THE POWER
OF BEING
UNDERSTOOD

CYBERPROTECTED

A commitment to securing Iowa's education system

Advancing technologies and evolving cyberthreats have today's educational institutions facing demands for increased security with diminishing budgets and fewer resources. With proactive planning and guidance, however, educational institutions can be in a better position to defend against or remediate cyberattacks.

Fortunately, the Iowa Association of School Boards (IASB) has recognized that cybersecurity is one of the most challenging issues facing its members. As a result, the organization has selected RSM US LLP as an affiliate to serve Iowa educational institutions to better their overall security posture.

RSM and the IASB have developed CyberProtectEd to help Iowa's education system overcome a host of cybersecurity challenges. These include:

Challenges	CyberProtectEd solutions
▪ Increased cybersecurity and information security risks ▪ Demands by parents, educators and students that their personal information is safe ▪ Increased regulatory burdens	RSM's highly experienced security consultants help you understand the risks to your organization (including applicable regulatory requirements) and how to solve them
▪ Limited IT budgets and IT resource constraints	RSM can perform security assessments and supplement current staff to assist with prioritization, strategy and remediation efforts
▪ A constantly changing and evolving threat landscape	RSM can conduct regular cybersecurity awareness training to help reduce the susceptibility of end users, which is often a district's weakest link

RSM offers a variety of services as part of the CyberProtectED program. You can choose any or all of the following solutions to develop a customized platform that fits your institution's needs:

Core cyberrisk assessment – The goal of this basic assessment package is to provide an analysis of your current cybersecurity posture in order to identify gaps and areas of improvement. We examine both internal and external areas of your institution to help you understand the full scope of your potential risks.

Advanced cyberrisk assessment – RSM's advanced cyberrisk assessment is intended for districts and institutions looking to understand the full threat landscape and their level of preparedness. These in-depth tests include:

- Wireless penetration testing – Our team tests your wireless network to determine if unauthorized access can be obtained by students or other guests.
- Internal and external penetration testing – A penetration test paints the picture of what information a hacker may be able to access, such as student or administrator information or other nonpublic information.
- Social engineering assessment – Email phishing and phone call attempts can be made to schools to test the overall security awareness of the district and likelihood of falling victim to one of these attacks.
- Physical security review – We will attempt unauthorized access to buildings by posing as an IT vendor or parent. This test can determine if an unauthorized guest would be allowed entrance to the building.
- Business continuity plan review – We provide a current-state analysis of key observations for enhancement and notable accomplishments for the plan.

CyberProtectED

IASB
Iowa Association
of School Boards

RSM

Cybersecurity training and awareness – Attackers continue to count on the susceptibility of end users to gain access to a network. This assessment will help you design training for staff and students, from reviewing your existing training content and processes to designing new ones. Examples of services included in this package are:

- Cyber awareness training and program development – As part of this assessment we will deliver a comprehensive and thoroughly tested security awareness training program to educate staff and students on recognizing threats. Using that training, we can develop a program to ensure ongoing education is part of an overall security program.
- Incident response program facilitation and guidance – This assessment will help prepare you for a cybersecurity incident by creating an incident response plan and running through that plan via a role-playing tabletop exercise.

Cybersecurity staff support – Most districts know that a security program is necessary, but they lack the talent and resources to make it happen. This program provides support for your internal IT staff from RSM's highly trained cybersecurity team. Examples of services in this package are:

- Virtual chief information security officer (vCISO) – As a vCISO for your district, RSM will assist with developing and implementing an overall cybersecurity strategy. This may include attending your cybersecurity steering committee meetings, yearly planning and budgeting, and prioritizing your cybersecurity efforts.
- Remediation assistance services – A district's IT staff is often very busy running day-to-day activities. RSM can supplement and assist your staff with cybersecurity remediation efforts to ensure you are able to act upon assessment findings.

Reporting package – Conducting regular assessments alone is not enough if the results are not relayed in a digestible way so that all interested parties can understand. All CyberProtectED programs come with a reporting package customized to help your superintendent and district staff understand the situation, with recommended priorities to better protect your district. As a CyberProtectED client you will receive:

- Board and executive briefing report – This report will break down assessment results at a high level to help your board and staff understand the major strengths and areas of improvement for your district. In addition, this report will contain a summary of all the assessment activities, results and recommendations for the path forward.
- Technical report and exhibits – These reports are intended as action plans for your technical staff and will outline testing results and recommendations for improvement. This includes a summary of the potential impact of the findings and technical details to assist IT staff with understanding risks and how to best implement changes.

The RSM difference

RSM is a leading national provider of security services. We have over 125 dedicated security and privacy professionals in the United States with deep, hands-on experience covering a wide range of industries. We hold numerous industry certifications including Certified Ethical Hacker (CEH), GIAC Penetration Tester (GPEN), GIAC Reserve Engineer of Malware (GREM), GIAC Certified Forensic Examiner (GCFE), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor/Manager (CISA/CISM) and Certified Information Privacy Professional (CIPP).

Our depth of experience enables us to understand your cybersecurity threats, no matter how complex or where they originate. Whether you need an experienced team to help you develop your cybersecurity strategy, test and remediate your network for vulnerabilities, prepare for an incident, or respond to an incident, we're ready to help.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed. RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International. RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood*® is a registered trademark of RSM US LLP.