

DOI: https://doi.org/10.48009/4_iis_2026_141

Expanding IS education to cyber-physical cross-sector dual governance: A case of nuclear-power AI data center convergence

Wenli Wang, *Robert Morris University*, wangw@rmu.edu

Keenan Murphy, *Robert Morris University*, murphy.keenan@gmail.com

Abstract

Information systems (IS) security and governance curriculum has traditionally focused more on cyber- than physical security and informational (e.g., finance, accounting, healthcare) than physical sectors (e.g., energy). However, the recent, rapid convergence of two forms of critical infrastructure— nuclear power generation and artificial intelligence (AI) data centers—exposes the limits of this cyber-focus, information-sector framing of traditional IS security and governance education and creates a timely, practical context for emerging cyber-physical cross-sector dual-governance reasoning. This paper presents an instructional-design teaching case to demonstrate how to expand IS security and governance curriculum to incorporate cyber-physical cross-sector dual governance. Drawing on nuclear-power AI data center partnerships and the governance frameworks (NRC/CFR, NERC CIP, ISO/IEC 27001, NIST CSF 2.0, and NIST AI RMF) that apply to their coupled systems, the paper introduces a teaching case on cyber-physical cross-sector dual governance. It includes learning objectives, a target course and level, mappings to the IS2020 model curriculum and ABET cybersecurity criteria, a comparative-framework student activity and assignment, and an assessment rubric. The contribution is pedagogical: the governance-reasoning skills students strengthen through this curriculum and case can transfer beyond the nuclear-power AI data center context.

Keywords: IS education, IT governance, cyber-physical system, nuclear-power plant, cybersecurity, critical infrastructure, AI data center

Introduction

The rise of cloud infrastructure and artificial intelligence (AI) continues to drive rapid growth in the number and scale of AI data centers across the United States. Demand for high-performance server infrastructure grows as more industries and government organizations transition to cloud-based computing for general information technology (IT) and AI applications. Research shows that, given current trends in AI adoption, energy demand from U.S. AI data centers will increase by roughly 160% by 2030 (Goldman Sachs, 2025) and U.S. AI data center electricity demand could nearly triple by 2030 (International Energy Agency, 2026). Meeting that demand is reviving interest in nuclear power as a carbon-free baseload source, and it is producing a distinct new pattern in industrial partnership: major cloud and AI providers pairing data centers directly with nuclear generation.

Traditionally, the IS security and governance curriculum has focused on IS areas itself and extended out only to information-intensive sectors such as finance, accounting, and health informatics. IS departments hence often co-design courses like FinTech, Accounting Information Systems, and Health Informatics with

the related disciplines. The main reason for this extension and co-design is because finance, accounting, and healthcare sectors are information-intensive—their daily business and transactions are embedded in their respective information systems. Their transactions are data and their assets are built upon these data. Consequently, one of their dominant risks are data breaches, fraud, and privacy loss.

These sectors' security and governance tools reflect this information-intensive origin: sector rules such as PCI-DSS and SOX in finance, HIPAA in healthcare, frameworks like NIST Cybersecurity Framework and ISO/IEC 27001, and a dedicated executive role—the Chief Information Security Officer (CISO)—whose mandate is mostly in informational security. Even the recent “stress” tests of COVID-19 pandemic have been information-centric, as it forced a sudden shift to wide-spread remote work, cloud services, and telehealth, straining data governance and access control. Yet it remained mostly a challenge of securing information and the systems that process it. The demand in skilled informational security and governance labor in these sectors in turn influences the IS curriculum on security and governance.

However, the traditional IS curriculum on security and governance is insufficient to cover the emergent needs due to the convergence of nuclear power generation and AI data centers, as traditional IS curriculum covers only briefly physical and operational infrastructure—industrial controls of physical operations, power generation, the grid, and so on.

The construction of nuclear-powered AI data centers concerns not only physical facilities but also their monitoring, control, and audit. It raises a fundamental governance problem—how to govern the coupled operations of nuclear-power plant and AI data centers. When the two are physical adjacent and operationally coupled, a physical, safety-critical facility and an informational, productivity-critical facility become one system, and the system security and governance covers and depends on both.

Yet they come from different domains, with different regulators, security priorities, vocabularies, and tolerances for downtime. Governing them together is harder than the cyber-focused, information-sector governance most IS graduates are trained for. This supply and demand gap—between the cyber-focused, information-sector governance IS labor market currently supplies and the cyber-physical cross-sector dual governance demand in new IS skills that the coupling generates—is what this paper and the teaching case address. This paper makes a pedagogical argument rather than a design-science one. Its thesis is that IS security and governance curriculum should be expanded to incorporate cyber-physical cross-sector dual governance—the coordinated governance of a physical system and an information system fused into a closely-coupled single operation—and that the nuclear-powered AI data center convergence is an example of such emerging context.

Consistent with prior instructional-design contribution in cybersecurity (Wang, 2016), this paper is presented as a teaching case: the motivation, design, objectives, content, activity/assignment, and assessment rubrics are proposed for classroom deployment. The contribution is a reusable teaching case in details with curriculum support: learning objectives, a target course level, mappings to a widely used IS model curriculum and to ABET criteria, a concrete comparative-framework activity/assignment with assessment rubrics. The paper does not propose a new governance architecture, endorse any company's approach, or offer proprietary security recommendations. Instead, it treats the landscape of emerging partnerships and the catalog of relevant governance frameworks as teachable content that students learn to compare, map, and integrate. It is expected that student can further transfer skills learned in other applicable fields.

The remainder of the paper is organized as follows. Section II provides the literature review on case-based and active learning, comparative modular education, and the need of expanding IS security and governance

educations. Section III introduces the background of the nuclear-power AI data center convergence trend and the relevant governance-framework landscape. Section IV describes the teaching case with learning objectives, target course/level, IS2020/ABET mappings, student activity/assignment, and its assessment. Section V discusses contributions and limitations. Section VI concludes.

Literature Review

The teaching-case design rests on established educational research and instructional-design precedent. Three strands are relevant: evidence that students learn reasoning best through cases and active engagement; prior IS-security modules that build learning around comparing structured artifacts and mapping them to accreditation outcomes; and the curricular gap left by cyber-focused, information-sector instruction. The following subsections take each in turn, together establishing both the form the case takes and the need it addresses.

Case-based and Active Learning

The case method has a long history as a vehicle for developing analytical reasoning in context rather than transmitting facts. Herreid (1994) characterized case studies as a means of teaching students to reason with ambiguous, real-world material, and Herreid and Schiller (2013) showed how case methods pair naturally with active, student-centered classroom formats. Broad evidence base supports active over passive instruction: Prince (2004) reviewed the research and found consistent benefits for engagement and retention, and Freeman et al. (2014), in a meta-analysis across science, engineering, and mathematics, found that active learning significantly raised student performance and lowered failure rates relative to lecture. These findings motivate a case built around a student-led, comparative analysis activity rather than a lecture on frameworks.

Comparative, Multi-artifact Modules in IS Security Education

Beyond the general case for active learning, instructional-design work in IS education has demonstrated the value of modules that ask students to compare structured artifacts and map them to objectives and accreditation outcomes. Wang et al. (2016), for example, developed a learning module in which explicit learning objectives, a staged instructional sequence, in-class "teaching tips," and ABET outcome mapping were combined and refined over several semesters. The present case adopts the same instructional-design pattern—objectives, a staged activity, instructor guidance, and accreditation mapping—applied to cyber-security cross-sector governance rather than to a single technical topic.

Expanding Information-sector IS Security and Governance Education

If the case method and comparative modules supply the pedagogical form, the curricular gap supplies the need. IS security and governance curriculum has understandably treated cyber- and physical/operational security and governance mostly as distinct concerns and focused mainly on cyber related issues. As a consequence, the security and governance frameworks students encounter are correspondingly information-centric—e.g., COBIT for IT and accounting-information-system governance—whereas those governing physical and energy infrastructure, such as U.S. Nuclear Regulatory Commission (NRC) regulations and NERC Critical Infrastructure Protection (CIP) standards, rarely appear in the IS curriculum. Curriculum guidance reflects this partition: the IS2020 competency model (ACM/AIS, 2020) and the CSEC2017 body of knowledge (Joint Task Force on Cybersecurity Education, 2018) organize security competencies by domain and treat organizational and societal security as distinct areas, but neither foregrounds reasoning across coupled cyber-physical cross-sector infrastructures. As operational technology, IT, energy, and computing increasingly interconnect, this partition leaves a gap: IS graduates are rarely exercised in comparing frameworks from different sectors especially cyber vs. physical, mapping which rules apply

where, and identifying the overlaps and gaps that coupling creates. The teaching case developed here is designed to fill that specific gap.

Background

What makes the nuclear-power AI data center convergence teachable is that it is real, current, and richly documented in respective sectors. This section develops that content in three parts—the motivating problem of AI's energy demand, a comparative set of real partnerships students can analyze, and the governance frameworks that apply to the coupled system.

Motivating the Teaching Case

A teaching case benefits from a motivating problem that students recognize as real and consequential. The energy demand of AI data center is a present-day practical problem. Strubell et al. (2019) offered one of the earliest analyses of the energy costs of training AI models, showing that training costs scale steeply with parameter count and search complexity. Luccioni et al. (2024) extended this by showing that inference can dominate the total energy footprint of deployed AI systems—often exceeding training energy—with order-of-magnitude variation across tasks.

Utilities have struggled to meet this AI model training and inference demand: the U.S. Energy Information Administration reports record national electricity consumption in 2025, driven substantially by AI and data-center growth (Disavino, 2026). Against this backdrop, nuclear power—long constrained in the U.S.—is experiencing a policy and market resurgence. The 2022 Inflation Reduction Act signaled support for nuclear generation (Clifford, 2022), and the 2024 ADVANCE Act reduced fees that had discouraged new reactor deployment, including small modular reactors (SMRs) (USDoe, 2024). California moved to extend rather than close the Diablo Canyon plant (CPUC, 2026; NRC, 2026a). Students readily recognize the tension: decarbonization goals plus surging AI demand are reopening a technology that had been in decline.

A Comparative Set of Industrial Partnerships

What makes this an especially instructive case is that the convergence spans a set of nuclear-power and AI data center partnerships that students can study comparatively, rather than a single firm (Table 1). Presenting several cases lets students compare structures, ownership models, and regulatory postures.

Table 1. AI data center–nuclear partnerships as a comparative teaching set

Partnership	Structure	Notable governance point
Amazon–Talen Energy (2024)	AWS data-center campus co-located with a nuclear station; direct power supply	FERC rejected an amended behind-the-meter interconnection agreement—an instructive cross-sector regulatory dispute (Power Engineering, 2024; Utility Dive, 2024)
Google–Kairos Power (2024)	Small Modular Reactors (SMRs) supplying up to ~500 MW of 24/7 carbon-free power by 2030; Department of Energy supported	Advanced nuclear positioned as core AI energy strategy (Robb, 2025; Hiller, 2024)
Microsoft–Constellation (Three Mile Island) (2024)	Recommissioning a retired reactor unit under a long-term data-center power agreement	Restart of a shut unit raises licensing and grid-reintegration questions (Mandler, 2024; Kearney, 2025)
Oracle (2024)	Gigawatt-scale data center powered by a trio of SMRs	Move beyond power-purchase agreements toward direct generation (Power Engineering, 2024b)
Meta (2024)	RFP for 1–4 GW of new nuclear (SMRs and larger reactors)	Signals demand-side scale driving new generation (Data Center Dynamics, 2024)

Taken together, these partnerships and endeavors show a repeatable operational pattern—co-locating or directly coupling AI data centers with nuclear generation—pursued by multiple firms under different structures. The two infrastructures also carry different operational modes and tempos; the teaching case uses this tension to motivate why cyber-physical cross-sector security and governance is worth studying.

Governance Framework Landscape

If the partnerships are the situations that students study, the governance frameworks are the rules they must reason with. The core of the teaching case is a set of governance frameworks that apply, in different combinations, to the coupled nuclear-AI system (Table 2). The learning goal is not to memorize each framework but to compare them, map them onto sectors and risks, and reason about where they overlap and where gaps remain. All are widely referenced and widely taught, which makes them appropriate assigned reading. Recognizing what a framework does *not* cover the entire coupled system—for instance, that the NIST AI RMF is software- rather than hardware-oriented, centers on generative AI software (Casamassa et al., 2025) rather than physical facilities, and does not address nuclear or energy-infrastructure risk—is itself a governance-reasoning skill that the teaching case aims to train students.

Table 2. Governance frameworks and their teachable scope

Framework	Sector / domain	Purpose	Key scope limit
NRC / Code of Federal Regulations	Nuclear generation	Safety, physical protection, federally mandated compliance (NRC, 2026b)	Nuclear-specific; silent on data/AI risk
NERC CIP standards	Bulk power / grid	Reliability and security of the electric grid (NERC, 2026)	Grid-focused; distinct from nuclear safety regime
ISO/IEC 27001:2022	Data center (ISMS)	Umbrella information-security management system (ISO, 2022; Amazon, n.d.)	Voluntary; general, not infrastructure-specific
NIST CSF 2.0	Cross-industry cyber	Common vocabulary of security outcomes (NIST, 2024b)	Sector-neutral; not physical/operational safety
NIST AI RMF (GenAI profile)	AI systems	AI-specific and generative-AI risk (NIST, 2024a)	Software- and GenAI-centric; light on energy/physical risk

The pedagogical payoff of assembling these frameworks side-by-side is that students see, concretely, that a single coupled facility may sit at the intersection of all five frameworks—with none covering the whole. The lesson generalizes: cross-sector infrastructure coupling raises governance questions (overlaps, gaps, vocabulary mismatches, coordination needs) that cyber-focus, information-sector training does not surface. In addition, international guidance such as IAEA (International Atomic Energy Agency) safety and security frameworks can be introduced as an optional extension.

The teaching case turns this convergence into a concrete, classroom-ready exercise. Students study a set of real industrial nuclear-power AI data center partnerships, inventory the governance frameworks that apply to each coupled facility, and reason about where those frameworks overlap, conflict, or leave gaps. The aim is not to memorize any single company's arrangement or any one framework, but to practice the transferable skill the convergence demands: comparing, mapping, and integrating governance across two sectors that were not traditionally designed to be governed together. The section that follows grounds the design in instructional-design research and then specifies the learning objectives, curriculum mappings, the student assignment, and its assessment.

Teaching Case

With the content and its pedagogical grounding established, the remaining task is design: turning the material into an in-class activity and a graded assignment. The case is designed as an active-learning, comparative-framework analysis. This section presents its four design components: learning objectives, target course and curriculum mapping, the staged activity with graded assignment, and the assessment rubric.

Learning Objectives

After completing the case, students should be able to meet the objectives in Table 3, which pairs each objective with its Bloom's-taxonomy level and the primary competency it develops.

Table 3. Learning objectives, cognitive level, and competency focus

#	Learning Objectives	Bloom's level	Primary competency
1	Describe the major governance frameworks for coupled critical infrastructure, including each one's sector focus, purpose, and scope limits	Understand	IS security / frameworks
2	Map which frameworks apply to each sector (nuclear, grid, data center) and to specific risk categories within a coupled facility	Apply	IT governance & compliance
3	Analyze overlaps, gaps, and interoperability challenges when frameworks from different sectors must be coordinated	Analyze	Governance reasoning
4	Evaluate and communicate a reasoned governance-coordination recommendation and transfer the reasoning to a novel cross-sector context	Evaluate	Critical thinking & communication

Target Course and Level

The case suits an upper-level undergraduate or introductory graduate course in IS security, IT governance, risk and compliance, or critical-infrastructure/cyber-physical systems security. It assumes basic security concepts (confidentiality, integrity, availability) and familiarity with the idea of a control framework but requires no prior nuclear or energy knowledge—the case supplies that context. It can be delivered in a single three-hour session or expanded into a two-week module.

Curriculum and Accreditation Mapping

The case aligns with the IS2020 competency model (ACM/AIS, 2020)—most directly Information Systems Security and IT Governance and Compliance, and secondarily Ethics, Impacts, and Sustainability plus the cross-cutting competencies of critical thinking and communication. It also aligns with ABET cybersecurity criteria: the Computing Accreditation Commission requires curricula to apply the crosscutting concept of *risk* and to cover Organizational Security and Societal Security (ABET, 2025), which in the CSEC2017 body of knowledge encompass risk management, security governance and policy, compliance, cyber law, and privacy (Joint Task Force on Cybersecurity Education, 2018). The case further advances ABET Student Outcome 6 by having student reason about how coordinated governance sustains operations across coupled infrastructures. Table 4 summarizes the alignment.

Table 4. Alignment of learning objectives with IS2020 and ABET

Objective	IS2020 competency area	ABET cybersecurity element
1 Describe	IS Security	Organizational Security (governance, compliance)
2 Map	IT Governance & Compliance	Risk (crosscutting concept)
3 Analyze	IT Governance & Compliance; Ethics/Impacts	Organizational & Societal Security

4 Evaluate & transfer	Critical thinking & communication (cross-cutting)	Student Outcome 6 (operations under risk)
-----------------------	---	---

Comparative Governance-framework Activity and Assignment

The activity proceeds in three phases:

Phase 1 — Case briefing and framework primer (instructor-led):

the instructor introduces the motivation and the partnership landscape (Table 1) as a comparative set, then briefly introduces each framework (Table 2) using its documentation as assigned pre-reading, emphasizing sector, purpose, and scope limits rather than memorizing controls.

Phase 2 — Framework-mapping group exercise (student-led):

In small groups, students complete a governance-mapping matrix (blank template in Table 5a; a completed sample in Table 5b) whose rows are risk/activity categories for a coupled facility and whose columns are the five frameworks.

Table 5a. Governance-mapping matrix — student assignment template

Risk / activity category	NRC/CFR	NERC CIP	ISO 27001	NIST CSF 2.0	NIST AI RMF
Physical protection (plant + center)					
Grid reliability					
Data confidentiality					
Data-center availability / continuity					
AI-model and data risk					
Cross-sector incident coordination					

(Students complete the matrix: for each cell, mark *Applies*, *Partial*, or *Does not apply*, and cite the basis.)

Table 5b. Governance-mapping matrix — sample student submission

Risk / activity category	NRC/CFR	NERC CIP	ISO 27001	NIST CSF 2.0	NIST AI RMF
Physical protection (plant + center)	Applies	Partial	No	Partial	No
Grid reliability	No	Applies	No	Partial	No
Data confidentiality	No	No	Applies	Applies	Partial
Data-center availability / continuity	No	Partial	Applies	Applies	No
AI-model and data risk	No	No	Partial	Partial	Applies
Cross-sector incident coordination	Partial	Partial	Partial	Applies	Partial

(Entries are illustrative; students derive and justify their own, revealing where coverage overlaps or is thin.)

For each cell, students indicate whether a framework clearly applies, partially applies, or does not apply, and cite the basis; they then annotate the matrix to identify overlaps (multiple frameworks addressing one concern with different vocabulary) and gaps (no framework cleanly covering a cross-sector concern), and select one real industrial partnership to discuss which frameworks would be in play.

Phase 3 — Synthesis (whole class): groups present and defend their overlap/gap findings; the instructor connects the exercise to the general lesson, using the FERC–Amazon–Talen episode to show how regulatory boundaries themselves become contested when sectors converge.

Phases 1–3 run in class as an ungraded activity; the graded assignment consists of the group's completed governance-mapping matrix and one-page coordination report, together with the individual skill transfer reflection.

Assessment and Evaluation

Grades are earned on the assignment, not on the in-class activity. The assignment combines a group artifact—the governance-mapping matrix and a one-page coordination report—with an individual skill transfer reflection. The assignment is assessed with the analytic rubric in Table 6. The group component (60%) is scored on completeness and accuracy of the mapping, correct identification of at least two well-justified overlaps and two well-justified gaps, appropriate use and citation of authoritative sources, and clarity of the report’s coordination recommendation. The individual skill transfer reflection (40%) asks each student to apply the same reasoning to a different cross-sector coupling of their choosing (e.g., a hospital with on-site power generation, or a water-treatment facility coupled with cloud analytics), identifying the relevant frameworks and one likely gap—directly assessing transferable security and governance reasoning rather than recall. To ensure individual accountability, the group grade is moderated by a brief confidential peer-contribution assessment, so individual marks can be adjusted for uneven participation. The 60/40 split weights the group assignment—which exercises the full mapping–overlap–gap chain (LO2–LO4) on a shared case—against the individual skill reflection, which isolates the highest-order objective (LO4 transfer) under individual accountability.

Table 6. Assessment rubric for the graded assignment

Criterion (weight)	Beginning	Developing	Proficient	Excellent
Mapping matrix — accuracy & completeness (30%)	Many cells wrong or missing	Several errors or omissions	Mostly accurate; minor gaps, basis cited	All five frameworks mapped correctly; each cell's basis cited
Overlaps & gaps — identified & justified (20%)	Fewer than two, or unjustified	Two named but weakly justified	Two overlaps and two gaps, adequately justified	≥2 each, precisely located and well-justified
Coordination memo & sources (10%)	Missing or incoherent	Vague; weak or missing citations	Clear recommendation; mostly authoritative sources	Actionable memo; authoritative sources cited throughout
Individual skill transfer reflection (40%)	No genuine transfer; recall only	Partial transfer; framework or gap weak	Appropriate framework and a valid gap for a new coupling	Well-scoped frameworks and a well-argued gap; reasoning clearly transferred

Group assignment = first three rows (60%); individual skill reflection = last row (40%). LO1 (naming frameworks) can also be additionally checked by the pre/post quiz.

The design above specifies what students do; the next question is what they should learn from it, and how that learning would be measured. As an instructional design, the case specifies its intended outcomes and the instrument for evaluating them, so that classroom deployment can test them directly. Stated in assessable terms, the expected outcomes follow from the objectives: students can name and characterize the five core frameworks; can produce a defensible governance-mapping matrix for coupled cyber-physical facilities; can identify and justify at least two overlaps and two gaps; and can transfer the analysis to an unfamiliar cross-sector scenario. Two evaluation measures are planned. First, a short pre/post framework-mapping quiz will measure gains in framework knowledge and mapping accuracy. Second, the group artifact and individual skill reflection will be scored against the Table 6 rubric, with the quality of overlap/gap identification and the skill transfer reflection serving as the primary evidence of higher-order reasoning. Reporting these results across one or more course sections is the immediate next step and will convert this design into a fully evaluated teaching case.

Discussion

Beyond the specific outcomes and their assessment, what does the case ultimately teach? The intended outcome is not that students learn facts about nuclear power or any company, but that they develop transferable dual-governance reasoning skills: inventorying the frameworks that apply to a coupled cyber-physical system, mapping them onto sectors and risks, and reasoning explicitly about overlaps, gaps, and coordination needs. These skills matter because convergence is broad and growing: IS graduates increasingly work on systems that cross sector lines—healthcare and cloud, operational technology and IT, energy and computing—and each crossing raises the same class of questions this teaching case makes concrete.

Several features make the teaching case pedagogically durable. It uses citable, authoritative material, so instructors can update it as frameworks and deals evolve without depending on proprietary content. Its multi-industrial partnership structure supports genuine comparison rather than a single-company study. It integrates cyber and physical dimensions and multiple regulatory regimes, exercising a breadth of reasoning single-framework case studies do not. And the individual skill transfer reflection explicitly tests whether students can carry the reasoning to a new context.

Several limitations are worth acknowledging. First, as an instructional design, the teaching case has not yet been deployed with students, so the expected learning outcomes remain to be validated empirically, although the evaluation plan above is designed to close this gap. Second, the frameworks and partnership landscape evolve quickly, so materials require periodic refresh. Third, the case is U.S.-centric in its core governance frameworks (NRC, NERC CIP, NIST), though ISO/IEC 27001 and optional IAEA references support international sections. Finally, the teaching case builds reasoning skills rather than hands-on technical controls; instructors wanting a technical lab component would pair it with separate exercises.

None of these limitations undercut the central claim—that the convergence is an effective vehicle for teaching cyber-physical cross-sector dual-governance. A natural next step is classroom deployment, which would both validate the expected learning outcomes and enable a student-in-the-loop refinement of the instructional design, which can iteratively improve the teaching case.

Conclusion

AI-driven data-center demand is increasing electricity consumption and reviving nuclear power, producing a repeatable pattern of major cloud and AI providers coupling data centers with nuclear generation. This convergence is a live, well-documented example of the governance challenges that arise when two critical-infrastructure sectors—with different regulators, security priorities, and frameworks—become operationally intertwined. This paper argued that traditional cyber-focused, information-sector IS security and governance curriculum should be expanded to incorporate cyber-physical cross-sector dual governance. It presented the nuclear-powered AI data center convergence as a teaching case for demonstrating how. The teaching case includes learning objectives, a target course with IS2020 and ABET mappings, a comparative-framework activity with assessment, and an instrument for evaluating expected outcomes. By learning to compare, map, and integrate the governance frameworks that apply to coupled cyber-physical facilities—and to transfer that reasoning to new contexts—students build governance-reasoning skills that will serve them across the many sector convergences they will encounter. Future work will deploy the teaching case in the classroom, gather pre/post learning evidence against the evaluation plan, and extend the case with international frameworks and additional convergence domains.

Acknowledgments

The authors used a generative AI assistant (Anthropic's Claude) to help format the manuscript to the journal template and edit language for clarity. All scholarly content, analysis, and conclusions are the authors' own; the authors reviewed and verified the manuscript and take full responsibility for its originality, validity, and integrity, consistent with the IIS AI Use Policy.

References

- ABET. (2025). *Criteria for accrediting computing programs, 2025–2026 — Cybersecurity program criteria*. Computing Accreditation Commission. Retrieved on 07/9/2026 from <https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2025-2026/>
- ACM/AIS. (2020). *IS2020: A competency model for undergraduate programs in information systems*. Association for Computing Machinery and Association for Information Systems.
- Amazon. (n.d.). *ISO/IEC 27001:2022 overview and FAQ*. Retrieved on 07/9/2026 from <https://aws.amazon.com/compliance/iso-27001-faqs/>
- Casamassa, J., Wang, W., & Masialeti, M. (2025). Generative AI governance for cybersecurity: An integrated approach. *Issues in Information Systems*, 26(3), 484–493.
- Clifford, C. (2022). What the climate bill does for the nuclear industry. CNBC. Retrieved on 07/9/2026 from <https://www.cnbc.com/2022/08/22/what-the-climate-bill-does-for-the-nuclear-industry.html>
- CPUC. (2026). *Senate Bill 846*. California Public Utilities Commission. Retrieved on 07/9/2026 from <https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/electric-costs/what-are-nuclear-electric-cost/senate-bill-846>
- Data Center Dynamics. (2024). *Meta launches nuclear power RFP, targets 1–4GW for data centers*. Retrieved on 07/9/2026 from <https://www.datacenterdynamics.com/en/news/meta-launches-nuclear-power-rfp-targets-14gw-for-data-centers/>
- Disavino, S. (2026). U.S. power use to beat record highs in 2026 and 2027 as AI use surges, EIA says. Reuters. Retrieved on 07/9/2026 from <https://www.reuters.com/business/energy/us-power-use-beat-record-highs-2026-2027-ai-use-surges-eia-says-2026-04-07/>
- Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences*, 111(23), 8410–8415. <https://doi.org/10.1073/pnas.1319030111>
- Goldman Sachs. (2025). *AI is poised to drive 160% increase in data center power demand*. Retrieved on 07/9/2026 from <https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand>
- Herreid, C. F. (1994). Case studies in science: A novel method of science education. *Journal of College Science Teaching*, 23(4), 221–229.

- Herreid, C. F., & Schiller, N. A. (2013). Case studies and the flipped classroom. *Journal of College Science Teaching*, 42(5), 62–66.
- Hiller, J. (2024). Google backs new nuclear plants to power AI. *The Wall Street Journal*. Retrieved on 07/9/2026 from <https://www.wsj.com/business/energy-oil/google-nuclear-power-artificial-intelligence-87966624>
- International Energy Agency (IEA). (2026). *Electricity 2026: Analysis and forecast to 2030*. Retrieved on 07/9/2026 from https://iea.blob.core.windows.net/assets/b73798cb-e452-42b9-9d8a-07542de7a041/Electricity_2026.pdf
- International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Retrieved on 07/9/2026 from <https://www.iso.org/standard/82875.html>
- Joint Task Force on Cybersecurity Education. (2018). *Cybersecurity curricula 2017 (CSEC2017): Curriculum guidelines for post-secondary degree programs in cybersecurity*. ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. <https://doi.org/10.1145/3184594>
- Kearney, L. (2025). Three Mile Island nuclear plant reboot fast-tracked to 2027. Reuters. Retrieved on 07/9/2026 from <https://www.reuters.com/sustainability/climate-energy/shut-three-mile-island-nuclear-plant-may-restart-2027-owner-says-2025-06-25/>
- Luccioni, A. S., Jernite, Y., & Strubell, E. (2024). Power hungry processing: Watts driving the cost of AI deployment? arXiv preprint arXiv:2311.16863.
- Mandler, C. (2024). Three Mile Island nuclear plant will reopen to power Microsoft data centers. NPR. Retrieved on 07/9/2026 from <https://www.npr.org/2024/09/20/nx-s1-5120581/three-mile-island-nuclear-power-plant-microsoft-ai>
- National Institute of Standards and Technology. (2024a). *Artificial intelligence risk management framework (AI RMF 1.0): Generative artificial intelligence profile*. U.S. Department of Commerce. Retrieved on 07/9/2026 from <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
- National Institute of Standards and Technology (NIST). (2024b). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. Retrieved on 07/9/2026 from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- North American Electric Reliability Corporation (NERC). (2026). *Critical Infrastructure Protection (CIP) standards*. Retrieved on 07/9/2026 from <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- Power Engineering. (2024). *AWS acquires data center campus connected to Susquehanna nuclear station*. Retrieved on 07/9/2026 from <https://www.power-eng.com/nuclear/aws-acquires-data-center-campus-connected-to-susquehanna-nuclear-station/>
- Power Engineering. (2024b). *Oracle designing data center to be powered by trio of small modular reactors*. Retrieved on 07/15/2026 from <https://www.power-eng.com/nuclear/smrs/oracle-designing-data-center-to-be-powered-by-trio-of-small-modular-reactors/>

- Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, 93(3), 223–231. <https://doi.org/10.1002/j.2168-9830.2004.tb00809.x>
- Robb, D. (2025). Google is betting big on nuclear energy — Here's why. TechRepublic. Retrieved on 07/15/2026 from <https://www.techrepublic.com/article/news-google-nuclear-energy-data-centers/>
- Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. arXiv preprint arXiv:1906.02243.
- USDoE. (2024). *Newly signed bill will boost nuclear reactor deployment in the United States*. U.S. Department of Energy. Retrieved on 07/9/2026 from <https://www.energy.gov/ne/articles/newly-signed-bill-will-boost-nuclear-reactor-deployment-united-states>
- U.S. Nuclear Regulatory Commission (NRC). (2026a). Diablo Canyon — license renewal application. Retrieved on 07/9/2026 from <https://www.nrc.gov/reactors/operating/licensing/renewal/applications/diablo-canyon>
- U.S. Nuclear Regulatory Commission (NRC). (2026b). Reactor license renewal. Retrieved on 07/9/2026 from <https://www.nrc.gov/reactors/operating/licensing/renewal>
- Utility Dive. (2024). *FERC rejects interconnection pact for Talen–Amazon data center deal at nuclear plant*. Retrieved on 07/9/2026 from <https://www.utilitydive.com/news/ferc-interconnection-isa-talen-amazon-data-center-susquehanna-exelon/731841/>
- Wang, W. (2016). A learning module for advanced cryptology. *Issues in Information Systems*, 17(4), 98–108.