SDSU | San Diego State University

Focusing Institutional Capacity on CMS and Cybersecurity Priorities

Bottom line: The university is implementing a temporary pause on major new IT-dependent initiatives so our Division of Information Technology, along with key stakeholders across all the Divisions, can concentrate on mandatory CSU system transitions and cybersecurity risk-reduction work.

Why this matters now

- The CSU Common Management System transition - including the Common Financial System (CFS) and the Common Human Resources System (CHRS) - is mandatory, multi-year, and foundational to payroll, financial operations, HR, and compliance (learn more: https://bfa.sdsu.edu/common-management-system).
- SDSU must also participate in CSU shared-services implementations, including CSUBUY, the Cyber Fusion Center, and a new Benefits Administration model through 2027.
- Following the popularization of AI tools nationwide, the higher education sector in particular has seen a 2000% increase in attempted phishing and fraudulent activity. SDSU is actively implementing a phishing and financial fraud resilience plan to address ongoing and increasingly sophisticated threats.

What is being paused

- Major new software rollouts
- Major system upgrades
- Special projects requiring significant support from IT, Human Resources, or Financial Operations

What can still move forward

Eligible: Legally or regulatorily required initiatives

Eligible: Work directly aligned with the CFS or CHRS transition

Eligible: Efforts essential to cybersecurity, financial integrity, or broader institutional risk mitigation

Pause or Reconsider: All other IT-dependent new initiatives should be deferred and revisited after major milestones are achieved and operations stabilize

Exceptions: Need to be elevated to the divisional VP for review. If supported by the VP, the request will be escalated to the Council of Vice Presidents for a "go" or "no-go" decision.

Leadership takeaways

- This is a sequencing decision, not a retreat from innovation.
- The biggest risks of adding more initiatives now are delay, integration issues, change fatigue, and failed adoption.
- Leaders should set expectations that near-term capacity (over the next 12-18 months) is being reserved for enterprise systems, security, and compliance-critical work.

What message should you share with your team, as a divisional or unit leader? *For the next phase, SDSU is intentionally concentrating institutional capacity on mandatory CMS transitions and cybersecurity priorities. Units should expect tighter prioritization of new IT-dependent work until those core milestones are delivered and stabilized.*