

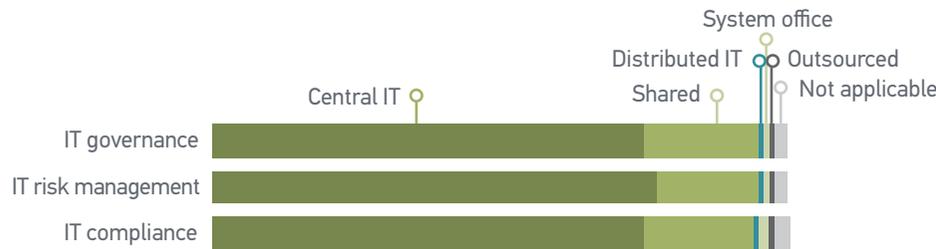
Institutional investment in IT and reliance on information systems have grown. So, too, has the need for reliable structures and measures to ensure IT success and minimize failure. IT governance, risk, and compliance

(GRC) programs develop a framework for the leadership, organization, and operation of an institution's IT programs. GRC concepts are found throughout the EDUCAUSE Top 10 IT Issues lists. From optimizing the use of educational technology to managing

institutional data and ensuring appropriate IT organizational development, IT GRC programs are an institutional need.

Organizational unit responsible for IT functions

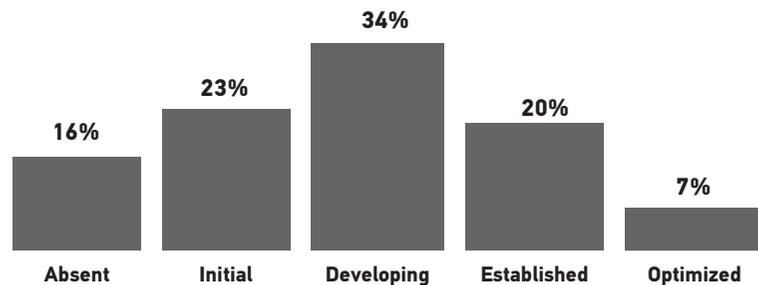
At most institutions, central IT units are primarily responsible for IT GRC activities.



What is IT governance?

IT governance consists of decision-making processes that ensure the effective and efficient use of IT in enabling an institution to achieve its strategic objectives. The maturity of IT governance at individual institutions varies by a roughly bell-shaped distribution. Most institutions have formal IT governance programs in place. However, only 7% of institutions demonstrated the across-the-board strength to qualify as optimized, with all governance capability components in place, sustainable, adaptable, and scalable. About 16% of institutions rated their IT governance capability as absent, meaning that if they address IT governance at all, it is in an improvised, irregular way.

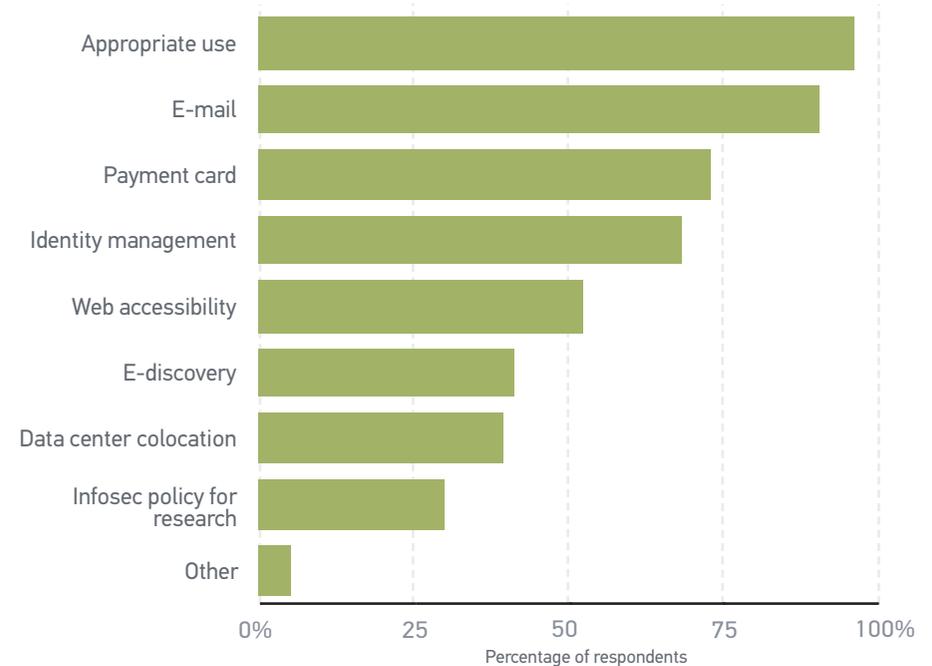
IT governance maturity



What is IT compliance?

IT compliance means operating institutional IT systems and resources in a way that meets the laws and regulations affecting those systems. It also means complying with institutional policy about the use of institutional IT systems and resources, as well as the contracts relating to those systems and resources.

IT policies in place



Information for this Spotlight was derived from the CDS 2015 module on IT Organization, Staffing, and Financing. Only U.S. institutions with a designated Carnegie class of AA, BA, MA, or DR were analyzed for this bulletin.

ORGANIZATIONAL CAPACITY TO PROVIDE RISK MANAGEMENT

Organizational Capacity to Address IT Risk

IT risk is a business risk. Specifically, it's the business risk associated with the use, ownership, operation, involvement, influence, and adoption of institutional IT systems. As institutions increasingly rely on IT systems, the risk grows, forcing institutions to consider IT risk from a strategic perspective, which ensures that the use of IT contributes to institutional goals.

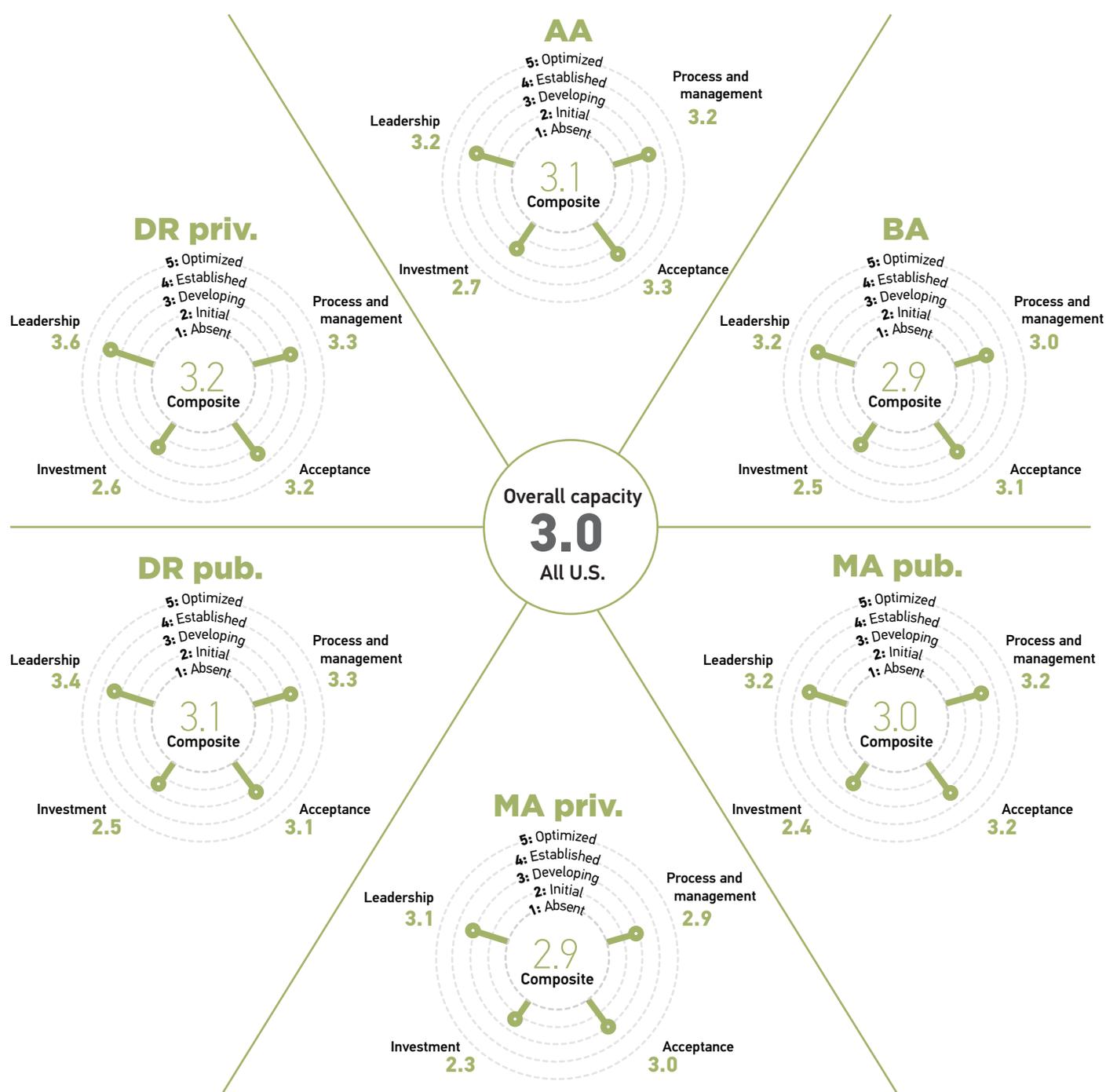
Since 2002, the EDUCAUSE Core Data Service (CDS) has been providing higher education CIOs and senior IT leaders with the benchmarks they need to make strategic decisions about IT at their institutions. In 2014, CDS was enhanced to help institutions understand their maturity in delivering IT risk management programs. Understanding this maturity will help institutions evaluate and improve their IT risk management practices.

RISK MANAGEMENT PROGRAM MATURITY IS ASSESSED IN FOUR KEY AREAS:

- **Process and Management:** Understanding how the institution engages in IT risk management processes and identifies, prioritizes, responds to, and communicates about IT risk
- **Acceptance:** Understanding how the institutional community responds to IT risk management activities and the implementation of IT controls
- **Investment:** Understanding how the institution supports IT risk management activities through staffing and financial backing
- **Leadership:** Understanding how institutional leadership supports IT risk management activities

RISK MANAGEMENT PROGRAM MATURITY IS SUMMARIZED BY THE FOLLOWING SCALE:

- 1: Absent:** Capability components are largely not achieved. Little to no planning is under way.
- 2: Initial:** Capability components exist either latently or slightly. Early planning and discussions may be under way.
- 3: Developing:** High-priority capability components may be largely or fully achieved, while other components are still maturing. Active planning and strategic attention are under way.
- 4: Established:** Capability components have been developed but may not yet be incorporated into institutional culture and practices. Efforts to improve sustainability or scalability are under way.
- 5: Optimized:** Capability components have been developed with an eye toward sustainability, adaptability, and scalability. Components are fully integrated into institutional practices and culture (and may be influencing both).



See Also

- Leah Lang, "2015 CDS Benchmarking Report," March 2016.
- EDUCAUSE IT GRC Program

About the Authors

Joanna L. Grama is the Director of Cybersecurity and IT GRC Programs at EDUCAUSE.
 Leah Lang is the Director of Analytics Services at EDUCAUSE.

