

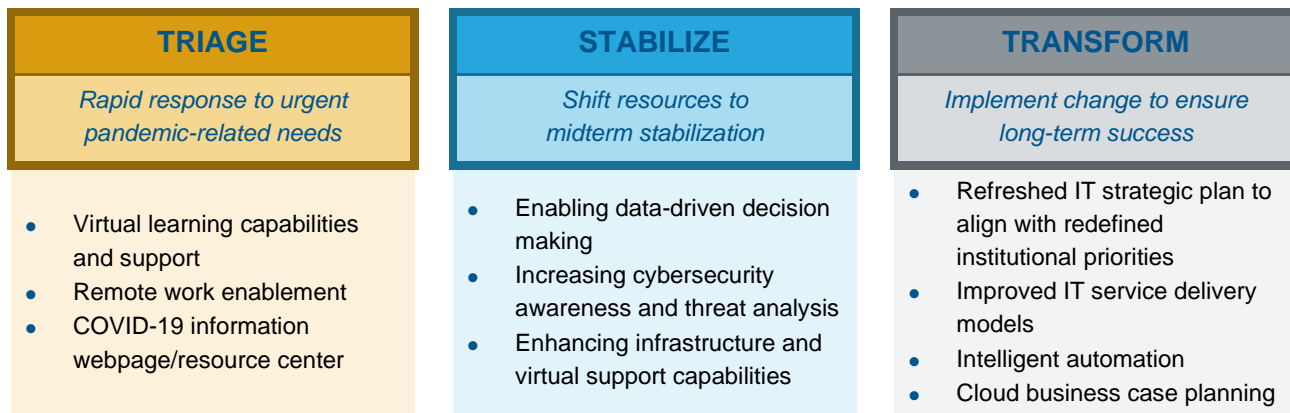
HIGHER EDUCATION COVID-19 RESPONSE: IT LEADERSHIP IN THE MIDST OF COVID-19

As the COVID-19 pandemic creates extraordinary global challenges, leaders across all industries are searching for ways to secure the short- and long-term viability of their organizations. Most chief information officers (CIOs) of colleges, universities and academic health centers have felt even more pressure than usual, bearing the significant responsibility of meeting immediate needs while concurrently supporting their institutions' strategic goals.

Technology leaders who balance their focus across these diverse needs during this difficult period will firmly establish and elevate their value as critical members of their institutional leadership teams. CIOs and their teams have the skills and expertise needed to add tremendous value to their institutions. Whether helping to navigate urgent pandemic-related needs or supporting broad organizational goals, the actions information technology (IT) leaders take in the coming months will continue to cement their status as strategic partners.

In a [recent white paper](#), Huron outlined a three-phase framework for higher education's evolution through this pandemic and impending recession. In this framework, the sector enters first into a triage phase, then transitions to a period of stabilization while it begins to explore opportunities for fundamental transformation.

Information technology and institutional cybersecurity programs can benefit from this model, and there are implications leaders should consider as they navigate each phase.



Triage: Immediate IT Support Needs

IT organizations have had to respond rapidly to institutional efforts to move courses online and support remote staff. The most common actions include the creation of websites that offer a host of services such as online training sessions and tips on how to work remotely, the extension of help desk hours and the negotiation of discounted internet access rates for staff, faculty and students.

More innovative responses include the deployment of chatbots to complement contact centers in addressing the spike in requests for information. These chatbots provide automated responses to common questions and assist in avoiding ambiguity and delayed replies.

Some additional actions that institutions would be wise to consider (if they haven't already) include:

- Judiciously applying bandwidth throttling to ensure access to the most essential users.
- Creating self-service toolkits so employees can quickly set themselves up to work remotely.
- Expanding virtual private network (VPN) access.
- Ensuring adequate software licenses are available for all needed tools.
- Leveraging virtual desktops to give employees and students access to applications on their personal computers.

Stabilize: Aid Decision Making and Reduce Risk

COVID-19 emergency planning has consumed institutional leadership teams across the country. It is imperative that CIOs engage in discussions with other leaders to determine what data and analytics solutions they can provide to assist with the urgent decisions they are making. IT governance and data governance structures should be leveraged to prioritize reporting requirements and ensure consistent data definitions are being used campuswide.

Business intelligence capabilities related to forecasting, visualization and dashboarding should be infused into both finance and enrollment discussions to provide chief financial officers (CFOs) and provosts additional analysis methods. CIOs have an opportunity to be strategic partners with their peer executives in the midst of these trying times by enabling data-driven decision making — a capability that can contribute to the long-term viability of their institutions.

Another key operational imperative that CIOs will need to focus on is cybersecurity. Threat actors will attempt to exploit remote worker vulnerabilities by deploying additional cyberattacks and phishing scams. Malicious websites are already being established with the goal of luring in unsuspecting technology users to spread viruses.

Technology leaders should make every effort to implement both technical and policy-oriented measures to reduce the associated risks. Increased deployments of VPNs, multifactor authentication and data loss prevention technologies can provide users with guardrails that reduce, block and/or detect unwanted intrusions. These investments combined with enhanced cybersecurity training and awareness efforts (that focus on safe online and secure information management practices) can minimize risk in an already volatile time and strengthen institutions' IT infrastructures for the future.

Transform: Refresh Long-Term Strategy and Improve Service Delivery

One of the more essential tasks leadership teams will eventually need to complete entails renewing campuswide strategic planning. These efforts will define new institutional priorities that focus on the long-term optimization of services, the development of new business models and the deployment of innovations across all functions. IT organizations will play a vital role both in implementing their own transformational efforts and in enabling other campus units to realize their strategic goals. CIOs will need to lead efforts to refresh their IT strategic plans so that they fully align with, support and even drive the new institutional priorities that will soon emerge.

IT leaders will also need to focus on initiatives that materially change how services are delivered to and consumed by constituents as the cost, efficiency and efficacy of IT service delivery come under increased scrutiny. By engaging in a thorough review and rationalization of institutional systems and services, IT leaders can start defining an enhanced future state.

Shifting the delivery of commodity IT services (e.g., infrastructure, network, security management, hardware/software procurement) to a more centralized shared services model has the potential to drive significant savings and reduce security risks and vulnerabilities. Institutions can also create a healthy balance of other IT service delivery methods by leveraging on-premise, third-party-hosted, fully outsourced or cloud-based services. These evolved IT service delivery models allow institutions to realize cost savings and avoidance, shift legal or regulatory risks to service providers, and improve service performance, availability and integrity.

Authored by Matt Jones, Merritt Neale and Manoj Krishnan

Access other educational resources on our [COVID-19 resource page](#). For more information, [contact us](#).