

CTO and CFaO Responsibilities

Exhibit 1. Technology vs Facilities vs Shared Responsibilities

Domain	CTO Core Knowledge and Oversight	Chief Facilities Officer Core Knowledge and Oversight	Shared responsibility (must be jointly governed)
Primary mission	Digital services, cyber risk, academic/admin enablement, user experience	Safe, reliable, compliant operation of the built environment; building and utility uptime	Translate mission into a single, agreed “campus reliability + experience” agenda (students/faculty outcomes and safe operations)
Operating “platform”	Apps, data platforms, networks, identity, cloud	Buildings, central plants, utilities, trades, contractors	Treat buildings as a cyber-physical platform: operational uptime requires secure digital enablement; digital services depend on physical continuity (power/cooling/space)
Signature enterprise systems	ERP/SIS/CRM/HRIS/LMS, IAM/SSO, ITSM, SIEM/SOAR, data lake/warehouse	BMS/BAS, EMS, SCADA (as applicable), CMMS/EAM, metering, lighting controls, fire alarm, access control, video, conveyance systems	Systems integration strategy (APIs, historians, time-series, CMMS-BMS workflows) and “system-of-systems” architecture decisions
OT/BMS scope	Needs working fluency with OT realities and constraints	Owens OT operations and vendor ecosystem	OT governance charter: what counts as OT, what is in scope, and who owns lifecycle decisions across buildings/central plant/campus-wide platforms
Standards bodies (typical)	NIST, ISO/IEC, IETF/IEEE, ITIL/COBIT; privacy regs	ASHRAE, NFPA, ICC, NEC, OEM, and AHJ code interpretations	A unified standards registry: cybersecurity + safety codes + interoperability requirements, aligned to procurement and project delivery
Key OT protocols and integration	Must understand BACnet/IP, Modbus TCP, MQTT, OPC UA (if present), and SNMP patterns and security implications	Deep expertise in BACnet (IP/MS/TP), Modbus (RTU/TCP), LonWorks, KNX, DALI, proprietary buses	Protocol selection guidance, gateway strategy, tagging/metadata conventions, and secure integration patterns (including vendor access methods)
Network vs plant emphasis	LAN/WAN, Wi-Fi, DNS/DHCP, segmentation, firewalls, identity	Central plant operations, HVAC, hydronics, steam/chilled water, boilers/chillers	Network design that respects operational constraints: segmentation, deterministic performance needs, RF realities, and maintenance windows

Domain	CTO Core Knowledge and Oversight	Chief Facilities Officer Core Knowledge and Oversight	Shared responsibility (must be jointly governed)
Wiring and distribution	Low-voltage structured cabling, fiber, PoE, telecom rooms, edge compute	High-voltage distribution, switchgear, generators, ATS, plus control wiring	Power + network interdependence: UPS strategy for OT/edge, generator-backed comm rooms, and outage coordination that protects both IT and life-safety
Cybersecurity	Security policy, monitoring, incident response, third-party risk, and identity	Physical/operational realities; safety-first operations; vendor practices	OT security program (e.g., segmentation, MFA for remote access, logging, vulnerability management) tuned to uptime + safety constraints
Safety and compliance	Data/privacy compliance; cyber policy	Life safety (fire alarm/egress), OSHA/EHS, inspections, code compliance	Joint risk governance for cyber-physical safety: how cybersecurity controls interact with life-safety and emergency procedures
Change cadence	Fast cycles: patches/releases; hardware refresh 3–7 yrs	Slow cycles: assets last decades; controls mid-cycle modernization	Portfolio planning that bridges cadences: align “IT refresh rhythm” with “capital renewal rhythm,” and define when to modernize controls vs. full system replacement
Lifecycle time horizons	Short: software weeks–months; endpoints/servers 3–7 years; cloud contracts 1–3 years	Long: buildings 30–70+ years; major MEP 15–30; controls 10–20; roofs/envelopes 20–40	A shared lifecycle map and funding model: design for “upgradeability” (modular controls, open protocols) while managing long-lived assets and shorter-lived digital layers
Performance metrics	Availability, security posture, user satisfaction, cost-to-serve	IAQ, comfort, EUI, service calls, uptime, asset life, backlog	A single scorecard that links digital + physical KPIs (e.g., IAQ/comfort tied to controls reliability, energy tied to analytics, uptime tied to both OT and network resiliency)
Procurement lens	Licensing/subscriptions, data clauses, security requirements, APIs	Capital projects, service contracts, commissioning specs, and maintainability	Joint procurement standards: security-by-design, interoperability, data ownership, commissioning requirements, and “no black-box” clauses where feasible
Vendor ecosystem	SaaS/cloud/MSPs/telecom/cyber	A/E, GC, MEP, controls contractors, OEMs, commissioning agents, ESCOs	Unified vendor governance: remote access rules, incident notification, data sharing, commissioning acceptance, and performance-based contracting

Domain	CTO Core Knowledge and Oversight	Chief Facilities Officer Core Knowledge and Oversight	Shared responsibility (must be jointly governed)
Workforce and skills	Network/cloud/security/data engineers, architects, service desk	Trades, operators, BAS techs, facilities engineers, planners	Joint training plan: OT cybersecurity basics for facilities; building systems literacy for IT; shared “operator UX” and adoption focus for new platforms
Documentation and sources of truth	CMDB, architecture standards, data dictionaries	As-builts, O&M manuals, sequences, TAB/Cx reports, one-lines, point lists	A harmonized “digital backbone” for documentation: asset registry + system diagrams + point metadata + change history, maintained as part of operations.
Data estate and governance	Data architecture, access controls, retention, analytics, privacy	Point accuracy, sensor calibration, operational context, maintenance history	Shared data governance: naming/tagging standards, data quality SLAs, access policies, privacy boundaries, and ethical transparency for pervasive sensing
Digital twin strategy	Platforms, integration, security, analytics, and user experience	Ground truth, spatial/static accuracy, operational workflows	Joint digital twin roadmap: what problems to solve first, what data is required, how insights become work orders, and how value is measured and sustained
Incident response	Cyber IR playbooks, SOC escalation	Operational response, safety protocols, vendor dispatch	A combined cyber-physical incident playbook: who declares, who isolates networks, how fail-safe modes work, and how to restore operations safely
Common failure modes	Shadow IT, misconfiguration, credential sprawl, vendor lock-in	Controls drift, calibration failure, deferred maintenance, and undocumented changes	Shared controls to prevent drift: change control, commissioning discipline, configuration baselines, and periodic “re-commissioning + security validation” cycles

Note: The shared-responsibility column is the real bridge: it’s where universities either build a coherent smart-campus operating model—or end up with duplicated platforms, unsafe workarounds, and modernization fatigue.