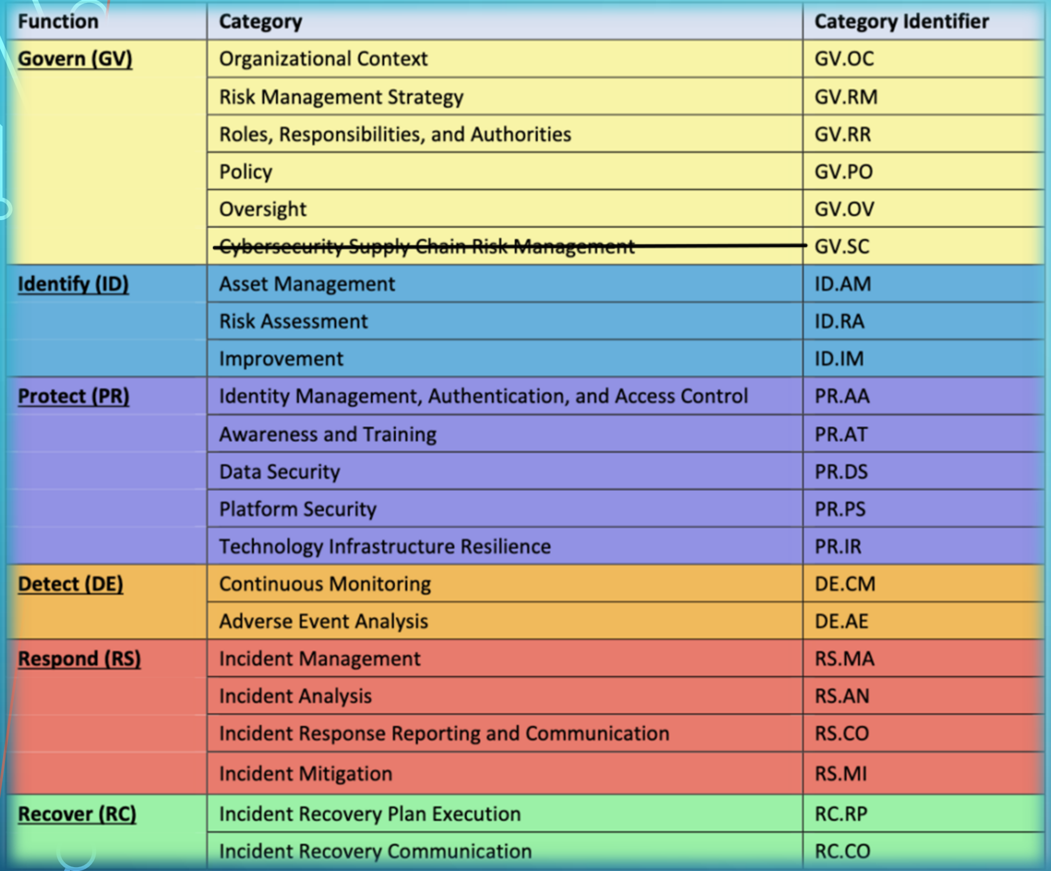
Assign Roles and Responsibilities

Clarify roles, including escalation paths for incident response within the district.

Develop Policies and Monitor Compliance

Create and annually review cybersecurity policies and monitor compliance continuously.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

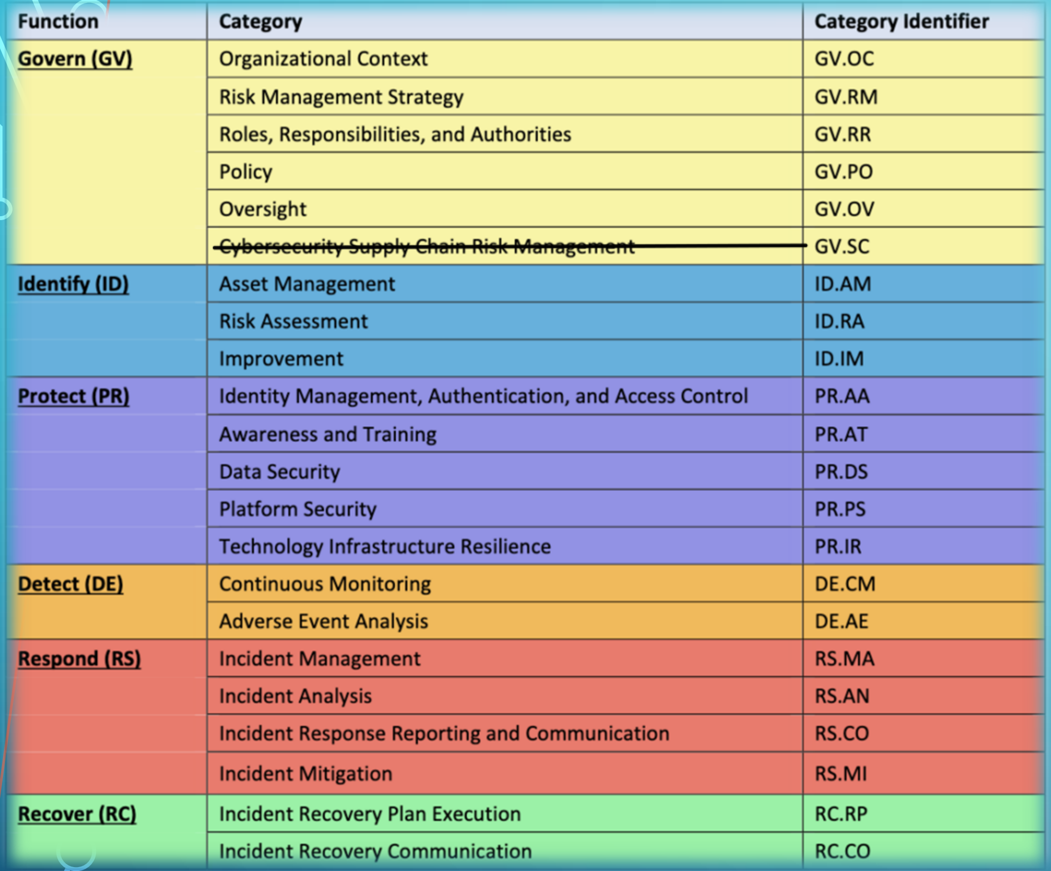
1. Organizational Context (GV.OC)

Our mission is to provide a safe and effective learning environment for all students.

Cybersecurity is essential to protect student data, educational resources, and administrative systems.

Stakeholders include students, parents, staff, vendors, and regulatory bodies. We comply with FERPA, COPPA, and other applicable laws and regulations.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



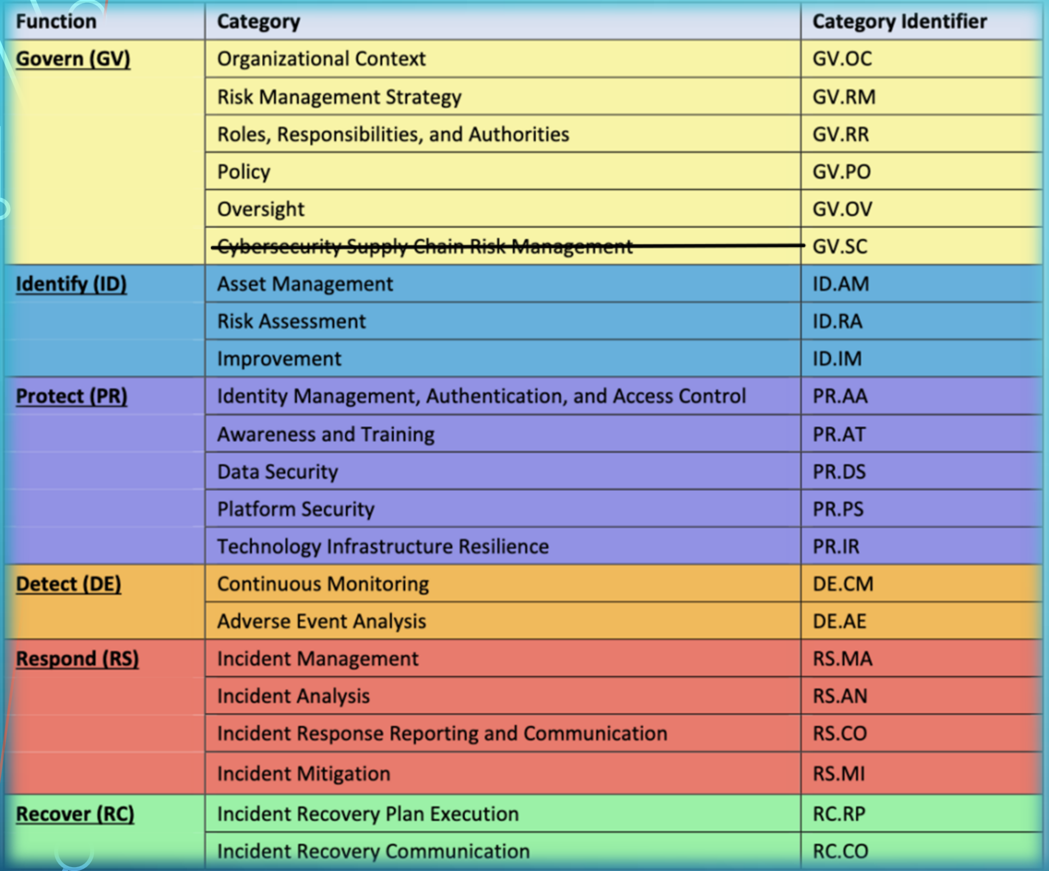
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

2. Risk Management Strategy (GV.RM)

The district maintains a risk register to identify, assess, and prioritize cybersecurity risks.

We define our risk appetite as low, with a focus on minimizing exposure to threats that could disrupt educational services or compromise sensitive data.

Cybersecurity risks are integrated into our overall enterprise risk management strategy.



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

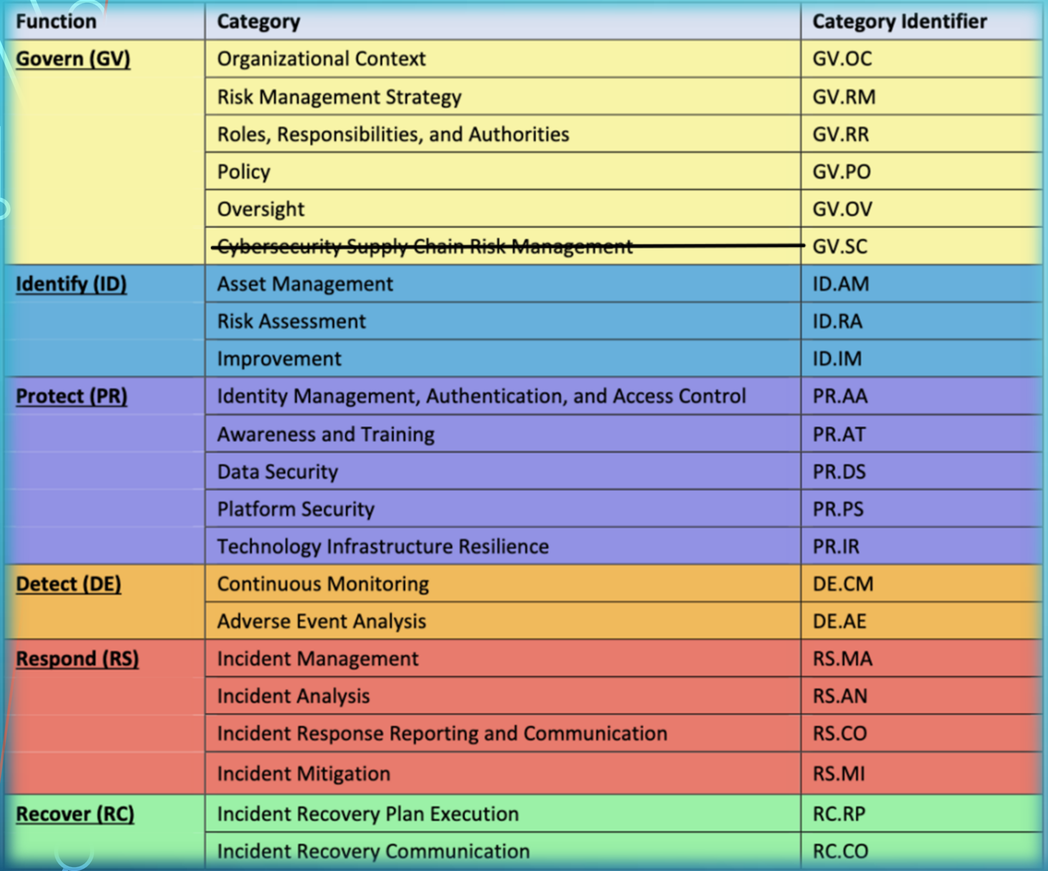
3. Roles, Responsibilities, and Authorities (GV.RR)

The Superintendent oversees cybersecurity governance.

The IT Director is responsible for implementing cybersecurity controls and reporting incidents.

All staff are expected to follow cybersecurity policies and participate in annual training.

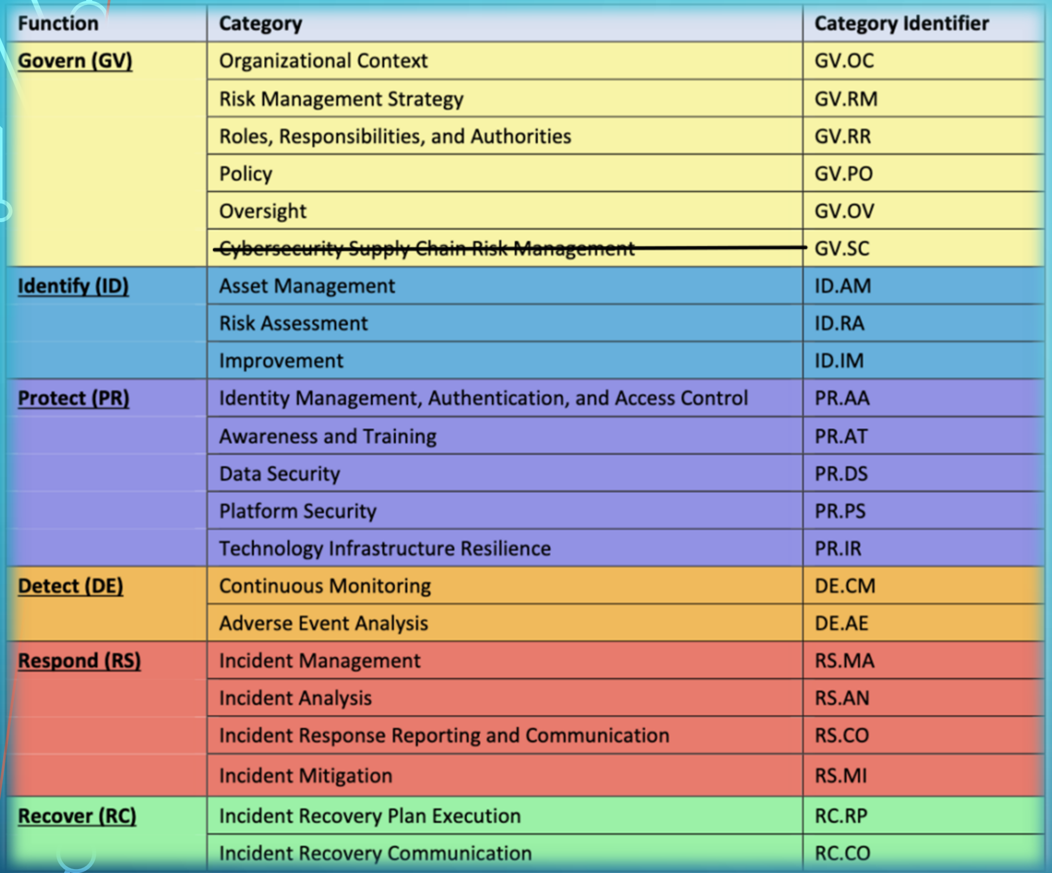
4. Policy Development (GV.PO)



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

The district has established the following cybersecurity policies:
- Information Security Policy
- Identification and Authentication Policy
- Security Assessment and Authorization Policy
- Systems and Services Acquisition Policy

These policies are reviewed annually and updated as needed to reflect changes in technology and threat landscape.



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	~~Cybersecurity Supply Chain Risk Management~~	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

5. Oversight (GV.OV)

Cybersecurity performance is monitored through regular audits and assessments.

The School Board receives quarterly reports on cybersecurity posture, including incidents, training completion rates, and compliance metrics.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

BENEFITS OF GOVERN FOR K-12 DISTRICTS

Data Protection

GOVERN helps shield sensitive student and staff data from unauthorized access and cyber threats.

Regulatory Compliance

Aligning cybersecurity with laws like FERPA and COPPA ensures district compliance and legal adherence.

Threat Resilience

GOVERN strengthens defenses against ransomware and phishing, minimizing operational disruptions.

Stakeholder Trust

Demonstrating due diligence fosters trust and accountability among parents, staff, and auditors.

REVIEW NIST 2.0 WORKSHEET

NIST 2.0 EXPECTATIONS

IT Director with collaborate with stake holders, composing the framework.

Align framework with Organizational Mission and Objectives.

Establish Governance and Accountability.

Integrate Risk Management.

Communicate and monitor polices.

Foster a Cultural Shift.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

UPDATE

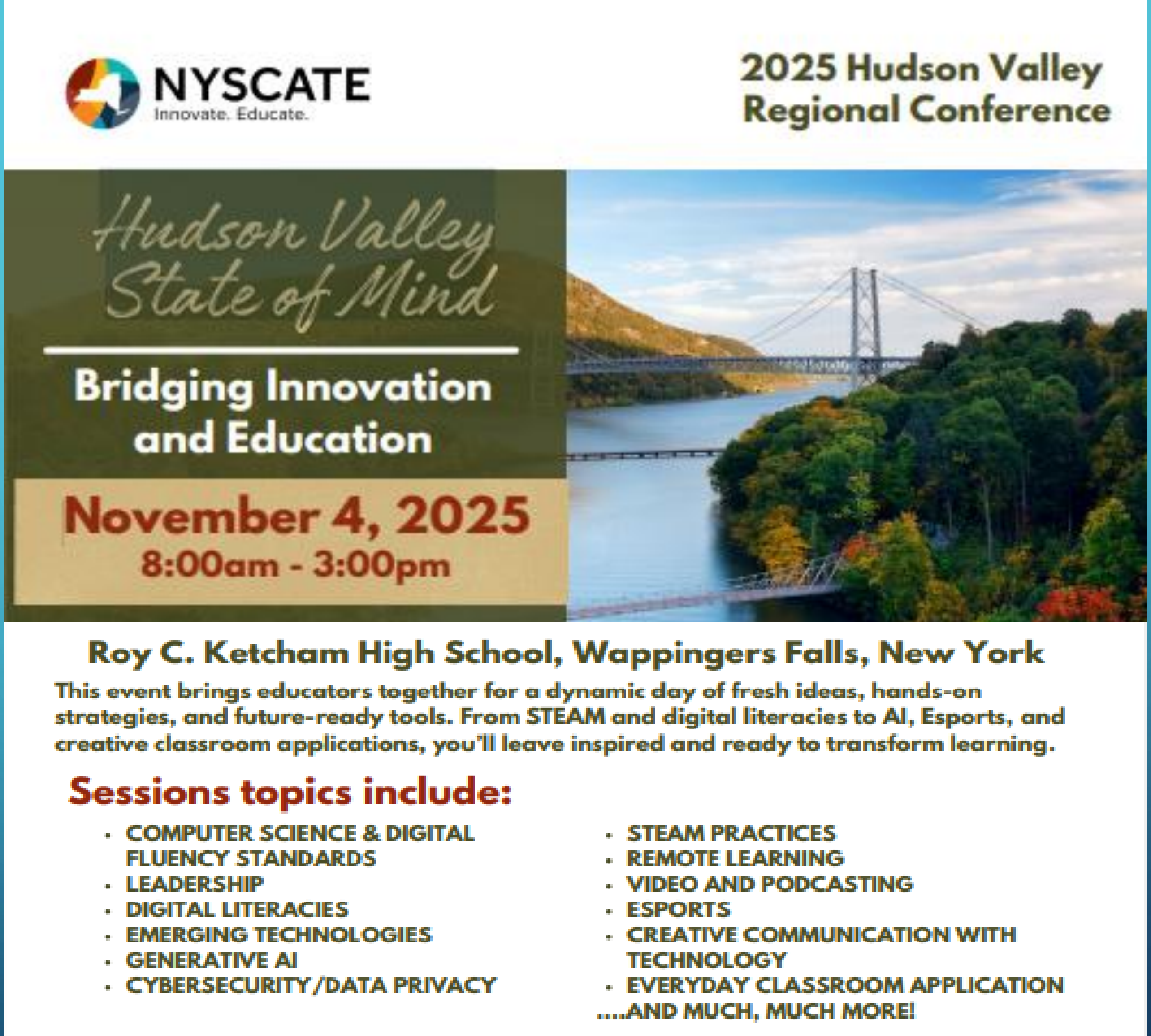
TECHNOLOGY CONSULTANT WORK UPDATE (ULSTER BOCES PARTNERSHIP)

- Met on 10/30/2025 with Mollie Cahill and Julianne Ross-Kleinman (Ulster BOCES) to begin to plan an in-house professional development series for teachers in grades 9-12.
- Topics: Using District Technology and Artificial Intelligence to Drive Project-Based Learning Lesson Planning and Assessment. How does Project Based Learning connect with the NY Inspires Initiative and the New York State Portrait of Graduate work that we are beginning to explore.
- Target Dates: First Sessions in December, Second Sessions in Spring Semester

AI CIRCLE TEAM UPDATE

- On 10/7/2025, educators from across the county and beyond joined the **AI Circle**, a professional development conference held at the Jane Bullowa Conference Center.
- School district teams explored how AI can enhance teaching and learning through hands-on sessions, collaboration, and creative lesson design.
- The **AI Circle** is a year-long deep dive into how to meaningfully and safely integrate AI into our district.
  - Critically evaluate AI's role in teaching and learning
  - Develop a district vision related to AI
  - Leverage AI tools to design and implement AI enhanced lessons or projects

NYSCATE HUDSON VALLEY REGIONAL CONFERENCE



NYSCATE
Innovate. Educate.

2025 Hudson Valley
Regional Conference

Hudson Valley
State of Mind

Bridging Innovation
and Education

November 4, 2025
8:00am - 3:00pm

Roy C. Ketcham High School, Wappingers Falls, New York

This event brings educators together for a dynamic day of fresh ideas, hands-on strategies, and future-ready tools. From STEAM and digital literacies to AI, Esports, and creative classroom applications, you'll leave inspired and ready to transform learning.

Sessions topics include:

- COMPUTER SCIENCE & DIGITAL FLUENCY STANDARDS
- LEADERSHIP
- DIGITAL LITERACIES
- EMERGING TECHNOLOGIES
- GENERATIVE AI
- CYBERSECURITY/DATA PRIVACY
- STEAM PRACTICES
- REMOTE LEARNING
- VIDEO AND PODCASTING
- ESPORTS
- CREATIVE COMMUNICATION WITH TECHNOLOGY
- EVERYDAY CLASSROOM APPLICATION

....AND MUCH, MUCH MORE!

Mr. Hein (Director of Technology) and Mr. Masopust (Asst. Superintendent for Educational Services) will attend to continue to explore how to leverage technology to enhance instruction

FUTURE MEETING DATES

- *Monday, December 8, 2025, 3:30 p.m. - High School Room 102*
- *Monday, February 9, 2026, 3:30 p.m. - High School Room 102*
- *Monday, April 27, 2026, 3:30 p.m. - High School Room 102*