Xacta® for Higher Education

Cybersecurity Challenges for Higher Ed: Visibility and Accountability

How to manage risk to federated architectures, illuminate security blind spots, and assure federal compliance with confidence.

Higher education is facing a new world of cybersecurity and are now required to comply with multiple domestic and international regulations. The rapid move to remote learning provided an irresistible opportunity for malicious actors, who have been targeting schools with denial-of-service and ransomware attacks that deprive students and faculty access to remote learning environments, while saboteurs “zoombomb” live classrooms with inappropriate material, verbal harassment, and the doxxing of class participants.

Institutions that receive federal or DoD grants for research programs face the additional challenge of adhering to NIST SP 800-171 or implementing the new Cybersecurity Maturity Model Certification (CMMC) guidelines for their collaborative programs. Higher ed CTOs and CIOs are under a lot of pressure, but they can make their jobs easier and their academic communities safer by automating workflows, continuously assessing their cybersecurity posture, and working with a single source of security truth to achieve visibility and compliance

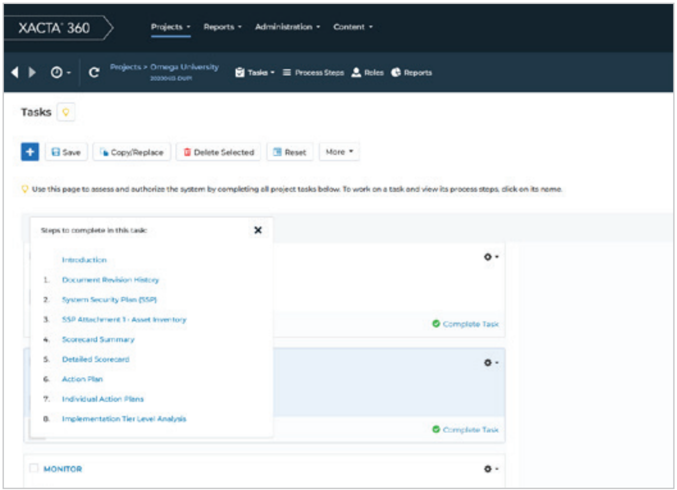
> **Ransomware is the Number 1 cyber threat facing higher education, with attacks on colleges doubling between 2019 and 2020.**
>
> *– “Cybersecurity in Higher Education”; BlueVoyant, February 2021*

Even before the pandemic, colleges had to support a wide diversity of devices, including instructional technology, lab equipment, IoT devices, and BYOD tablets and laptops, as well as dealing with the student-owned phones and gaming systems that were brought onto campus each day. And now, networks are connecting with additional devices beyond their control: home computers that may be running outdated operating systems and SaaS services that professors may be using to store sensitive data or important research.

Without knowing who or what is accessing the network and where data is moving, there is no way to apply proper policies or decide which assets need which controls. Visibility exposes that information so that resources can be directed where they are needed, whether that means updating a policy, adding a new firewall, or segmenting critical data behind additional defenses.

“We don’t know what we have to do to meet CMMC.”

Large universities operate like commercial enterprises, with the added complexity of meeting federal grant funding requirements. If a university receives a grant to conduct R&D for the Department of Defense, it must meet the same cybersecurity requirements the DoD would have to meet if it did the project in-house.



Use this page to assess and authorize the system by completing all project tasks below. To work on a task and view its process steps, click on its name.

Steps to complete in this task

Introduction
1. Document Revision History
2. System Security Plan (SSP)
3. SSP Attachment 1 - Asset Inventory
4. Scorecard Summary
5. Detailed Scorecard
6. Action Plan
7. Individual Action Plans
8. Implementation Tier Level Analysis

Automated workflow and documentation capabilities in Xacta allow you to easily implement cybersecurity frameworks and standardize outputs.

But awareness of CMMC requirements is often not fully understood by all the stakeholders involved in writing and submitting grant applications and conducting research. The risk of misunderstanding CMMC is high: an overlooked requirement can seriously impact a project’s budget or result in losing the funding entirely. And the clock is ticking: all organizations engaging with the DoD have to be CMMC compliant by October 1, 2025 if they want to keep their programs alive.

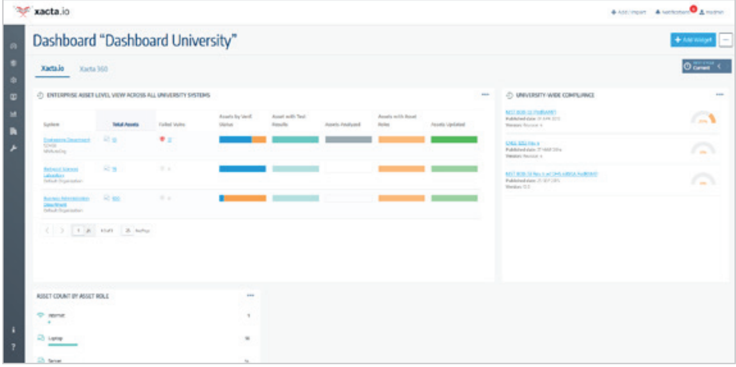
> **At least five nation-state campaigns were conducted against universities since 2019. And those are just the ones that were caught.**
>
> *– Cybersecurity Dive*

Limited IT staff. Limited understanding of CMMC. Limitless threats.
But there is a way to prepare!

Get your institution to the next level of cybersecurity maturity with Xacta®, a cyber risk management and compliance solution that provides visibility, continuous auditing, and continuous vulnerability reporting.

You don't have the people? You can still have the power.

Xacta does the work of six people for the price of one, freeing up IT staff to focus on strategic efforts instead of performing repetitive manual tasks that inject the wildcard of human error into the cybersecurity process.



Xacta's dashboard puts all of your asset, vulnerability, and compliance data into a unified view for simplified analysis and remediation.

Many educational institutions are operating on a distributed responsibility model: network engineers pull network security data, while endpoint people focus on standards compliance and patching. All that data has to be normalized and shared in order to become actionable. Xacta eliminates those manual steps by using APIs to capture data from across the environment and make it available through a single console. IT staff gains a comprehensive view the school's security and compliance posture, while CTOs get the information they need to make immediate decisions.

Save audit time and effort by aligning and mapping security controls.

Colleges and universities have to comply with diverse range of IT security standards. Xacta's extensive policy library contains the controls most commonly used in higher education, including the NIST standards and ISO 270001. It also supports specialized standards that certain departments and functions must meet, including HIPAA, HITECH, PCI-DSS, and others. Xacta's industry-unique Predictive Mapping™ capability crosswalks one standard to another for one-to-many mappings to reduce audit fatigue by enabling you to test once and comply with multiple standards.

Always be ready for an audit (and confident about your documentation).

Xacta offers customizable workflows and no-code templates that can be easily tailored to your requirements. Flexible baseline tailoring simplifies and speeds implementation, and a no-code interface makes it easy for IT staff to enact changes on the fly in the future. And, Xacta provides a centralized body of evidence that enables you to automatically generate the reports and documentation you need to demonstrate that you've taken the right steps to keep the academic community safe.

Inheritance offers compliance synchronization with cloud providers.

Xacta accelerates cloud adoption for higher education by operationalizing shared security models and allowing cloud users to automatically inherit extensive security compliance information related to the cloud services that they use. This automated inheritance capability can reduce time and effort for critical compliance activities up to 90%.

Protect your school's federal research programs.

Xacta enables you to identify gaps in your protection of CUI and plan the security technologies you should implement in order to meet federal and defense requirements. Xacta simplifies and centralizes CMMC activities and enables you to manage your certification efficiently over time with automatic control periodicity. When it's time for C3PAO review, you can be confident your institution is ready. Xacta also helps ensure your campus incubator's cloud-based federal apps and services are FedRAMP-ready on launch day.

Your investment in Telos offerings for cybersecurity, risk management, and compliance may be eligible for coverage by GEER funds through the U.S. Department of Education. Contact the grants and funding office for your institution or state or ask your Telos representative for further information.

Learn more about how Xacta helps you manage and defend against cyber risks.

Contact us for a conversation and demonstration of how Xacta helps protect students, faculty, administration, and critical assets and systems by automating cyber risk and security best practices.

Telos® Solutions that **empower** and **protect** the enterprise.™

XFHE-022024-W