2017 Trends and Technologies: Security, Identity, Privacy, and GRC
Introduction

Since 2014, EDUCAUSE has examined higher education’s top strategic technology priorities. This year, in addition to reviewing the overall list of strategic technologies, EDUCAUSE will publish nine separate reports examining in detail the technology domains we asked about and reviewing each domain’s component technologies and the trends associated with those technologies. This report covers the 20 technologies and 9 trends included in the security, identity, privacy, and GRC (governance, risk, and compliance) domain.

For the second year in a row, information security tops the EDUCAUSE Top 10 IT Issues list. Information security is an evergreen topic on the list because higher education leaders are becoming more aware of the risks that arise when evolving technologies, business practices, and user expectations collide in a way that doesn’t protect the resources and data that institutions are entrusted to protect. Ensuring that institutions adopt a layered and constantly adapting approach to reducing information security risk is key.

The deployment of appropriate technologies is an important piece of the calculus of risk reduction, especially where such deployments focus on reducing institutional information security risk so that the institution can effectively and efficiently meet its underlying missions to educate students, conduct research, and provide outreach to its communities. Deployment of security, identity, privacy, and GRC technologies also helps stretch the limited resources of today’s higher education information security departments, where only 3% of central IT spending is devoted to information security and there are only two central IT information security FTEs per 10,000 institutional FTEs.

The focus of this report is the trends and strategic technologies associated with security, identity, privacy, and GRC. Mature, commonly deployed technologies (such as financial information systems or networks) may be among the most mission-critical technologies, but they are generally more likely to receive operational rather than strategic attention. Strategic technologies, by contrast, are the relatively new technologies institutions will be spending the most time implementing, planning for, and tracking in 2017. None of the 20 security, identity, privacy, and GRC technologies analyzed in this research is currently in place in more than 30% of institutions.

Technologies are what IT organizations do. Trends, on the other hand, are widespread external factors that influence institutional and IT strategy and often spur the adoption of technologies. This report examines the trends that institutions are paying the most attention to and that are influencing emerging institutional IT strategy the most. This year’s trend list included 9 items closely associated with security, identity, privacy, and GRC.
Covered in This Report

Trends

- Campus safety
- Changing vendor-institution relationships (bypassing IT to work directly with business-area leaders)
- Changing vendor-institution relationships (moving from a transactional to a strategic relationship)
- Compliance environment
- Continued complexity of security threats
- Incorporating risk management approaches into IT strategy and service delivery
- Increasing complexity of technology, architecture, and data
- Institutional international strategies (international campuses and partnerships, internationalization of student body, etc.)
- Platform-agnostic vulnerabilities

Technologies

- Applications of analytics to security
- Cloud access security broker (CASB)
- Cloud-based identity services
- Cloud-based security services
- Content-aware DLP
- Cryptocurrencies
- Database encryption*
- DDoS prevention products and services
- DNSSEC
- E-signature technologies
- End-to-end e-mail encryption
- Enterprise GRC systems
- Federated identity technologies
- IT risk management automation
- Life-cycle contract management
- Mobile device management*
- Next-generation firewalls
- Privacy-enhancing technologies
- Private-cloud computing
- SIEM (context-aware security)

*Part of the overall 2017 Top 10 Strategic Technologies
Findings and Recommendations

What do we know about the kind of progress higher education might make with security, identity, privacy, and GRC technologies? What trends might influence this progress? While our data can never be a substitute for an institution’s own information security strategic plan or roadmap, this report can inform an institution’s overall IT strategy and information security technology-deployment strategy.

The Trends

We characterized a trend as “influential” if it was already incorporated into IT strategy or exerting a major influence over emerging IT strategy. We used that characterization to classify the trends into four levels of influence, based on the prevalence of influence across institutions:

- **Most influential:** Trends that are influential in 61% or more of institutions
- **Taking hold:** Influential in 41–60% of institutions
- **Worth understanding:** Influential in 21–40% of institutions
- **Limited impact:** Influential in 20% or less of institutions

Understand how the most influential trends are affecting your institution.

One trend is influential at 61% or more of colleges and universities:

- *Continued complexity of security threats.* The security threat landscape is increasingly complex, with cloud applications, the Internet of Things, complex technology architectures, and sophisticated emerging threats requiring a flexible and layered institutional information security approach. Finding new tools and technologies to help identify and mitigate these threats is of great importance to IT professionals.

Review the trends that are taking hold and address them at your institution.

Four trends are influential at 41–60% of institutions (listed below from highest to lowest level of influence):

- *Increasing complexity of technology, architecture, and data.* The pace of change in technology continues to increase. As institutions try to keep up, they are finding that the environments they manage are becoming more and more complex. New technologies need to be incorporated into the environment, older technologies need to be updated, and end users expect it all to work seamlessly. As the IT environment grows, IT complexity grows exponentially.
Compliance environment. The regulatory environment impacting higher education IT systems and the data contained in those systems can seem labyrinthine. Data elements in many IT systems may be protected by a number of different federal, state, and local laws and industry regulations. The complicated regulatory environment can be difficult to understand, making it even harder to secure IT systems in a compliant manner.

Campus safety. The safety and security of campus students, faculty, staff, and visitors is a priority for higher education institutions. Institutions regularly evaluate their campus operations to strengthen and improve them in order to provide a safe, secure, and welcoming environment. Similarly, the security of campus resources, including IT resources and data, is a concern. Institutions must regularly review and improve their IT operations to ensure the security of their most important IT system and data resources.

Incorporating risk management approaches into IT strategy and service delivery. The term “risk management” refers to a detailed, thoughtful process whereby an institution identifies and assesses the risks that could keep it from meeting its goals and then creates a plan for prioritizing and addressing those risks. It is a mechanism for managing uncertainty. As IT strategy and service delivery models evolve beyond traditional offerings, addressing IT risk more strategically involves focusing on information technology’s impact on the achievement of institutional goals rather than on the simple identification of risks related to physical inventories of assets in isolation.

Understand these trends, and consider their possible role at your institution.

The influence of two trends is limited to 21–40% of institutions. Higher education is monitoring these trends (listed below from highest to lowest level of influence) with respect to emerging IT strategy and the deployment of information security strategic technologies:

Changing vendor-institution relationships (moving from a transactional to a strategic relationship). Next-generation enterprise IT is characterized by a shift in IT’s role from being a technology provider to a service broker and partner. This shift allows for a different level of conversation between institution and vendor, as IT can broker a strategic conversation between the two, bringing technology investments into closer alignment with the institutional mission in the process. In the broker role, IT can ensure that conversations about information security and privacy take place.
Changing vendor-institution relationships (bypassing IT to work directly with business-area leaders). As cloud-based services become increasingly common, individual departments have begun to negotiate directly with vendors and bypass IT departments to select and purchase technology-related services. This practice makes it difficult for IT staff to maintain standards for architecture and integration, and it complicates concerns for information security, compliance, privacy, data management, and data governance. IT departments are responding in part by developing expertise in relationship-management skills, allowing them to communicate better with both campus stakeholders and the vendor community.

The remaining two trends were of limited impact in our research: institutional international strategies (international campuses and partnerships, internationalization of student body, etc.) and platform-agnostic vulnerabilities.

The Technologies

The list of strategic technologies included in our survey was derived from the 2016 list and from several authoritative sources that annually identify emerging and maturing technologies in higher education.\(^5\) A total of 20 of the technologies in the survey pertain to security, identity, privacy, and GRC. For each of those technologies, respondents selected one of six response options to indicate the level of activity for that technology at their institution in 2017:

- **Institution-wide deployment**: Full production-quality technical capability is in place, including ongoing maintenance, funding, etc., with deployment potentially supporting institution-wide access.

- **Expanding deployment**: In 2017, we will move from initial or partial to broader or even institution-wide deployment.

- **Planning, piloting, initial deployment**: This technology is not yet available to users; however, meaningful planning for deployment is either in development or in place. Staff are investing significant time (multiple person-weeks of effort) and resources in executing the plan to pilot or deploy this technology within a defined time frame.

- **Tracking**: Multiple person-days of effort will be assigned but restricted to monitoring and understanding this technology (much more than just reading articles).

- **No deployment**: None of this technology is in place, and no work will be under way or resources committed for this technology in 2017.

- **Don’t know**: I don’t know what this technology is.
We assigned attention scores to the responses, and the scores were weighted to highlight responses indicative of higher levels of activity (expanding deployment; planning, piloting, initial deployment; and tracking) over responses that suggest little or no activity of that kind (institution-wide deployment, no deployment, and don’t know).

Understanding what peer institutions (both current and aspirational) are doing can help you gauge whether your institution’s current approach is on track or might warrant reconsideration. Some technologies are more relevant for some types of institutions than others. We looked at broad demographic categories, including Carnegie class, institutional size, and approach to technology adoption, and found differences in attention score based on those factors. In figure 1, the U.S. mean is the average attention score for an item from all U.S. respondents. The minimums and maximums are the lowest and highest average attention scores among all groups within the categories of Carnegie class, institution size, and timing of technology adoption, with labels indicating which group or groups returned that score. In the event of a tie, all tied groups are represented.
Figure 1. Attention score averages and differences
Looking beyond attention scores, we sought to understand the kind of effort that the largest proportion of institutions is devoting to each technology. We created four attention categories by combining adjacent responses:

- Expanding deployment and institution-wide deployment, combined as **deploy and maintain**
- Planning, piloting, initial deployment and expanding deployment, combined as **pilot and deploy**
- Tracking and planning, piloting, initial deployment, combined as **decide and plan**
- No deployment and tracking, combined as **track and learn**

Although nearly every technology was represented to some degree in each attention category, we assigned each technology to the attention category with the greatest amount of institutional activity for that technology in 2017.

**Complete initial deployment and maintain these technologies.**

Our research shows that although many institutions are expanding deployment or already have some strategic security technologies in place, the bulk of the activity in 2017 will be at other levels. As a result, no technology was assigned to the **deploy and maintain** attention category.

**Pilot and start deploying these technologies.**

Similarly, no technology was assigned to the **pilot and deploy** attention category because larger proportions of institutions are devoting a different kind of attention this year.

**Decide when these technologies fit your strategy, and start planning.**

Institutions are carefully watching these two information security strategic technologies (listed below from highest to lowest attention score), **deciding and planning** for potential future deployment score:

- **Mobile device management.** Mobile device management is the approach an institution takes toward the policies, support, and procedures related to the variety of cell phones, tablets, and laptops on campus. Mobile device management involves a balance between the security of institutional data and the convenience and productivity of users. Some institutions use third-party products and services to manage mobile devices. Considerations include data security issues, support for personally owned equipment, and application management.
Federated identity technologies. These technologies and standards are used to share identity information between organizations (or across security domains).

Learn about and track these technologies.
Institutions are tracking and learning about the following information security strategic technologies (listed below from highest to lowest attention score):

- **Database encryption.** Database encryption is the process of encrypting data within a database so that the data are rendered unreadable without the decryption key. Often suggested as a way to protect sensitive data, database encryption can be costly and requires more storage space than a nonencrypted database.

- **DDoS prevention products and services.** Various products and services can be used to protect institutions from a distributed denial of service (DDoS) attack. A DDoS attack uses multiple systems to target a single IT system, swamping that system and preventing authorized users from accessing it.

- **Next-generation firewalls.** These firewalls incorporate application-level inspection, intrusion prevention, and intelligence from outside the firewall. They differ from stand-alone network intrusion prevention systems.

- **Private-cloud computing.** Private-cloud computing refers to cloud infrastructure operating for a single institution and closed to other use. Institutions have for some time used virtualization technologies to run parts of the environment on private-cloud virtualized platforms.

- **E-signature technologies.** A broad category, this includes technologies that allow you to electronically sign documents in order to authenticate, or prove, the identity of the signer.

- **Cloud-based security services.** These services are usually used in conjunction with on-premise services and tools to enhance an institution’s information security posture.

- **Cloud-based identity services.** Cloud-based identity services manage identification and authentication processes for IT systems or data. Authentication services ensure that only authorized individuals (or systems) are permitted to access IT systems and data.

- **End-to-end e-mail encryption.** This type of communication encrypts e-mail from the sender to receiver as it travels across communications networks.
- **IT risk management automation.** These integrated IT applications help automate risk assessment activities and track risk mitigation activities. They may also contain automated scanning tools to identify possible risk situations (e.g., usually the failure of a security control or baseline).

- **Content-aware DLP.** Content-aware data loss prevention (DLP) tools enable the dynamic application of security policy based on the content and the context of data. These tools identify sensitive data elements to protect those elements.

- **SIEM (context-aware security).** Security information and event management (SIEM) tools are used to gather security log data across multiple IT systems and present the data via a single interface for action.

- **Life-cycle contract management.** Life-cycle contract management refers to a formal process or system for managing contracts from the time of negotiation, through compliance, to renewal. Life-cycle contract management systems have the potential to create efficiencies and lead to cost savings. They also can increase compliance with regulations and other requirements.

- **Applications of analytics to security.** The application of data-collection and sophisticated analytics within security tools and technologies enables IT organizations to quickly identify and respond to threats to institutional IT systems and data.

- **Cloud access security broker (CASB).** A CASB is a service that applies institutional security policies, such as authentication and authorization rules, to cloud-based resources. A CASB extends institutional information security policies and practices to the cloud-based services that the institution uses.

- **DNSSEC.** Domain name system security extensions (DNSSEC) is a suite of specifications for ensuring the integrity and authenticity of the domain name system (DNS).

- **Privacy-enhancing technologies.** Privacy-enhancing technologies and tools protect a user’s personally identifiable information during online transactions.

- **Enterprise GRC systems.** This refers to integrated IT applications that typically offer “modules” that help automate institutional governance, risk, and compliance processes and reporting, such as managing the policy-development process, tracking legal requirements, monitoring and ensuring that compliance obligations are met, automating risk assessment exercises and tracking mitigation activities, and automating incident or issue tracking.

- **Cryptocurrencies.** Cryptocurrencies are digital currencies that use encryption technologies to control the creation and transfer of the units of currency. Bitcoin is a common example of a cryptocurrency.
Preparing for the Future

Understanding the technologies that are most relevant for your institution and how fast a certain strategic technology may be growing is critical to institutional IT strategy. We estimated the pace of growth based on the percentage of institutions we predict will implement each technology over the next five years (by 2022). Figure 2 positions each technology in one of 12 cells based on institutional intentions (the “recommendation for today”) and the expected pace of growth of that technology. Reflecting what was noted above, the figure shows that most of the technologies we tracked are still being explored—rather than deployed—by most institutions.

<table>
<thead>
<tr>
<th>Deploy and maintain</th>
<th>Pilot and deploy</th>
<th>Decide and plan</th>
<th>Track and learn</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mobile device management</td>
<td>Database encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Federated identity technologies</td>
<td>DDoS prevention products and services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Next-generation firewalls</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Private-cloud computing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E-signature technologies</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cloud-based security services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cloud-based identity services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Content-aware DLP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Life-cycle contract management</td>
</tr>
</tbody>
</table>

---

**Figure 2. Plans for 2017 and pace of growth for information security strategic technologies**
Conclusion

This year’s review of information security strategic technologies shows that institutional intentions to plan for and deploy these types of strategic technologies seem at odds with higher education leaders’ assessment that information security is a top issue in higher education. The reason for this disconnect could be that the technologies discussed in this report are, *by definition*, relatively new and have not yet achieved widespread operational implementation. It is also possible that the limited resources of institutional information security departments simply cannot be spent on technologies that are still maturing. Finally, it could be that institutional implementation of the security strategic technologies is deliberately cautious to ensure an open and transparent approach to information security activities and risk management.8

That said, the fast pace of technology change continues to contribute to the information security, identity, privacy, and compliance risks that higher education institutions are facing today. Indeed, the growing complexity of the security threat landscape is a trend that is exerting a major influence on institutional IT strategy. Understanding how the information security strategic technologies will fit into this complex landscape is critical to reducing institutional risk exposure. Deploying security, identity, privacy, and GRC strategic technologies to address these risks must be one part of a multilayered approach that includes sound governance and strategy, operational practices, and training for members of the institutional community.
Notes


2. See the 2016 EDUCAUSE Core Data Service Almanacs at the CDS Publications page.

3. Our rationale for including the security, identity, privacy, and GRC technologies in one domain is that EDUCAUSE Core Data Service research shows that central IT information security departments tend to have responsibility for identity management, privacy, and GRC practices in most U.S. higher education institutions. These technologies are referred to collectively as “information security technologies” in this report.

4. EDUCAUSE tracks these types of established technologies in the Core Data Service because they are widespread enough to enable institution-level benchmarking.

5. Primary sources were The Horizon Report, Gartner’s Top 10 Strategic Technology Trends for 2014, and multiple 2014 Gartner Hype Cycles (education, big data, cloud computing, cloud security, enterprise architecture, enterprise information management, GRC, identity and access management, IT operations management, privacy, business intelligence and analytics, and emerging technologies). We augmented those with several additional technologies, most notably in analytics.

6. DNSSEC was on the list of technologies with which institutions were unfamiliar in both 2017 (31%) and 2016 (23%). See Susan Grajek, Higher Education’s Top 10 Strategic Technologies for 2017, research report (Louisville, CO: ECAR, February 2017); and Susan Grajek, Higher Education’s Top 10 Strategic Technologies for 2016, research report (Louisville, CO: ECAR, January 2016).

7. Note that almost two-fifths of respondents to our survey were unfamiliar with enterprise GRC systems. See Grajek, Higher Education’s Top 10 Strategic Technologies for 2017.

8. Higher education institutions often seek to strike an appropriate balance between IT risk control and functionality/openness in order to reflect the unique freedoms expected in academia. EDUCAUSE research into the state of IT GRC programs in higher education shows that most institutions seek to achieve this balance through a slight preference for functionality and openness. See Jacqueline Bichsel and Patrick Feehan, Getting Your Ducks in a Row: IT Governance, Risk, and Compliance Programs in Higher Education, research report (Louisville, CO: ECAR, June 2014).