CES Architecture Success Scorecard-6 Score Model

Principles	0	1	2	3	4	5
CES IT Architecture standards require that all new solutions and investments meet a score of 3 or higher for each category	Does not meet standards; significant risks and/or defects identified	Does not meet standards; opportunities missed or broad complications	Areas of concern or improvements identified	Targeted standards for new solutions and investments	Industry leading practice, pattern or solution	Market influencing practice, pattern or solution; influence vendor roadmaps
Strategic Does the IT solution align to the IT strategic imperatives, and BYU's Strategic Plan objectives?	• Solution choices are outside BYU Strategic Plan objectives and IT imperatives • Solution is overlapping and/or substantially duplicative • Undue cost and complexity impact on University, CES or other sacred resources • Stakeholder support and/or long-term sponsorship is unknown, unpredictable, and unmanageable	• BYU Strategic Plan objectives and IT imperatives may have been compromised or disregarded • Solution has missed obvious opportunities to reuse existing capabilities (e.g. shared services) or eliminate duplication • Strategic value and long-term impact is not well-understood • Stakeholder or sponsorship support is inconsistent and vague	• Solution lacks a clear, objective link to one or more BYU Strategic Plan objectives and IT imperatives • Solution design shows lack of effort to reuse existing capabilities (e.g. shared services) or eliminate duplication even if some standards have been followed • Strategic value may be generally agreed upon, but demonstrating or sustaining that value may be difficult • Key stakeholders may be identified, but long-term sponsorship direction is not well-defined	• Initiative has a well-defined link to one or more BYU Strategic Plan Objectives and IT imperatives • No solution overlap on capabilities. • Reuse of existing capabilities (e.g. shared services) has been evaluated and used as much as possible • Key stakeholders and overall sponsorship is well-defined and understood	• Solution has a well-defined link to two or more BYU Strategic Plan objectives and IT imperatives • Solution maximizes the use of existing capabilities (e.g. shared services) and existing technology investments • Significantly reduces cost and complexity at a department/organization level • Demonstrates immediate and long-term strategic value for cross-functional departments and organizations	• Solution has a well-defined link to three or more BYU Strategic Plan objectives and IT imperatives • Solution introduced new strategic capabilities for the entire enterprise (or multiple CES institutions) that leverages both internal and external capabilities • Significantly reduces cost and complexity at an enterprise level (or multiple CES institutions) • Demonstrates substantial, long-term returns in enterprise strategic value • Key stakeholders and long-term sponsorship is well-defined with stakeholders and sponsors actively engaged on future funding, strategic development and success
Secure How secure is the solution and the data it stores, processes, or transmits?	• Solution security, or lack of it, exposes BYU and/or CES to new vulnerabilities, and threats • Solution presents additional risk to any other system it uses or integrates with in the enterprise (i.e. a "shared-fate" system) • Solution may be end-of-life (EOL) making patching either difficult or impossible.	• The network provides the only security available (e.g. ACLs, IDS/IPS, firewalls), leaving the solution vulnerable to anyone who can penetrate the network or higher technology layers • Solution may be end-of-life (EOL) making patching either difficult or impossible.	• Some solution security controls have only been implemented at lower layers (e.g. platform layer) • Application-layer security is rudimentary and is limited to basic access controls • Not all critical functions can be monitored (i.e. logs or events are not available to consume, are inconsistent or absent)	• All critical functions can be monitored (i.e. logs or events are available to consume) • Solution employs defense-in-depth capabilities, enabling proactive detection or prevention at multiple architectural layers (where applicable) • Layers have been tested during development and release (either through vendor attestations, local assessments, or penetration testing)	• All functions and data are grouped by function and/or classification, and can be secured, and monitored at that level. • All layers support comprehensive detection/prevention and application layer security is adaptable and defensible.	• Solution transforms how application and data security are handled at an enterprise level • Solution acts as a model for integrated, rapid security testing in the software development and release lifecycle • Solution provides integrated, comprehensive multi-layer security controls at an enterprise level
Simple Does the solution help simplify our IT portfolios and infrastructure overall?	• Solution choices add a whole new platform to the environment • Dramatically increases complexity and creates undue cost impact to the business.	• Solution is redundant or its complexity forces major changes in other systems • Solution adds significant complexity to the environment	• Solution is complex or redundant with existing technology • Impact has been largely mitigated through limited use or business accepts the impact	• Solution does not add to overall IT complexity • Solution reuses existing, supported technology. • Solution design has been reviewed and pared down, reducing it to essential components and/or services.	• Solution sets new standards through reuse and consolidation • Outright elimination of existing functionality and resources.	• Solution reduces the number of platforms in the environment • Transforms IT through the maximized reuse and rabonalization of internal and external capabilities.
Solid How resilient and responsive is the solution when dealing with faults, interruptions, and failure modes?	• Single points of failure exist in critical areas with no redundancy and mitigation • Impacts would be damaging to the enterprise • Failure conditions are mostly unknown, unpredictable and unmanageable	• Failure potential in the solution has not been fully explored or understood • Business process can tolerate some level of failure • Little to no automated testing, monitoring and alerting	• Solution is partially redundant but has known weaknesses • Business generally accepts the implementation and approach • Impact has been largely mitigated through limited use	• Solution addresses interruptions and failure modes by being redundant • State is synchronized and fully recoverable • Solution is able to remain functional using failure recovery techniques (redundant fail-overs, scaling etc.) • Solution provides proactive health monitoring with relevant, actionable alerts/events or provides standard interfaces for conducting monitoring	• Solution is stateless • Fully redundant or dynamically scaling architecture • Capable of full operational failure recovery • Solution gracefully and automatically degrades on disruption (e.g. circuit breakers, caching, partial responses)	• Solution exhibits zero user-perceived interruptions • Stateless client and proven fault tolerance. • Solution is self-managed, self-reporting, self-optimizing, and self-healing, based on its operating environment
Scalable How well does the solution accommodate growth and respond to fluctuations in demand while maintaining performance?	• Solution is highly sensitive to fluctuations in load and fails to perform in production • Impacts the performance of other integrated or related systems (e.g. "shared-fate" system) • Performance is unpredictable, unreliable and unmanageable • Solution scalability is unpredictable, unreliable and unmanageable	• Solution is unable to maintain performance at loads approaching capacity • Performance is unpredictable due to lack of sufficient monitoring or instrumentation • Solution cannot scale without significant engineering re-work or "after-the-fact" effort • Business cannot accept degradation or finds it critical to business workflow	• Solution is stressed at peak loads, causing a drop in solution performance • Business accepts the degradation or finds it not critical to the business workflow • Solution is scalable, but manual or "after-the-fact" effort is required	• Solution is scalable and is properly sized to accommodate peak loads • Solution performance is documented (i.e. performance can be monitored) and is predictable.	• Solution monitors itself dynamically • Triggers support notifications when the load is near capacity • Solution can be easily scaled on demand	• Solution scales itself dynamically • Any changes in the load on the system are imperceptible or transparent to users and integrating systems
Sustainable What level of effort is required to maintain, modify, or upgrade the solution?	• Solution maintenance requirements are unknown or have not been explored • Solution known to require frequent maintenance windows that impact the business • No documentation exists for the solution	• Routine maintenance requires extraordinary effort or on-site resources • Significant impact on performance or availability. • Documentation is outdated, inconsistent or does not reflect current operational state	• Patches and upgrades require on-site resources or special skills • Most maintenance can be done remotely • Documentation exists but is partially outdated, inconsistent or not sufficiently detailed	• All changes, patches, and upgrades are planned, scheduled and documented • Maintenance can be done with minimal impact on users or integrated systems • Documentation is available, easy to find and sufficiently detailed to allow teams to maintain future state • Needed modifications are in configuration settings rather than code that needs to be updated and maintained over time	• Routine changes and modifications have no perceived impact on users and integrated systems • All solution maintenance can be done remotely.	• Solution exhibits zero user-perceived downtime during any maintenance • Changes, patches, and upgrades completely transparent to the user • Maximizes delivered and shared capabilities to the highest extent possible and significantly reducing the amount of customization over time
Layers	**0**	**1**	**2**	**3**	**4**	**5**
CES IT Architecture standards require that all new solutions and investments meet a score of 3 or higher for each category	Does not meet standards; significant risks and/or defects identified	Does not meet standards; opportunities missed or broad negative impacts	Areas of concern or improvements identified	Targeted standard for new solutions and investments	Industry leading practice, pattern or solution	Market influencing practice, pattern or solution; influence vendor roadmaps
Support & Monitoring How easy is it to monitor the health of the solution (both user interaction and system integration perspectives) and troubleshoot or proactively identify problems?	• Solution requires frequent restarts to fix problems • Negatively impacts the operation and availability of other solutions • Requires local expert resources (e.g. developers, engineers) to troubleshoot all issues. • Reliability and support centers have no ability to monitor health or performance (logs, alerts, monitoring interfaces)	• Only the simplest troubleshooting, diagnostics and maintenance can be performed by support staff • All other maintenance and troubleshooting tasks require on-site, local expert resources. • Problems are difficult to identify and ability to preventing future occurrences not well understood.	• Most troubleshooting and diagnostics can be done remotely • Some complex problems will require local, on-site experts • Reliability and support center teams have some control to monitor health, but limited ability to proactively identify problems (KBs, logging, automated alerting, monitoring interfaces)	• All troubleshooting and diagnostics can be done remotely • Reliability and support centers have sufficient control to monitor ongoing health from user and system perspectives • Reliability and support centers can proactively identify the most common problems (KBs, logging, automated monitoring, monitoring interfaces)	• Solution sets new standards for support and monitoring through automated alerting and proactive monitoring capability • Solution performs self-healing and self-optimizing functions for the most common problems • Solution designed from the start to support reliability and support through robust monitoring, logging and alerting to report on health of system and dependencies	• Solution is self-managed, self-reporting, self-optimizing, and self-healing, based on its operating environment • Requires little, if any, external intervention.
Security How well does the solution meet BYU minimum security requirements, and enable security teams to proactively monitor, respond to, and prevent security events?	• Solution is not capable of meeting minimum security requirements • Provides no support for security teams to monitor and respond to security incidents.	• Solution meets some minimum security requirements • Other controls require significant effort and cost. • Security teams are provided little to no monitoring and incident response or prevention capability.	• Solution meets some minimum security requirements • Other requirements have documented mitigation's in place. • Security teams can monitor some critical functions but not all.	• Solution meets all minimum security requirements or has approved, documented mitigations in place. • Security teams can monitor all critical functions and effectively respond to security events.	• Solution meets all minimum security requirements • Security teams can comprehensively monitor all functions (inc. critical) of the solution with integrated tools and platforms.	• Solution goes beyond or exceeds minimum security requirements • Transforms capability to protect people, process, and technology through a fully integrated workflow to support proactive security monitoring and incident prevention capabilities.
Privacy How well does the solution meet the data privacy requirements of the institution and conform to the sector or state-specific privacy regulations?	• Solution has little to no data privacy controls • Not capable of protecting the privacy of user data • Does not operate in accordance with BYU's Privacy Policy.	• Solution is capable of supporting data privacy, but standards and requirements may have been compromised or disregarded in solution development.	• Solution meets many of the BYU privacy controls and standards • Controls are difficult to test, audit and report on.	• Solution conforms to the BYU privacy standards and legal requirements • Providing adequate capabilities to test, audit and monitor the function of implemented privacy controls.	• Solution meets all data privacy requirements • All controls being testable, auditable and reportable • Provides a reference pattern for future solutions.	• Solution transforms how data privacy is handled • Acts as a model for the development of future systems • Reduces the cost and complexity of maintaining data privacy at an enterprise level.
User Experience Does the solution provide the user a positive experience that minimizes or eliminates the need for training?	• Solution user experience is too complex, confusing or unusable.	• Solution is complex and not self-evident. • Users require significant training.	• Solution requires some training, but the system is not adaptive based on user needs.	• Solution requires some training • System optimizes the user experience based on user need.	• Solution is intuitive and self-evident • Allows a new user to become proficient with only minimal training.	• Solution allows any user to be productive immediately • No training required • System can execute a process on its own without user intervention.
Application How well does the solution incorporate a "cloud-first" strategy by prioritizing purchase of cloud platforms/services OR leverage cloud-native development patterns while working within BYU's approved application stacks?	• Solution is a custom-developed, isolated "point" solution • Does not encourage reuse or leverage investments in cloud-native and approved development stacks. • Missed obvious opportunities to prioritize the purchase of an existing cloud service or application to meet requirements	• Solution is custom-developed, which can be integrated • Missed obvious opportunities to leverage modern cloud-native development patterns (i.e. lift and shift approach) • Creates undue cost and support requirements.	• Application architecture supports standards and development stacks have been followed, but opportunities exist to leverage modern, cloud-native development patterns • Maintains some legacy integrations and custom components.	• Application architecture standards and development stacks have been followed, leveraged and reused • Solution uses modern, cloud-native development patterns, with no solution overlap on current technology • Reuse of existing capability has been evaluated where appropriate. • If applicable, maximized opportunity to purchase an existing cloud service or platform to meet requirements.	• Solution maximizes use of modern cloud-native development patterns • Meets or exceeds application architecture standards • Results in measurable cost savings for the organization • Reduction in support or other resource requirements	• Solution transforms enterprise capability, fully leverages existing capabilities, results in significant cost and support savings • Acts as a model for future, cloud-native, scalable implementation at an enterprise level.
Middleware & Integration How well does the solution integrate with other core systems and leverage existing shared enterprise services?	• Integrations required by the solution need frequent manual intervention by engineers. • Does not integrate well within existing environments • Solution does not use existing shared middleware services • Dramatically increases complexity and creates undue cost impact to the business.	• Integrations required by the solution need manual intervention by the user. • Solution does not use open, non-proprietary standards (data, protocols, interfaces) creating difficulties in interoperation and broader adoption. • Solution missed obvious opportunities to fully leverage existing shared services	• Solution complies with some architectural standards • Creates new integration interfaces that adds support and development complexity	• Solution conforms to BYU standards • Solution uses open, non-proprietary integration standards (data, protocols and network patterns) • Does not create any new integration interfaces for the enterprise.	• Solution improves enterprise integration through simplification • Maximized opportunities to reduce the number of integration interfaces • Net-cost reduction at the project level.	• Solution transforms enterprise integration on a large scale • Simplifies the enterprise integration landscape • Net-cost reduction at an enterprise level.
Data How well does the solution make data accessible and conform to BYU's data architecture standards?	• Solution is incapable of providing efficient data discovery, delivery or integration • Decision making capability thereby causing substantial complexity and undue cost.	• Data made available by the solution is difficult to access • Does not implement a Domain Data Store, OR standard access methods (APIs, events, streams etc.) • Data integration difficult and manually intensive.	• Solution does not have a complete implementation of a Domain Data Store • Solution provides partial implementation of standard access methods (API, events or streams etc.) • Custom data components must be developed to integrate with the solution.	• Solution has a complete implementation of a Domain Data Store • Solution has complete implementation of standard access methods (API, events or streams etc.) • Supports standard integration patterns making it easy for developers to access information.	• Solution improves enterprise connected data delivery and timely decision processing • Simplification of interfaces and net-cost reductions for the campus portfolios.	• Solution transforms enterprise capability for data delivery to connect decisions, understand decisions in context, make timely decisions, and protect information used in making decisions at an enterprise level.
Platform How well does the solution operate within the BYU infrastructure and reuse existing platforms?	• Platform infrastructure is not planned • No history of platform success with the solution (OS, container infrastructure, platform tooling, storage etc.).	• Solution is proven in industry but not at BYU or within CES • At odds with current platform standards, infrastructure, or tooling	• Solution complies with IT platform standards, infrastructure and tooling • Long-term impact to platform infrastructure is not well understood.	• Solution utilizes existing IT platform infrastructure and implementation patterns • Solution is proven in industry and BYU (or CES) • Long-term impact to platform infrastructure is well understood and sustainable.	• Solution uses internal and external platform infrastructure (e.g. cloud services, vendor support) to lower cost and engineering support requirements for BYU (or CES). • Platform implementation pattern maximizes "cloud first' strategy and reduces or eliminates on-premise dependencies.	• Solution uses existing infrastructure at no cost to BYU (or CES) • Creates a net platform infrastructure reduction • Achieves full, long-term platform sustainability.
Network How well does the solution perform on the network and operate within the existing network infrastructure?	• Solution threatens to hamper the operation of users, the network, platform infrastructure, and other applications dependent on the network. • Network dependencies are not understood leading to unpredictable performance and unmanageable requirements	• Solution performance on the network partially satisfies business requirements • Solution cannot tolerate degraded network performance • Significantly impacts the ability for network teams to provide sustained support	• Solution performance on network mostly satisfies business requirements • Solution can tolerate some degraded network performance • Long-term impact to network infrastructure and/or architecture is not well understood. • On-premise datacenter dependencies exist that can impact network performance issues or cascading service failures	• Solution performance completely satisfies business requirements • Long-term impact to the network infrastructure is well-understood, sustainable and adaptable. • On-premise datacenter dependencies have been minimized or eliminated. Existing dependencies are asynchronous.	• Solution adapts to the network performance available • Resilient to degraded network capability and is mostly imperceptible to the user. • Solution eliminates all on-premise dependencies or uses fully asynchronous integrations that are imperceptible to the user	• User perceives instantaneous response everywhere, at any time, even while within an unreliable or unavailable network.