J Euro Eco His.
ISSN : 0391-5115
Volume 2, Isue 1 (2021)

THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Cybersecurity Education for Future Accountants: A Competency-Based Curriculum Framework for Assurance, Advisory, and Governance Roles

Ayaan Rahman, PhD
Department of Accounting & Information Systems, Eastbridge University of Business, Kolkata, India

Meera Nair, MBA, CPA (Dummy)
School of Management, Coastal Institute of Commerce, Kochi, India

Tariq Hassan, MSc (EdTech)
Center for Digital Learning Innovation, North Valley University, Guwahati, India

Abstract

As organizations digitize financial processes and migrate data to cloud platforms, cybersecurity risk increasingly determines the reliability of accounting information, the integrity of financial reporting, and the effectiveness of internal controls. Accountants—whether in assurance, corporate finance, internal audit, taxation, or advisory—are now expected to understand cyber risk impacts on financial statements, evaluate technology controls, interpret security reports, and communicate risk to governance bodies. However, cybersecurity education within accounting programs remains uneven, frequently treated as an elective or embedded superficially within accounting information systems courses. This paper proposes a competency-based framework for cybersecurity education tailored to accounting roles, aligning learning outcomes with audit/assurance expectations, governance responsibilities, and professional standards. Using a design-science-oriented approach, we develop a curriculum architecture that integrates foundational cyber concepts (confidentiality, integrity, availability), technology controls (identity access, logging, encryption), risk management (threat modeling, incident response), and assurance artifacts (SOC reporting, control testing, evidence). The paper provides a practical course map, assessment strategies, and implementation guidance for emerging economies and resource-constrained institutions. We conclude that embedding cybersecurity as a longitudinal thread across accounting curricula—supported by labs, case-based learning, and cross-disciplinary collaboration—improves graduates' employability and strengthens the profession's contribution to digital trust.

Key Words: cybersecurity education, accounting curriculum, audit analytics, internal controls, SOC reports, risk management, digital trust, AIS

Introduction

Accounting is fundamentally a trust profession. Stakeholders rely on accounting systems to record transactions accurately, safeguard assets, produce reliable financial statements, and support compliant decision-making. In digital environments, this trust is directly shaped by cybersecurity controls and cyber resilience. A compromised enterprise resource planning (ERP) system, a ransomware attack that corrupts ledgers, or credential theft enabling unauthorized journal entries can each translate into misstatements, control failures, regulatory exposure,

and reputational damage. As a result, accountants increasingly operate at the intersection of finance, technology, and risk.

Yet many accounting programs still treat cybersecurity as a specialized "IT topic" rather than a core element of accounting competence. Graduates may understand internal control frameworks conceptually but lack the ability to evaluate access logs, interpret a SOC 1 report, assess segregation-of-duties conflicts in role-based access, or communicate cyber-related financial reporting risks to audit committees. This gap is especially visible when new professionals join audit teams that use technology control testing, or when corporate accountants participate in governance processes like risk assessments and incident reporting.

This paper addresses the curriculum problem: **What cybersecurity knowledge and skills should future accountants possess, and how can accounting programs teach them effectively without turning the degree into an IT major?** The objective is not to make accountants security engineers. Rather, it is to build **cyber-informed accounting professionals** who can (a) identify cybersecurity risks relevant to financial reporting and business continuity, (b) evaluate technology controls and evidence, (c) collaborate with IT and security teams using shared language, and (d) exercise professional judgment under digital threats.

We contribute a structured, competency-based framework and a practical curriculum blueprint. Our approach emphasizes:

1. **Role relevance:** cybersecurity content tied to audit, reporting, tax, governance, and advisory tasks;
2. **Evidence orientation:** focusing on what accountants examine—controls, logs, reports, policies, exceptions, and analytics;
3. **Integration:** cybersecurity as a thread across courses (AIS, auditing, managerial accounting, ethics, capstone); and

Assessment readiness: rubrics, cases, and lab exercises that institutions can implement with modest resources.

2. Background and Related Literature

2.1 Cybersecurity as an Accounting Issue

Cybersecurity affects accounting through multiple pathways. First, cyber incidents can compromise transaction processing, leading to incomplete or inaccurate recording. Second, they may weaken internal controls over financial reporting—particularly when identity and access management fails. Third, cyber events can create material disclosures (contingent liabilities, going concern concerns, operational disruptions) and require judgments about impairment, revenue recognition disruptions, or restoration costs. Finally, auditors must consider technology risks when planning and performing audits, especially around automated controls and IT-dependent manual controls.

Professional practice has increasingly reflected this reality: audit methodologies commonly include IT general controls (ITGCs), access reviews, change management evaluation, and reliance on service organization reports. Accountants also work with frameworks such as COSO for internal control, COBIT for IT governance, and security-oriented references like NIST and ISO 27001.

2.2 Skills Gap in Accounting Education

Prior education research on accounting information systems has long argued that accounting graduates need technology literacy. However, cybersecurity is often addressed as a subset of AIS, resulting in uneven depth. Common challenges include limited faculty expertise, crowded curricula, lack of lab infrastructure, and uncertainty about "how technical" accountants should become. Where cybersecurity appears, it may be delivered as conceptual lectures rather than competency-driven experiences (e.g., interpreting logs, analyzing access risks, or conducting a control walkthrough).

A competency approach helps because it shifts the question from "Which cybersecurity topics should we cover?" to "What must graduates be able to do?" This orientation aligns with outcomes-based education and professional expectations from accounting bodies emphasizing technology, risk, and professional judgment.

2.3 Competency and Standards Alignment

A credible curriculum framework should align with:

- **Internal control and governance frameworks** (e.g., COSO; COBIT) for risk/control language;
- **Cybersecurity frameworks** (e.g., NIST CSF) for core functions (Identify, Protect, Detect, Respond, Recover);
- **Audit risk standards** (e.g., risk assessment standards that emphasize understanding information systems and controls); and
- **Professional education guidance** (e.g., IFAC International Education Standards) emphasizing competence, ethics, and professional judgment.

The literature suggests that integration across auditing, AIS, ethics, and capstone courses is more effective than a single elective because students repeatedly apply cyber thinking in accounting contexts.

3. Research Aim, Questions, and Contribution

3.1 Aim

To design a competency-based cybersecurity education framework tailored to future accountants and translate it into an implementable curriculum blueprint.

3.2 Research Questions

RQ1: Which cybersecurity competencies are most relevant to entry-level and early-career accountants across assurance, corporate finance, and governance roles?

RQ2: How can accounting programs embed cybersecurity learning outcomes across the curriculum without excessive technical prerequisites?

RQ3: What teaching and assessment methods best demonstrate cyber-informed accounting competence (evidence evaluation, control reasoning, and communication)?

3.3 Contribution

This paper contributes:

- A **competency model** linking cybersecurity functions to accounting tasks and evidence;
- A **curriculum architecture** (modules, course mapping, learning outcomes, and assessments);
- Practical **implementation guidance** for institutions, including resource-light labs and case

strategies.

4. Methodology: Design-Science-Oriented Curriculum Development

We use a design-science-oriented methodology commonly applied to educational interventions and professional curriculum design. The method is appropriate because the goal is to create an artifact (a curriculum framework) that solves a practical problem and is grounded in theory and standards.

4.1 Steps

1. **Problem identification:** cybersecurity skill gap for accounting graduates;
2. **Objective definition:** role-relevant competencies, integrable curriculum, assessable outcomes;
3. **Design and development:** competency model and course map;
4. **Demonstration:** sample modules, cases, and assessment rubrics;
5. **Evaluation logic:** feasibility, alignment, coverage, and assessment validity (discussed via implementation considerations);
6. **Communication:** artifact presented as figures, tables, and structured guidance.

4.2 Scope and Assumptions

The framework is designed for undergraduate and postgraduate accounting programs. It assumes basic digital literacy (spreadsheets, databases concepts) but no advanced programming requirement. Technical depth is calibrated to what accountants need to **evaluate risk, controls, and evidence**—not to build security tools.

5. Cybersecurity Competencies for Accountants

Cybersecurity competence for accountants can be grouped into four domains: **(1) Cyber foundations for trust, (2) Controls and assurance evidence, (3) Risk and incident reasoning, and (4) Communication, ethics, and governance.**

5.1 Domain 1: Cyber Foundations for Trust

Accountants must understand how digital systems create, store, and transmit financial data. Foundational competence includes:

- The CIA triad (confidentiality, integrity, availability) and its mapping to accounting assertions;
- Authentication vs. authorization; role-based access control; least privilege; segregation of duties;
- Data lifecycle: creation → processing → storage → archival → disposal, and related risks;
- Common threat types (phishing, malware, ransomware, insider threats) at a conceptual level.

This domain builds vocabulary and mental models so accountants can collaborate with IT/security teams without misunderstanding terms like “privileged access,” “change management,” or “encryption at rest.”

5.2 Domain 2: Controls and Assurance Evidence

This is the most accounting-specific domain. Competence includes:

- Understanding IT general controls: access, change management, operations, backups;
- Application controls: input validation, automated approvals, system configurations;
- Evaluating evidence: screenshots, access listings, ticket logs, configuration exports, SOC reports;

- Interpreting service organization assurance (SOC 1/SOC 2 concepts), complementary user entity controls, and exceptions;
- Linking control failures to audit risks and financial statement assertions.

The goal is to create graduates who can participate meaningfully in audits and internal control projects, even if specialists perform penetration tests.

5.3 Domain 3: Risk and Incident Reasoning

Accountants need to evaluate risk scenarios and implications for reporting and governance:

- Risk assessment methods: likelihood, impact, inherent vs. residual risk;
- Incident response phases and the accounting implications of downtime and data compromise;
- Business continuity and disaster recovery concepts (RTO/RPO) and their relevance to financial operations;
- Third-party and supply chain risk: cloud providers, payroll processors, payment gateways.

This domain supports professional judgment in assessing disclosures, control deficiencies, and operational resilience.

5.4 Domain 4: Communication, Ethics, and Governance

Cybersecurity creates ethical and governance challenges: data privacy, surveillance, responsible disclosure, and transparency to stakeholders. Accountants must be able to:

- Communicate cyber risks in plain language to non-technical stakeholders (CFO, audit committee);
- Apply professional ethics when handling sensitive data;
- Understand governance responsibilities and documentation expectations;
- Recognize legal/regulatory considerations at a high level (privacy obligations, breach notification concepts) while deferring legal interpretation to experts.

6. A Role-Relevant Framework Linking Cybersecurity to Accounting Work

Figure 1

Cybersecurity Competency Framework for Accountants (Mapping Functions → Accounting Tasks → Evidence)

NIST CSF Function	Accounting Task	Typical Evidence / Artifact
IDENTIFY	Understand systems in audit planning; map risks to assertions	System narratives, dataflow diagrams, risk registers
PROTECT	Evaluate access control & change management	User access lists, SoD matrix approval workflows, tickets
DETECT	Assess monitoring & exception handling	Log samples, alert reports, SIEM summaries (conceptual)
RESPOND	Review incident impact on reporting & controls	Incident timelines, post-incident reports, approvals

RECOVER	Evaluate BCP/DR and continuity for finance	Backup policies, DR test results, restoration evidence

Explanation: This figure translates cybersecurity from abstract "security topics" into the accountant's daily reality: tasks and evidence. A curriculum built on this mapping naturally supports audit readiness, internal control effectiveness, and governance communication.

7. Curriculum Architecture and Course Mapping

A practical accounting program can integrate cybersecurity through a **three-layer structure**:

- **Layer A (Core thread):** cybersecurity concepts embedded in AIS, Auditing, Ethics, and Capstone;
- **Layer B (Skills modules):** short labs/cases inserted across semesters;
- **Layer C (Electives/advanced):** optional deeper topics (forensic analytics, continuous auditing, cloud assurance).

7.1 Proposed Learning Outcomes (Sample)

By graduation, students should be able to:

1. Explain how cybersecurity risks affect financial reporting assertions and internal control objectives.
2. Perform a basic access risk review using role-based access data and identify segregation-of-duties conflicts.
3. Interpret a SOC-style report summary and identify complementary user entity controls and key exceptions.
4. Document a cyber-related control walkthrough and propose an appropriate test of design and operating effectiveness.
5. Communicate a cyber incident's accounting implications (control deficiency, disclosure considerations, operational impact) to a governance audience.

7.2 Course Mapping (Illustrative)

AIS (Accounting Information Systems):

Students learn system narratives, dataflows, controls, and cyber foundations (CIA, access control, change management). Labs include role-based access and simple log reasoning.

Auditing and Assurance:

Students connect ITGCs and application controls to audit risk, evidence, sampling, and reliance decisions. Casework includes SOC report interpretation and control deficiency evaluation.

Managerial/Cost Accounting (Integration Point):

Students evaluate cyber risk as operational risk: downtime costs, recovery investment decisions, and risk appetite, linking cyber controls to performance and budgeting.

Taxation (Integration Point):

Students discuss data confidentiality, taxpayer data protection, secure transmission, and identity verification risks.

Professional Ethics / Governance:

Students examine confidentiality duties, responsible handling of sensitive data, and

governance communication under uncertainty.

Capstone:

Students complete a simulated engagement: risk assessment, control evaluation, reporting memo to audit committee, and reflection on ethical choices.

8. Teaching Methods and Learning Activities

8.1 Case-Based Learning (Accounting-Centered)

Cybersecurity becomes meaningful when students confront realistic scenarios:

- A ransomware disruption during month-end close;
- Unauthorized vendor master data changes causing fraud;
- Cloud payroll provider outage affecting accruals and disclosures;
- Phishing leading to compromised CFO email and payment diversion.

Cases should require students to identify: (a) impacted processes, (b) control failures, (c) evidence needed, and (d) reporting implications.

8.2 Lab Exercises Without Heavy Infrastructure

Programs often lack advanced labs. A "resource-light" approach uses:

- Spreadsheet-based access matrices (users, roles, permissions);
- Simulated ticket logs (change requests, approvals, emergency fixes);
- Mock SOC report excerpts (control objectives, tests, exceptions);
- Simple log samples (failed logins, privileged access usage) for pattern recognition.

These can be delivered through learning management systems using downloadable datasets.

8.3 Interdisciplinary Collaboration

Accounting faculty can collaborate with computer science or information systems departments for guest lectures or joint modules. The accounting instructor frames the content around internal control, audit evidence, and financial reporting implications, ensuring relevance.

9. Assessment Design: Measuring Cyber-Informed Accounting Competence

9.1 Why Traditional Exams Are Not Enough

Cybersecurity competence for accountants is demonstrated through applied judgment: evaluating evidence, documenting control reasoning, and communicating risk. Multiple-choice tests alone cannot capture these skills.

9.2 Recommended Assessment Components

1. **Control Walkthrough Report (Individual):** Students document process narratives, identify control points, and link risks to assertions.
2. **Access Review & SoD Analysis (Individual):** Given a user-role dataset, students identify conflicts and propose remediation (role redesign, compensating controls).
3. **SOC Interpretation Memo (Team):** Students interpret key controls, exceptions, and complementary controls; evaluate reliance implications.
4. **Incident Response Accounting Memo (Individual):** Students write a governance-focused memo on implications for reporting, controls, and continuity.
5. **Capstone Simulation (Team):** A multi-week project combining risk assessment, evidence evaluation, and final presentation.

9.3 Sample Rubric Dimensions

- Correctness of risk-control mapping;
- Quality of evidence reasoning;
- Professional judgment and prioritization;
- Clarity and governance-friendly communication;
- Ethical sensitivity and documentation quality.

10. Implementation Considerations for Emerging Economies and Resource-Constrained Institutions

10.1 Faculty Capability Development

Faculty constraints are a major barrier. Institutions can start with:

- Short faculty workshops on NIST CSF concepts and audit-relevant controls;
- Shared teaching packs (datasets, cases, rubrics);
- Partnerships with local audit firms and professional bodies for guest sessions.

10.2 Curriculum Crowding and Integration Strategy

Rather than adding a full new course immediately, programs can embed cybersecurity outcomes into existing courses. For example, adding one lab and one case per semester creates cumulative learning without curriculum overload.

10.3 Industry Engagement

Firms can provide anonymized process narratives, sample access review templates, and practical insights on common control issues. This improves authenticity and graduate readiness.

10.4 Ethical and Legal Boundaries

Teaching must emphasize that students should not perform real hacking or intrusive testing. Activities should focus on governance, control evaluation, and evidence interpretation using simulated data.

11. Discussion

11.1 Why This Framework Works for Accounting

The framework is built around accounting roles and artifacts. It avoids the trap of turning cybersecurity education into a technical survey course detached from accounting practice. By organizing content around tasks and evidence—access reviews, change tickets, control walkthroughs, SOC reports—students practice the exact reasoning demanded in audits and internal control roles.

11.2 Implications for the Profession

Graduates with cyber-informed accounting competence can strengthen digital trust in multiple ways:

- Better internal control documentation and testing;
- More credible risk communication to governance;
- Improved collaboration with IT/security, reducing misunderstanding;
- Enhanced ability to respond to incidents with disciplined documentation and reporting.

11.3 Risks and Limitations

This paper proposes a design artifact rather than reporting multi-institution empirical outcomes. Future research should evaluate learning gains, employer satisfaction, and certification alignment across different contexts. Another limitation is the fast evolution of cybersecurity threats; however, a competency-based structure is resilient because it teaches reasoning patterns, not only tool-specific knowledge.

12. Conclusion and Recommendations

Cybersecurity is now inseparable from accounting reliability and assurance quality. Accounting education must respond by developing cyber-informed graduates who can evaluate technology controls, interpret assurance artifacts, and communicate risk effectively. This paper proposed a competency-based framework and curriculum architecture that embeds cybersecurity across accounting programs through integrated modules, evidence-centered labs, and applied assessments.

Recommendations:

1. Treat cybersecurity as a longitudinal thread across AIS, auditing, ethics, and capstone courses.
2. Teach cybersecurity through accounting evidence and artifacts (access lists, tickets, SOC concepts, control walkthroughs).
3. Use applied assessments emphasizing professional judgment and governance communication.
4. Build faculty capacity through partnerships and shared teaching resources.
5. Continuously refresh cases to reflect evolving threats while keeping competencies stable.

Image 1 (Insertable Conceptual Illustration)

Title: "Cyber Risk Pathways to Financial Misstatement"

Description (for insertion in the paper): An infographic showing a cyber event (phishing → credential theft → unauthorized access → journal entry manipulation → misstated revenue) with arrows linking to impacted assertions (occurrence, accuracy, completeness) and control points (MFA, privileged access monitoring, journal entry review).

(You can place this as a visual panel near Sections 1 and 6.)

References (APA Style)

1. AICPA. (2017). *System and Organization Controls (SOC) for service organizations: Trust services criteria*. American Institute of Certified Public Accountants.
2. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory, 36*(4), 1–27.
3. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal control—Integrated framework*. COSO.
4. Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162–176.
5. Deloitte. (2018). *Cyber risk and the audit committee*. Deloitte Insights.
6. Information Systems Audit and Control Association (ISACA). (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
7. International Auditing and Assurance Standards Board (IAASB). (2019). *ISA 315 (Revised*

2019): Identifying and assessing the risks of material misstatement. IFAC.

8. International Federation of Accountants (IFAC). (2019). *International Education Standards (IES): Handbook of International Education Pronouncements*. IFAC.
9. Kopp, L. S., Leyer, M., & Stark, R. (2021). The influence of digitalization on the future of the accounting profession. *Journal of Accounting Literature, 47*, 1–20.
10. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. U.S. Department of Commerce.
11. Pathways Commission. (2012). *Charting a national strategy for the next generation of accountants*. American Accounting Association & AICPA.
12. Pwc. (2020). *Cybersecurity and the CFO: Managing risk, reporting, and resilience*. PwC Reports.
13. Richardson, V. J., Teeter, R., & Terrell, K. (2022). *Accounting information systems: The crossroads of accounting and IT* (3rd ed.). Wiley.
14. Sutton, S. G., Holt, M., & Arnold, V. (2016). The reports of my death are greatly exaggerated—Artificial intelligence research in accounting. *International Journal of Accounting Information Systems, 22*, 60–73.
15. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
16. World Economic Forum. (2020). *Principles for board governance of cybersecurity*. WEF.