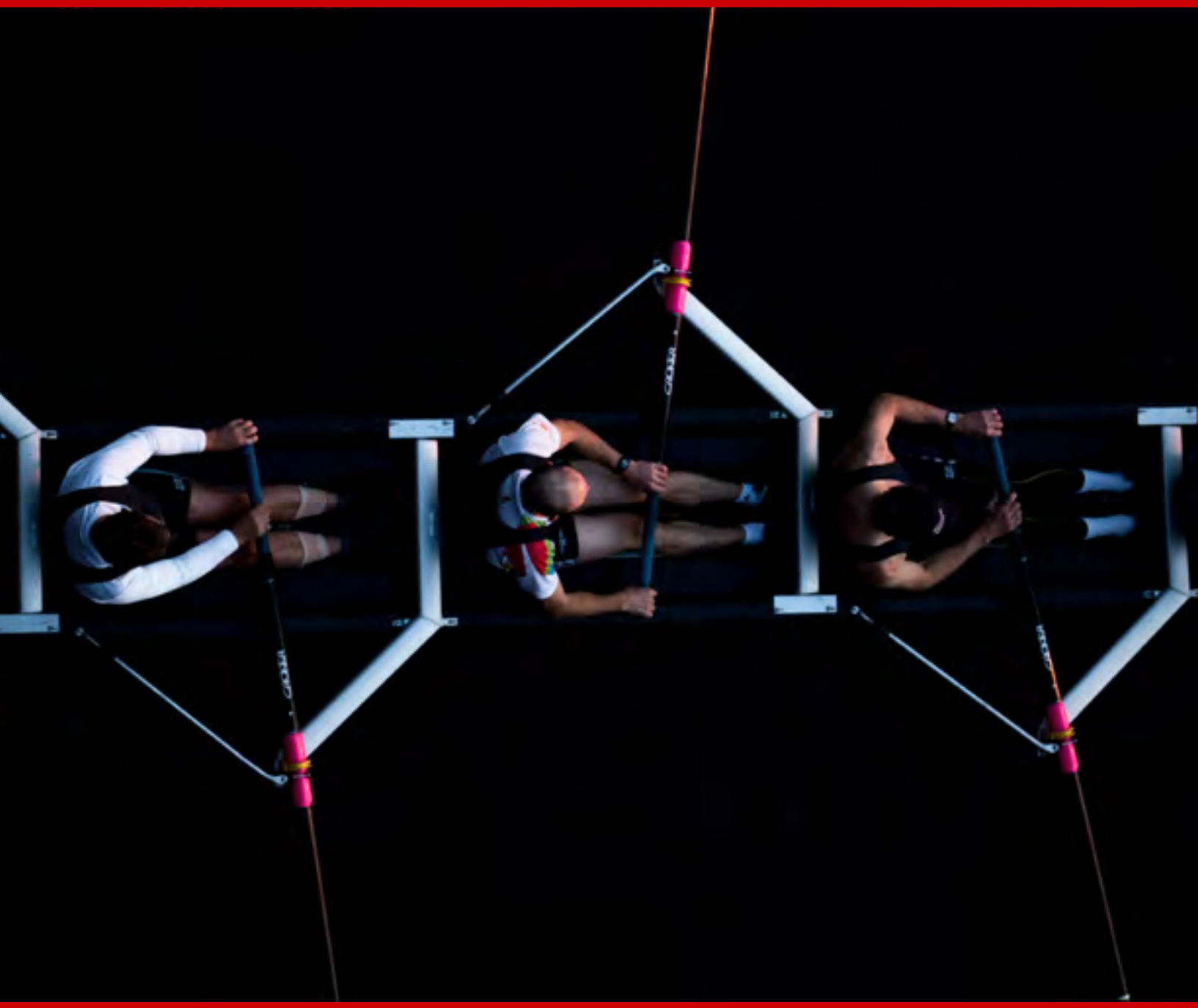
WHITE PAPER

HITACHI
Inspire the Next

Choosing the Right Program Can Be a Game Changer

Tips for Colleges and Universities on Selecting and Sequencing Your IAM, PAM, and IGA Implementations



Hitachi ID

Driving Modernization and Digital Transformation in Higher Education

Work and learning are moving from place-based to remote, and the cybersecurity threats to higher education institutions are shifting with them. With hybrid, remote, and distance learning here to stay, universities are on a quest to provide seamless yet secure, modern learning experiences equivalent to in-person models. The continual change in pressures and threats has upended higher education cybersecurity strategy. For institutions to prevent, detect, and respond to these new threats new technologies and strategies are required.

New security methodologies like Zero Trust, where no one is trusted by default across the deperimeterization of infrastructures, are required to lower these new risks and defend against breaches. New models such as Zero Trust are only the beginning, however. Higher education institutions will need the technology to make it happen. So, what's the solution?

As the virtual university IT architectures now rival the physical campus establishment in importance, universities are fighting to keep up but it doesn't have to be this way. The student information system and identity administration were important before, and suddenly, this complex network of populations including students, faculty, staff, alumni, affiliates, and more demand a new level of precision. Identity access management (including identity governance) and privileged access management is the answer. These powerful elements of a digital transformation can revolutionize your systems and enable new required strategies like Zero Trust to modernize, stay competitive, and combat threats.

With the acceleration of modernization and digital transformation,

35%

of campus leadership is struggling to respond to these changing circumstances and new opportunities rapidly, and 33% are finding difficulty enabling a seamless student experience, according to Educause.[1]

1. "Educause Driving Digital Transformation in Higher Education Research Report," 2020, D. Christopher Brooks, Mark McCormack

Identity Access Management vs. Identity Governance

Identity governance, a subset of identity access management, also plays an important part in your digital strategy. As the policy-based orchestration of user identity management and access control, identity governance helps support higher education IT security and regulatory compliance but it's only a piece of the puzzle, not the full picture. Identity access management and automation is the best combination and option (providing full coverage and maintenance) in an age of heightened security threats.

Staying Competitive with Automated Identity Access Management

Higher education institutions prioritize efforts that bring the most significant value and tangible results due to industry-wide budget constraints. So, as identity access management and identity governance become a cornerstone of the modern, digital-first college or university in the post-COVID paradigm, they have needed to embrace this crucial component of digital transformation, unintentionally or purposefully, to remain competitive and survive.

That's why strategic identity access management deployment can be a make or break step for higher education institutions, and choosing the right vendor can be a game-changer for your college or university's digital transformation. You have many choices when selecting a modern identity access management and privileged access management solution, but only a few were purpose-built for higher education in mind, and that higher ed experience can make a world of difference.

The Unique Identity Access Management Challenges in Higher Education

Higher education faces many unique access management challenges compared to enterprise counterparts.

With their ubiquity, perhaps your institution has accepted these struggles as unavoidable. It doesn't have to be that way. By choosing an access management solution and partner with relevant higher education experience, your institution can quickly navigate industry-related challenges and recover countless hours for your IT leadership and teams to dedicate to more impactful and strategic projects.

These challenges include:

Large transient user populations

More than any enterprise organization, colleges and universities have an unprecedented level of natural turnover between semesters, undergraduate and graduate programs. This process involves revoking entitlements, changing identities, and reorganizing credentials at a massive scale. It's often a manual process and can be highly vulnerable to human error and misappropriated profiles and accounts.

Your IT staff has limited bandwidth, and this time-consuming and delay-ridden onboarding process can put a strain on valuable resources. And if the process breaks down, it creates disused accounts that can increase the attack surface available to hackers, increasing your vulnerability and risk.

An implementation solution that inherently understands higher education culture will cut down on the number of inappropriate access rights and stray accounts by introducing automatic access deactivation and control processes. These tools will strengthen governance and reduce vulnerability. By automating these time-intensive functions, IT teams at colleges and universities gain efficiency and increased optimizations, giving them more time for strategic initiatives.

Limited budgets and resources

Compared to their complexity and size, higher education institutions work with limited resources and budgets.

They require a scaling pricing model that fits budgets of all ranges and a solution they can deploy in phases according to where your organization is in its digital transformation.

Legacy homegrown systems

Constrained budgets have also had another unfortunate consequence. Many higher education institutions run on empty with open-source, legacy, and homegrown access management systems running the school's entire identity program. They may have met the institution's needs at one point or another, but they have grown inefficient and bound together with a patchwork of hotfixes and coding injections over the years.

By prioritizing updating legacy access management systems and processes with a partner well-versed in higher ed, you can combat risk and reclaim hours. And with a higher ed digital transformation strategy that brings all of the crucial actions of access, identity, and privilege together, you'll be better equipped to manage and sequence your identity access management and privileged access management implementations while reducing the risk of unauthorized access.

Preferred name changes and preferred pronouns

Name changes are typical for numerous reasons, including marriage, divorce, or a change in gender identity in the contemporary context. Under the Obama Administration, the Departments of Education and Justice released guidance on school's responsibilities towards transgender students.

From the traditional to modern name change needs, higher education institutions need to stay capable of making these adjustments to receive public funds, maintain reputation, and develop a beneficial and forward-looking student experience.

Blended roles and multiple affiliations

Unlike their enterprise counterparts, it's not unusual for someone at a college or university to simultaneously maintain two or more roles, like a staff member also enrolled in classes or a graduate student who is also a teacher's assistant.

Schools need a robust privileged access system versatile enough to support these multi-role conditions, maintain personal information integrity, and strengthen the institution's cybersecurity with these overlapping affiliations.

The Power of Higher Education Experience

It's clear from these vertical-specific challenges and the ever-growing importance of access management as a digital transformation enabler that this critical decision has significant implications for your college and university's long-term viability and competitiveness.

Ultimately, you need a solutions partner that will walk with you throughout your access management journey and, consequently, digital transformation. An experienced vendor can help you select and sequence your identity access management, privileged access management implementations and help ensure flawless execution and performance at every phase.

The right partner can assist you in critical strategy decisions moving your access management culture beyond legacy systems and into the future by:

- Embracing the higher education culture
- Prepping you before your modernization and digital transformation
- Providing a practical approach to implementation
- Outlining actual, achievable steps that help you complete smaller bite-sized pieces of more significant projects, access management, and digital transformation
- Budgeting, supporting, planning, and giving access compatible with higher education resources

Selecting and Sequencing Your Identity and Privileged Access Management and Governance Solution

Build Your Roadmap

Before executing your identity and privileged access management modernization, your higher education institution should inventory its business processes and technical infrastructures. This prerequisite audit will build your roadmap and includes a:

Network security audit

- Approved-use, communications, antivirus, identity, password, encryption, remote access policies, and more

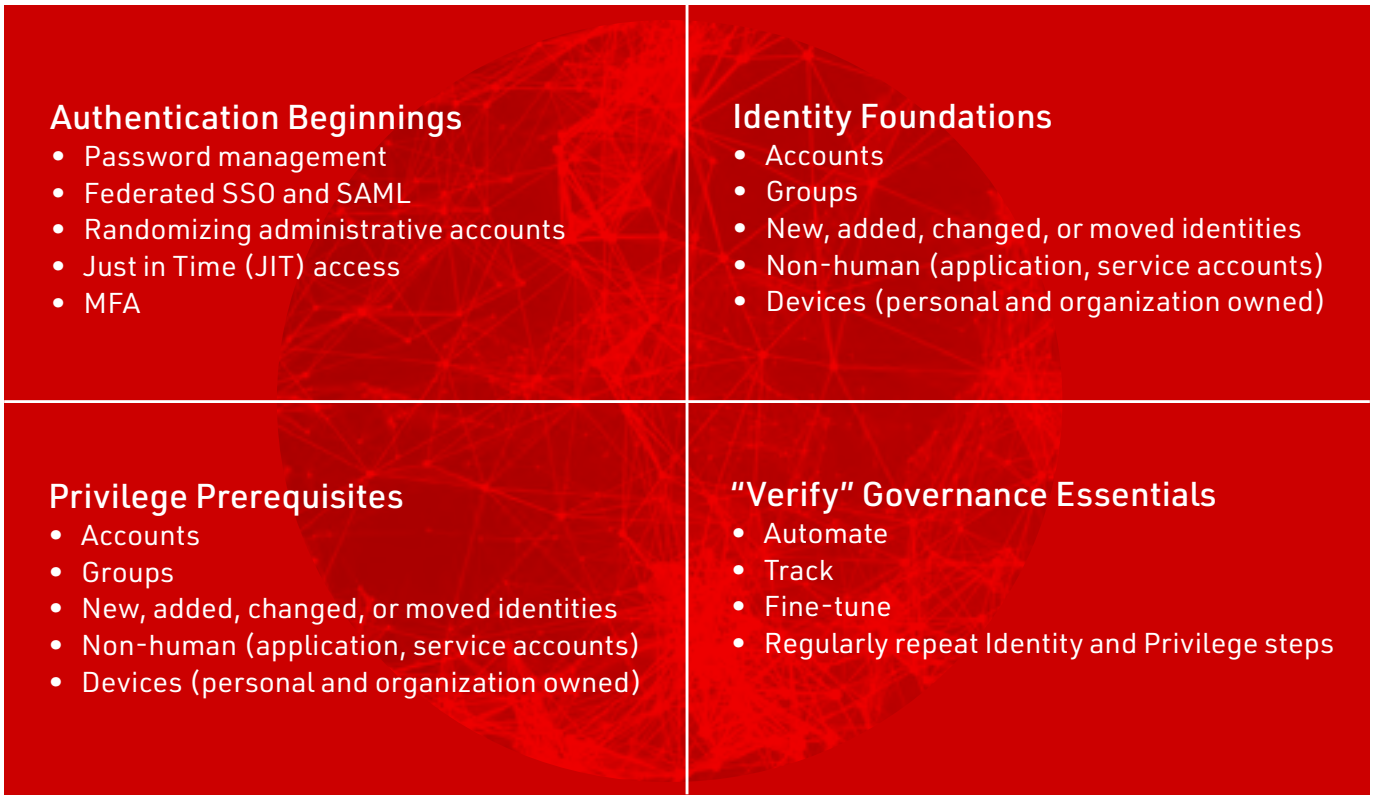
Role catalogue

- Employees, students, parents, volunteers, research subjects, camp attendees, and the internal owners of these roles

Inventory audit

- Identities, groups, applications, integrations, and servers

By determining the foundation of what's in your network, you can then choose the next steps in selecting and sequencing your access management digital transformation, including:



Identify Your Quick Wins

By focusing on authentication first, your organization can "start small" with viable and high-yielding ROI projects utilizing components like password management, federated SSO and SAML, randomizing administrative accounts, just in time (JIT) access, and MFA.

These authentication and privilege steps will close significant cybersecurity gaps in your network. Moreover, this work can help you overcome a common roadblock institutions often face in gaining decision-maker support. Many leaders need a path that resonates with them before they will greenlight a digital transformation project.

Higher Education Access Management Vendor Checklist

For many colleges and universities, identity access management and identity governance solutions have historically been out of reach due to cost. But that is changing. Today, many cutting-edge access management platforms are easy to install and implement while remaining affordable.

To find the right vendor for your identity access management and identity governance deployment with valuable, relevant experience, you'll need to ask the right questions and examine the solution through the lens of higher education, asking such questions as:

1. Deployment

- ✓ How is identity access management and identity governance deployed?
- ✓ Does it work on-premises, in the cloud, or physical or virtual environments (hybrid)?

2. Total cost of ownership and efficiency

- ✓ Does it result in cost and time savings by replacing manual processes with automation, allowing you to retask resources for more strategic initiatives?
- ✓ What are your direct and indirect costs to support the solution over its lifetime in the higher education vertical?

3. Time-to-value

- ✓ How soon will the implementation improve your cybersecurity and decrease your attack surface and risk?
- ✓ How soon will you realize a positive institutional impact (providing a seamless and efficient experience for end-users, streamlining processes, enabling your organization to embrace new technologies and initiatives)?
- ✓ How long will it take to achieve your end-game goals with the solution?

4. Scalability

- ✓ Does the solution scale both vertically as well as horizontally to meet your needs now and in the future?
- ✓ As you uncover new threats or your roadmap evolves, can you turn the platform's services on or off as needed without installing other products?

5. Integrations

- ✓ How does it integrate with the rest of your security ecosystem (SIEM, service desk, analytics, e-mail)?
- ✓ Does your solution synergize with your current security processes and frameworks and maximize your existing implementations and applications?

6. Longevity

- ✓ Will the solution vendor advance with you and grow your access management and cybersecurity program?
- ✓ Are the vendor and platform resource-ready and feature-rich to meet the access management use cases of tomorrow?

7. Higher Education Requirements

- ✓ Will you need expensive customization and time-consuming service level agreements to make the solution work for higher education use cases?
- ✓ Does the vendor have higher education references you can contact?
- ✓ Does the solution simplify your vendor and program deployment, streamline service agreements, and lower overall cost?

By gathering answers to these questions, you will have the foundational requirements and understandings needed to inform your partner selection process. But, these questions are only the beginning.

Further Vendor Resources

Dive deeper into your search for the right identity and privileged access management and governance vendor with this Ten Step Process of Selecting a Technology Vendor to Update Your Solution from Identity Works.

Higher Education Community Vendor Assessment Toolkit (HECVAT) from the Higher Education Information Security Council (HEISC) is a questionnaire framework specifically designed for institutions to measure vendor risk. It is becoming a standard in higher education. Before your organization purchases a third-party solution, ask the vendor to complete a HECVAT assessment to confirm information, data, and cybersecurity policies exist to safeguard your critical institutional and user information.

Why Finding the Right Partner Matters

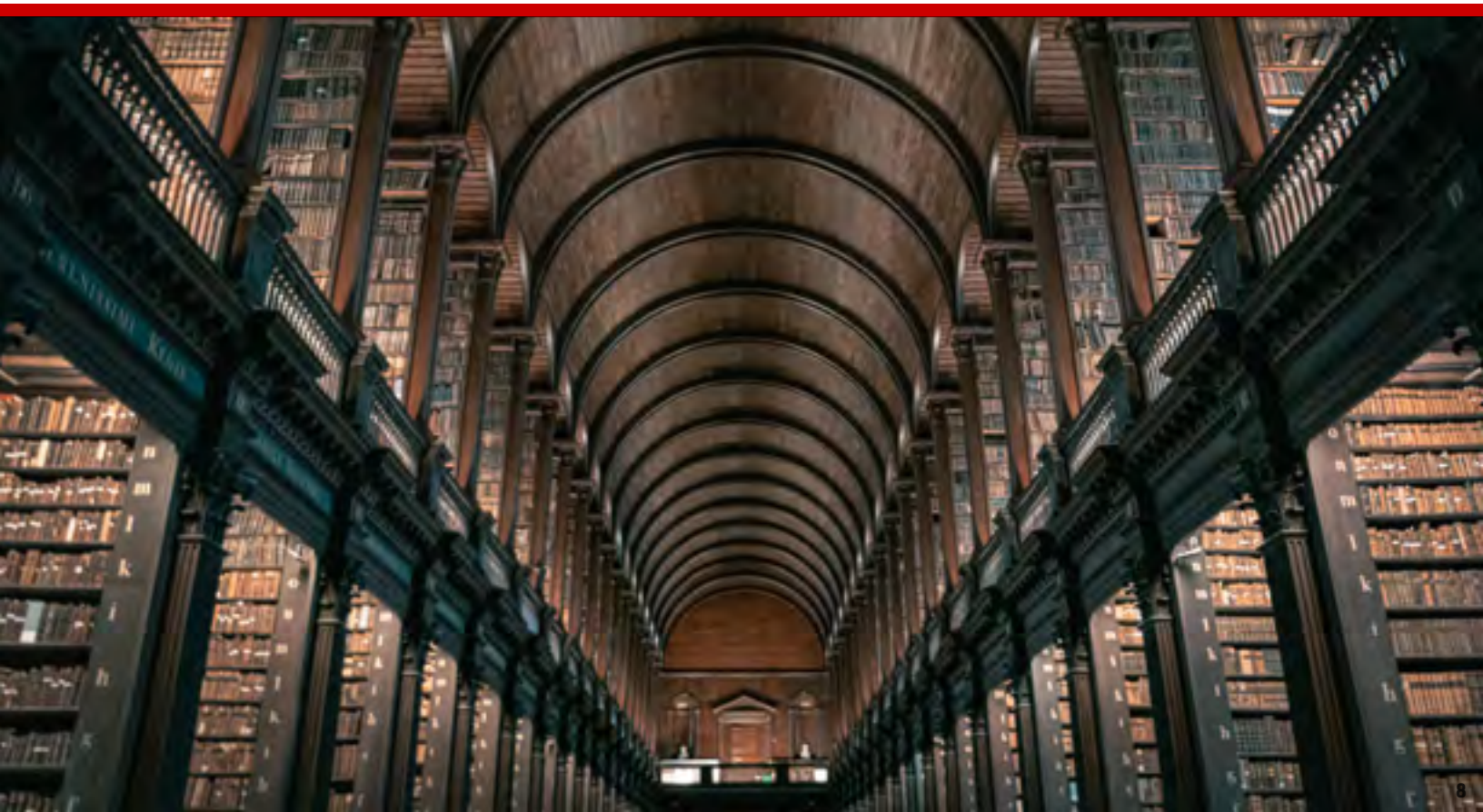
To successfully modernize your access management efforts (including identity access management and privileged access management), you need a vendor that has fully embraced the higher education paradigm with deep knowledge of the unique challenges higher education faces paired with higher ed deployment experience. And a partner that also offers a platform designed to tackle these problems without pricey custom code injections or specialized service contracts.

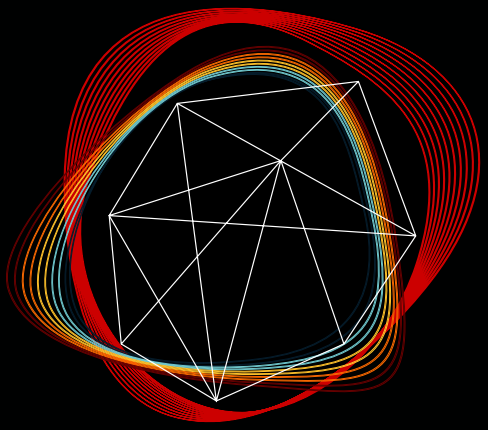
Here's why: Suppose a college or university starts with an enterprise access management system fashioned by a software vendor unfamiliar with the special needs of the higher education vertical. It can be a very costly deployment as change control orders continue to drive up the implementation costs.

Because the access management system doesn't address all of the institution's identity and privileged challenges, the vendor must implement time-consuming customizations and clumsy workarounds attempting to make the solution just "work." In many cases, it's like fitting a square peg into a round hole.

The path to addressing your institution's needs is filled with half measures and many problems simply unanswered. A vendor familiar with the space may have taken such requirements into the original build of the software keeping such extraneous costs to a minimum.

It is essential to find the right partner.





POWER OF ONE

Ready-Made for Higher Education

The ever-growing importance of access management and digital transformation means that vendor selection is a critical decision. With budgetary constraints and a significant focus on ROI, your access management platform should be ready for higher education. There's little room for time-consuming customization or expensive specialized service.

The Power of One: Hitachi ID Bravura Security Fabric

The Hitachi ID Bravura Security Fabric solves the latest, evolving access management challenges for today's colleges and universities and is the industry's only single platform for multi-factor, adaptive authentication, identity access management, and privileged access management.

Unlike many of today's commercial access management solutions, it's designed for higher education-specific challenges out of the box without expensive customization. It's also platform-agnostic, integrating various cloud, platform, and security systems with ease while conquering the complicated network of higher education populations. Additionally, it automates the complex life cycle management of large, dynamic, and unusual user bases -- all without custom code injections or additional staff.

The Hitachi ID Bravura Security Fabric meets all of your access management, digital transformation, and cybersecurity needs with the leading-edge features and applications colleges and universities require to remain competitive and thrive in the modern digital landscape. It's packed with future-ready technological and architectural building blocks enhanced by decades of reliability to protect, manage, and govern your entire identity and access infrastructure for the next generation. All of this scalable capability comes bundled with Hitachi ID's global support.

BONUS: Hitachi ID Bravura Security Fabric integrates with the latest security tools, including the Internet of Things (IoT), Operational Technology (OT), Information Technology Service Management (ITSM), and Security Information and Event Management (SIEM).

Next Steps

Gain access to a universal set of standards to assess a program's risk in Educause and GreyCastle's Security Vendor Assessment Program. Fill out this form to get started.

The program leverages your existing HECVAT questionnaire and other modalities to empower your higher education institution to streamline its purchasing process and vendor onboarding.

ASSESS your security risks now. Fill out this form to get started.

LEARN MORE about how Hitachi ID helps universities and colleges master their identity access management and governance solutions. Visit Now

We Are Hitachi ID

As a recognized market leader, we deliver access governance and identity administration solutions to organizations globally, including many Fortune 500 companies. By leveraging decades of experience, we provide the industry's only single platform identity and privileged access solution to simplify implementation as your IAM and PAM roadmaps evolve.

Hitachi ID Systems, Inc.

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
hitachi-id.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@Hitachi-ID.com