A Framework for Multi-University Cybersecurity Curriculum Gap Analysis

Fabien Sechi[1,2], and Sabarathinam Chockalingam[2]

[1] Department of Information and Communication Technology, University of Agder, Grimstad, Norway.
fabien.e.sechi@uia.no

[2] Department of Risk and Security, Institute for Energy Technology, Halden, Norway.
{Fabien.Sechi, Sabarathinam.Chockalingam}@ife.no

Abstract. With the global demand for cybersecurity professionals consistently exceeding supply, higher education institutions plays a critical role in addressing the skills gap. This requires aligning curricula not only with evolving workforce requirements but also with international standards that ensure consistency and quality. However, systematic approaches for identifying curricular strengths and gaps across universities remain underdeveloped. To address this gap, this paper introduces a methodological framework that integrates the *Cyber Security Curricula 2017 guidelines* with a *curriculum maturity model* to evaluate cybersecurity education across institutions. We demonstrate the framework through a comparative case study of three universities: *Norwegian University of Science and Technology (NTNU), Østfold University College (HiØ), and The Virginia Polytechnic Institute and State University (Virginia Tech).* Across three universities (NTNU, HiØ, Virginia Tech), the framework mapped 110 courses, with 44% Core Cybersecurity and 56% Cybersecurity-Related. NTNU excelled in Data Security, HiØ in Organizational and Human Security, and Virginia Tech in Societal Security. Common strengths included Cryptography, Risk Management, and Network Architectures, while persistent gaps appeared in Storage Security, Identity Management, Usable Security, and lifecycle aspects of System Security. These results highlight the value of a structured, evidence-based approach for identifying curricular strengths and weaknesses. This framework is designed to be replicable in other higher-education contexts seeking program improvement.

Keywords: CSEC2017 · Curriculum evaluation · Cybersecurity education · Gap analysis · Maturity model

1 Introduction

The persistent shortage of cybersecurity professionals, estimated at over three million worldwide, highlights the urgent need to strengthen education and training pipelines [1]. As digitalization reaches every critical sector, universities are increasingly tasked with preparing graduates whose skills not only meet workforce demands but also align with international standards that ensure quality

and comparability across institutions. However, systematic approaches for evaluating cybersecurity curricula remain underdeveloped. Existing programme comparisons are often ad hoc, limiting their ability to provide rigorous or replicable insights. At the same time, the very definition of a "cybersecurity professional" is contested. Some programmes emphasise technical competencies, while others focus on managerial, organizational, or policy-related areas [2].

The challenge is further complicated by the widespread role of professional certifications. Employers increasingly require certifications even for candidates with advanced academic degrees, creating uncertainty about redundancy and overlap between certifications and university curricula. Researchers argue that certifications should be more systematically integrated into academic programmes, but consensus is limited and empirical evidence remains scarce [3]. These tensions highlight the need for structured, evidence-based methods to identify curricular strengths and weaknesses in ways that are transparent and comparable across institutions. Addressing these challenges will also establish stronger collaboration across universities, enabling resource sharing, best-practice exchange, and the utilization of institutional strengths to build more balanced and globally relevant cybersecurity education.

To that end, this paper introduces a methodological framework for multi-university cybersecurity curriculum gap analysis that is replicable. The framework combines the **Cyber Security Curricula 2017 (CSEC2017) taxonomy**, covering eight Knowledge Areas (KAs) and fifty-four Knowledge Units (KUs), with a **five-level maturity model** adapted from the Community of Practice literature. CSEC2017 ensures consistency in coverage assessment, while the maturity model translates quantitative metrics into interpretable profiles of curricular development.

We demonstrate this framework through a comparative case study of three universities that represent contrasting educational contexts: the Norwegian University of Science and Technology (NTNU) [4], Østfold University College (HiØ) [5], and The Virginia Polytechnic Institute and State University (Virginia Tech) [6]. The dataset includes bachelor- and master-level courses delivered between 2020 and 2023, collected through official catalogues, faculty inputs, and a unified metadata template (capturing type, language, course codes, syllabi links, and credit weight) [7]. PhD-level courses and courses not offered during this period were excluded to reflect actual student exposure.

This paper makes three important contributions:

1. A framework that integrates the CSEC2017 taxonomy with a five-level maturity model to enable systematic, standards-aligned curriculum gap analysis.
2. A validated coding and evaluation approach for mapping courses to CSEC2017 KAs and distinguishing core cybersecurity versus cybersecurity-related content with reliability.
3. A comparative case study of three universities (NTNU, HiØ, and Virginia Tech), demonstrating how the framework identifies curricular strengths, blind spots, and opportunities for improvement.

The findings are relevant to university programme directors, curriculum committees, accreditation agencies, and recruiters in technology, intelligence, and critical infrastructure sectors who seek evidence-based alignment between curricula and professional competence.

The remainder of this paper is structured as follows: Section 2 provides background on CSEC2017 guidelines and maturity models in education. Section 3 introduces the proposed framework, outlining its conceptual foundations and core components. Section 4 describes the research design, including institutional sampling, data collection, coding procedures, and maturity assessment. Section 5 presents the quantitative findings from the comparative case study, while Section 6 complements these with qualitative insights on transparency, orientation, and interdisciplinarity. Finally, Section 7 concludes the paper by summarizing contributions, acknowledging limitations, and identifying avenues for future research.

2 Background

Cybersecurity curriculum evaluation has traditionally relied on fragmented approaches, making systematic comparison across institutions difficult. To address this, two key foundations inform our study.

2.1 Cyber Security Curricula 2017 (CSEC2017)

The CSEC2017 guidelines define eight KAs and 54 KUs that structure the domain of cybersecurity education [8]. Each KU is associated with topics and learning outcomes that represent essential competencies. For example, within **KA1 - Data Security**, the Cryptography KU covers topics such as symmetric and asymmetric encryption, key management, and digital signatures, with learning outcomes requiring students to demonstrate the ability to apply secure encryption methods in practical contexts. Similarly, within **KA6 - Human Security**, the Usable Security and Privacy KU addresses user authentication, human–computer interaction, and security awareness, with outcomes emphasising the ability to design or evaluate security mechanisms from a usability perspective. Other KAs reflect different layers of the cybersecurity ecosystem. **KA4 - Connection Security** includes KUs on secure communication protocols and network architectures, while **KA7 - Organizational Security** covers governance, risk management, compliance, and incident response. This structure ensures that both technical and non-technical dimensions are incorporated. Figure 1 illustrates the hierarchy from KAs to Learning Outcomes.

The eight KAs provide the organising structure for cybersecurity curricula; their essential concepts represent proficiency all students should encounter, irrespective of programme emphasis. Figure 2 lists the KAs.

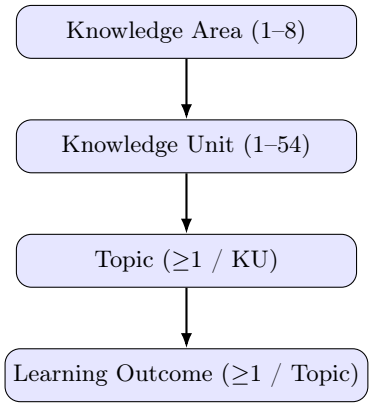

Fig. 1. CSEC2017 hierarchy used for course mapping.

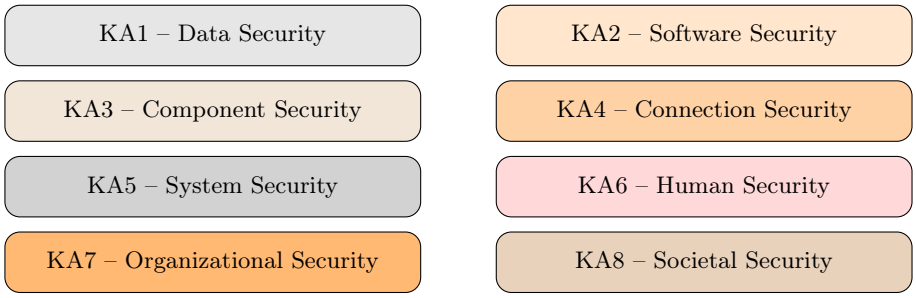

Fig. 2. Eight Knowledge Areas (KAs) in CSEC2017.

2.2 Maturity Models in Education

While CSEC2017 defines the scope and content of cybersecurity education, it does not provide a mechanism for assessing how well these elements are integrated into curricula. For this purpose, Capability Maturity Models (CMMs) have been applied in education and technology management [9, 10, 11]. Marshall et al. [9] proposed an e-learning maturity model to help institutions assess their current processes and define a roadmap for improvement. Their model spans five maturity levels: initial, planned, defined, managed, and optimizing. This is supported by four pillars: student learning, resource creation, project support, and organizational management. Each level specifies requirements across these pillars, providing a staged pathway toward continuous improvement. Solar et al. [10] developed a maturity model for Information and Communication Technology in school education. It introduces domains (e.g., management, infrastructure, teachers, students), Key Domain Areas (KDAs), and measurable critical variables. Maturity is determined by aggregating capability levels across these variables, allowing institutions to identify weaknesses and prioritize development. Across these efforts, maturity models share the goal of translating

quantitative indicators (e.g., coverage, capability levels) into qualitative profiles that are meaningful for institutional improvement.

3 Our Proposed Framework

Our framework integrates two complementary foundations: CSEC2017 taxonomy and a maturity model. Together, these components enable systematic, standards-aligned analysis of cybersecurity curricula across universities.

3.1 Conceptual Basis

CSEC2017 provides the structural taxonomy for cybersecurity education, defining 8 KAs and 54 KUs, each associated with essential topics and learning outcomes. This taxonomy ensures that both technical and non-technical competencies are included and allows curricula from different institutions to be mapped against a shared benchmark. Maturity models provide the interpretive layer. By assigning each KU a maturity level, they translate raw coverage into qualitative profiles of curricular development. This helps stakeholders move beyond binary "covered vs. not covered" measures and understand progression along a development pathway.

3.2 Components of our Framework

The framework operates through three main components:

- **Curriculum Mapping**: Each course is mapped to relevant CSEC2017 KUs, distinguishing between Core Cybersecurity (C) and Cybersecurity-Related (CR) courses. This ensures sensitivity to programme structure while maintaining comparability.
- **Coverage Analysis**: For each institution, KU coverage is aggregated into KA-level summaries. This provides a quantitative view of which areas are well addressed and where systematic gaps exist.
- **Maturity Profiling**: KU coverage percentages are interpreted using a five-level rubric adapted from the Community of Practice maturity model:: *Initial, Awareness, Evolving, Operational, Sustainable*, from Community of Practice literature [12]. The purpose of this rubric is to translate raw coverage percentages into qualitative profiles of curriculum development, making results more interpretable for stakeholders.
  (i) **Initial (0-19%):** Minimal or no exposure to a given KU; content is absent or only mentioned incidentally.
  (ii) **Awareness (20-39%):** Students are introduced to the topic at a surface level, often through elective or peripheral courses, without systematic depth.
  (iii) **Evolving (40-59%):** The curriculum shows developing depth, with multiple courses engaging the KU but coverage remaining uneven or fragmented.

(iv) **Operational (60-79%):** The topic is robustly integrated into the programme, supported by core courses, practical exercises, or assessments.
(v) **Sustainable (80-100%):** Comprehensive and consistent integration across the curriculum, with reinforcement through advanced courses, projects, or interdisciplinary offerings.

These levels provide a structured way to interpret curricular strengths and weaknesses. By combining these components, the framework produces:

- Curricular profiles that highlight strengths and blind spots across institutions.
- Comparative insights that allow benchmarking across universities.
- Actionable pathways for curriculum improvement, grounded in both international standards (CSEC2017) and maturity-based evaluation.

4 Research Design

The research design was developed to apply our proposed framework consistently across multiple institutions. It combines institutional sampling, systematic data collection, course classification, mapping to CSEC2017, and maturity assessment, supported by quality assurance measures.

4.1 Institutional Sample

Two Norwegian universities: NTNU and HiØ, and one US university: VirginiaTech, were purposefully selected to maximize variation in size, governance, and educational traditions while maintaining comparability in degree levels (bachelor and master). Institutional facts (e.g., official naming, type, language, student population, campuses) were compiled using a unified template and verified against official sources and catalogues [4, 5, 6, 7].[3]

4.2 Data Collection

Unified Template A unified metadata template was designed to capture both institutional descriptors (type, language of instruction, enrolment, campus structure) and programme artefacts (course codes, titles, syllabi or catalogue links, credit weight, delivery period). A central element of the template is the mapping of each course to the CSEC2017 taxonomy [8]. Figure 1 depicts this hierarchy. While our analysis counts coverage at the KU level, CSEC2017 assumes at least one topic per KU and at least one learning outcome per topic.

[3] The University of Oslo (UiO) was catalogued during scoping but remained outside the analytic sample; its entry was retained only to document screening decisions [7].

Data Cleaning and Harmonization To harmonize data across systems, credit units were normalized (ECTS versus US credits were recorded but not used in the baseline coverage metric), course identifiers were standardized, and broken links were replaced with authoritative alternatives where available. Inconsistent naming was resolved by prioritizing the official catalogue form valid for the year of delivery [7].

4.3 Coding and Classification

Each course was classified as:

- **Core Cybersecurity (C):** courses with explicit cybersecurity learning outcomes (e.g., cryptography, network security, incident response).
- **Cybersecurity-Related (CR):** courses providing enabling competencies (e.g., operating systems, networks, software engineering, law, or management).

Course learning outcomes were then mapped to the CSEC2017 KUs. A KU was recorded as covered only when at least one assessable learning outcome explicitly aligned with the KU definition. To ensure reliability, two independent coders reviewed a stratified subset of courses, achieving 94% agreement before reconciliation.
For each course, coders reviewed catalogue descriptions and, where available, syllabi and learning outcomes. A KU was marked as *covered* if at least one learning outcome or topic explicitly aligned with the KU's essential concepts. Courses mentioning a topic without assessable outcomes (*topics-only mentions*) were excluded from mapping to avoid inflating coverage. Where alignment was indirect but substantive (e.g., "secure software lifecycle" discussed within a general software engineering course), the KU was recorded under the CR label. All mappings were documented at KU granularity to allow later aggregation to KAs.

4.4 Maturity Assessment

For each institution and KA, coverage was computed as the ratio of distinct KUs marked as covered to the total number of KUs in that KA. Course credit weights were recorded but not applied to coverage calculations. This decision reflects structural differences in programme architecture: for example, bachelor degrees typically span four years in Europe compared to three in the US, while master programmes also vary in duration. Applying credit weights would therefore risk introducing distortions rather than clarity. Nonetheless, this decision represents a potential validity limitation, as it may understate the intensity of coverage in longer courses or programmes.

Maturity levels were then assigned using the thresholds shown in Table 1, adapted from the Community of Practice maturity model for educational interpretation [12].

Table 1. Thresholds for Maturity Assignment

Level	Coverage (%)	Interpretation
Initial	0–19	Minimal exposure
Awareness	20–39	Introductory coverage
Evolving	40–59	Developing depth
Operational	60–79	Robust coverage
Sustainable	80–100	Comprehensive integration

4.5 Quality Assurance

Validity was supported through:

- **Triangulation of multiple data sources (catalogues, repositories, faculty input):** For NTNU and HiØ, corresponding faculty directly completed the unified template and clarified ambiguous cases. For VirginiaTech, the research team populated the same template from multiple departmental catalogues and faculty-provided course lists, including the Undergraduate Cyber Minor, Graduate Cyber Certificate, and policy-oriented offerings. Duplicates were resolved and metadata cross-checked against public catalogues to ensure alignment with the academic years under study [7]. This triangulation across repositories strengthened dataset completeness.
- **Inter-rater reliability checks to minimise coder bias:** To ensure coding consistency, 25% of the courses were double-coded. Agreement on C/CR classification and KU assignments reached 94%. Discrepancies were adjudicated through coder discussion and, when necessary, consultation with faculty informants. The reconciled set of mappings constitutes the basis for all reported results.
- **Audit trail of coding decisions and data transformations:** All mappings, codebooks, and decision logs were maintained under version control. The combination of a unified template, explicit mapping rules, and stored adjudication notes provides an audit trail sufficient to reproduce or extend the analysis in other institutional contexts [7].
- **Ethical Safeguards:** Relying only on publicly available or faculty-approved data and avoiding any student-level information.

5 Quantitative Results and Discussion: Case Study

The analysis revealed clear differences in course portfolios, coverage of KAs, and maturity levels across the three universities. NTNU contributed 52 relevant courses, Virginia Tech 50, and Østfold 8. Pivot tables aggregated KU hits, enabling heat-map visualisation of coverage density. Resulting maturity profiles highlighted, for instance, HIOF's *Operational* standing in *Organisational Security* versus NTNU's *Initial* standing in *Human Security*.

5.1 Course volumes and C/CR balance

Our counts reflect only courses **mapped in the collection**; some relevant classes may be absent if they did not clearly align with KUs. Because cybersecurity learning builds on substantial prerequisites, we distinguish **Core (C)**, courses whose primary intent is cybersecurity, from **Cybersecurity-Related (CR)**, feeder or enabling courses (e.g., operating systems, networks, software engineering, policy) that are **pre-requested** to study cybersecurity in depth.

Using this lens, the portfolios are:

- **NTNU:** 52 total → 29 C / 23 CR (≈ 55.8% C).
- **VT (Table 5):** 50 total → 19 C / 31 CR (≈ 38% C).
- **HIOF:** 8 total → 3 C / 5 CR (≈ 37.5% C).

Aggregating **unweighted** across institutions yields ≈ 43.8% C / 56.2% CR; **weighted by course volume**, ≈ 46.4% C / 53.6% CR. In other words, a slight majority of offerings function as scaffolding for core cybersecurity.

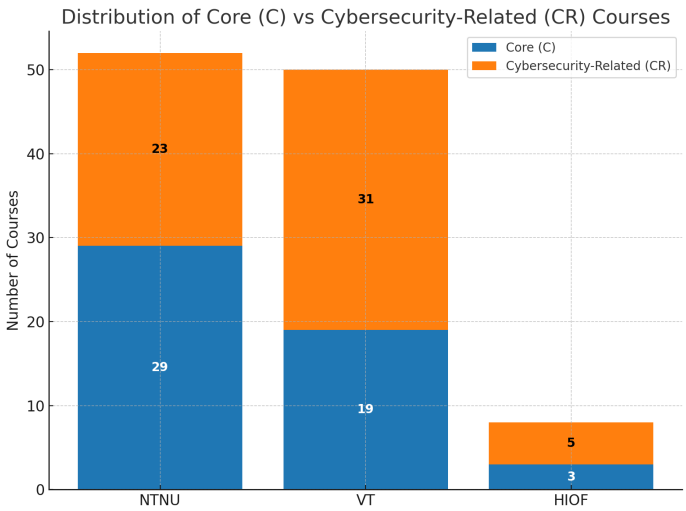

Fig. 3. Distribution of Core (C) vs. Cybersecurity-Related (CR) courses across NTNU, VT, and HIOF.

Interpretation.

- NTNU's mix is core-heavy, signaling depth within dedicated cyber tracks.
- VT and HIOF are CR-heavy, emphasizing foundational breadth that feeds into later specialization.
- At the ecosystem level, programs appear to prioritize pipeline building: ensuring sufficient CR coverage so students can succeed in advanced C courses.

Design implications. A balanced target of roughly 40–50% C with 50–60% CR is consistent with mature programs: CR sustains on-ramps across disciplines; C consolidates advanced competencies. Where CR dominates, adding capstone C courses (e.g., secure systems, network/application security, cryptographic engineering, incident response) can convert breadth into demonstrable expertise. Where C dominates, ensure CR coverage remains healthy (OS, networks, software engineering, data systems, governance/policy) to protect learning progression and accommodate non-CS entrants.

Limitations. Counts are title-based and conservative; some CR courses may deliver substantial cyber depth, and some C courses may vary by instructor/term. Still, the observed C/CR balance provides a useful proxy for curricular maturity and readiness to scale comprehensive cybersecurity programs.

5.2 Coverage by Knowledge Area (KA)

Using CSEC2017 KAs, we assigned a maturity level to each university per KA based on KU coverage thresholds c.f. figure 4.

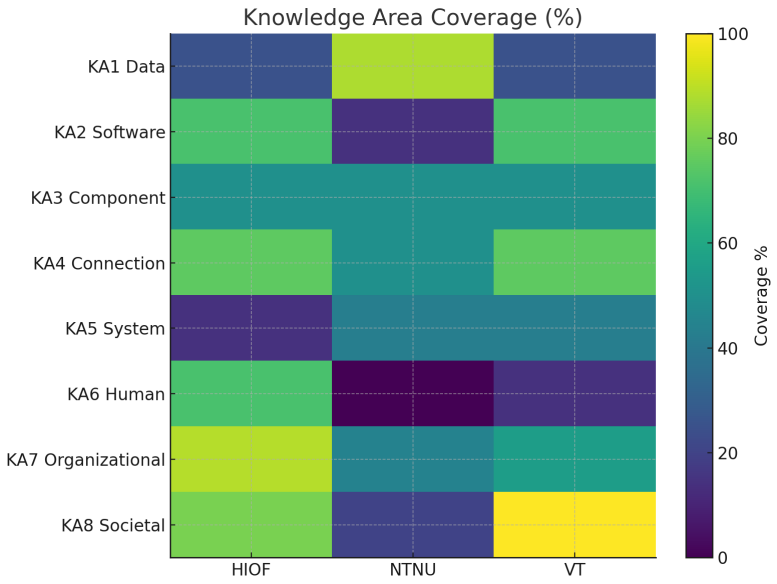

Fig. 4. KAs Coverage

Key outcomes:

– **HIOF**: *Operational* in KA2 Software Security, KA4 Connection Security, KA6 Human Security, KA7 Organizational Security, KA8 Societal Security; *Awareness* in KA5 System Security; *Evolving* in KA1 Data Security and KA3 Component Security.

- **NTNU**: *Operational* in KA1 Data Security; *Evolving* in KA3, KA4, KA5, KA7; *Awareness* in KA2 and KA8; *Initial* in KA6 Human Security.
- **VT**: *Sustainable* in KA8 Societal Security (all KUs covered); *Operational* in KA2 Software Security and KA4 Connection Security; *Evolving* in KA1, KA3, KA5, KA7; *Awareness* in KA6.

Example — KA1: Data Security. KA1 comprises eight KUs: *Cryptography, Digital Forensics, Data Integrity & Authentication, Access Control, Secure Communication Protocols, Cryptanalysis, Data Privacy, Information Storage Security.* Based on our mapping:

- **NTNU** attains *Operational* (7/8 KUs), with broad coverage spanning cryptography, digital forensics, integrity/authentication, access control, secure protocols, cryptanalysis, and privacy.
- **HIOF** is *Evolving* (2/8 KUs), covering cryptography and data privacy.
- **VT** is *Evolving* (2/8 KUs), primarily through cryptography and cryptanalysis.

KA1 illustrates uneven maturity across institutions: NTNU provides a deep and balanced portfolio, while HIOF and VT offer only partial exposure. This gap is actionable: NTNU's existing modules could be leveraged to help HIOF and VT expand into missing KUs such as Digital Forensics, Access Control, and Secure Communication Protocols.
Conclusion from KA1. A targeted, cross-institutional uplift strategy—sharing syllabi, co-developing labs, and aligning assessments—would likely move HIOF and VT from *Evolving* toward *Operational* in Data Security, while also promoting greater curricular coherence across the three universities.

5.3 Knowledge Unit (KU) strengths and gaps

At KU granularity, several strengths and gaps emerge consistently across HIOF, NTNU, and VT (triangulated from the KA/KU mappings above).

Cross-site strengths (Sustainable when aggregated). Risk Management and *Security Program Management* (KA7) reach **Sustainable** when aggregating across sites: all three universities offer at least one relevant course. Other KUs trending strong include *Cryptography* (KA1), *Common System Architectures* (KA5), *Network Architecture* and *Network Services* (KA4), and *Cybercrime* (KA8).

Systematic gaps (Initial or low Awareness).

- **KA1 Data Security**: *Information Storage Security* is **Initial** (no mapped courses at any site). Meanwhile, *Digital Forensics*, *Data Integrity & Authentication*, *Access Control*, and *Secure Communication Protocols* sit at **Awareness** (covered by only one university); *Cryptanalysis* and *Data Privacy* are **Evolving**.

- **KA6 Human Security**: *Identity Management* and *Usable Security & Privacy* remain **Initial** overall. HIOF provides **Awareness** or better for personal compliance/awareness/behavioural privacy, but NTNU is **Initial** for the KA and VT is **Awareness**.
- **KA5 System Security**: *System Access*, *System Control*, and (in cross-site aggregation) *System Retirement* are **Initial**; *System Testing* is **Awareness** (NTNU only); *Common System Architectures* is **Sustainable**.

Methodological note on thresholds. We apply KU category thresholds as follows: *Initial* (0%), *Awareness* (≥20%), *Evolving* (≥50%), *Operational* (≥80%), *Sustainable* (100%). With $n = 3$ universities, the ≥80% threshold can conflate with 100%. To avoid a ceiling effect, we report *Sustainable* only when all three universities cover the KU, and interpret *Operational* pragmatically as "broad, near-universal coverage" (i.e., 2/3 or 3/3, depending on rounding policy). Results here explicitly label *Sustainable* when all three are covered.

Deep-dive example (Initial) — KA1 *Information Storage Security* **Finding:** The KU *Information Storage Security* is **Initial**—no mapped courses at HIOF, NTNU, or VT. This is striking given the maturity of adjacent KUs (e.g., *Cryptography* is Sustainable and *Data Privacy* is Evolving). The gap likely persists because storage topics are implicitly assumed to be "covered" in OS, databases, or crypto courses, yet explicit outcomes around storage-specific risk and assurance (e.g., key custody for at-rest encryption, data remanence, sanitization, storage-level access mediation, and privacy-by-design in data stores) are not assessed.

Desired KU coverage (syllabus topics).

- **Disk and file encryption:** hardware vs. software encryption, full-disk vs. file-level, key hierarchy and escrow, secure key storage (TPM/HSM), performance impacts.
- **Data erasure & remanence:** overwriting, degaussing, crypto-erase, physical destruction; SSD-specific wear leveling and implications.
- **Data masking & tokenization:** test data provisioning, privacy-preserving transformations, format-preserving encryption, reversibility trade-offs.
- **Database security:** authentication/authorization paths, row/column-level security, auditing, query-level redaction, app-mediated access, ORMs and pitfalls.
- **Data security law & governance:** mapping to GDPR/PII/PHI, retention/minimization, lawful basis for processing, records of processing, DPIA; linkage to KA7/KA8.

Leverage existing strengths (short bridge from current catalog).

- **NTNU** already runs strong KUs in KA1 (cryptography, forensics, access control) and KA5 (system security). A 2–3 ECTS "*Information Storage Security*" add-on can reuse crypto labs (key mgmt.), forensics (data remanence), and systems (filesystems, LVM, ZFS).

- **HIOF** has KA2/KA4 strengths (software & networks) and KA8 coverage (policy). A storage security module can anchor in software engineering (secure configuration, decommissioning) and databases (SQL/DBMS security).
- **VT** has OS and software security depth: extend OS labs to include LUKS/BitLocker/FileVault comparisons, SELinux/AppArmor policy snippets, DB row/column security, and crypto-erase benchmarking.

Minimal uplift plan (to move from Initial → Evolving within one cycle).

1. **Create one focused module (2–3 ECTS) at <u>two</u> universities** (any two of HIOF/NTNU/VT) covering the five topics above; include at least three hands-on labs:
   - Lab 1: *Full-disk vs. file-level encryption* (TPM-backed keys, recovery flows, performance measurement).
   - Lab 2: *Sanitization on SSDs vs. HDDs* (simulate wear-leveling; contrast wipe, crypto-erase, and physical destruction policies).
   - Lab 3: *DB security* (implement row/column-level access, audit trails, masking/tokenization for test data).
2. **Assessment:** short design memo (policy + threat model), lab reports with reproducible artifacts (scripts/configs), and a viva on compliance mapping (GDPR data minimization/retention).
3. **Governance integration:** align outcomes with KA7 (*Security Program Management*) and KA8 (*Privacy/Cyber Law*) to ensure organizational traceability (e.g., retention schedules, DPIA excerpts).

Targets and indicators.

- **Coverage target:** move to **Evolving** (2/3 universities) within one academic year; optionally aim for **Sustainable** (3/3) in the next cycle.
- **Learning KPIs:** $\geq$80% of students can (i) implement at-rest encryption with secure key mgmt., (ii) select correct sanitization method per medium, (iii) configure DB security features to pass a simple audit checklist.
- **Program KPIs:** at least one capstone or thesis per site applies the KU to a real system (e.g., storage security posture review); inclusion of storage-specific controls in internal course security checklists.

The KA1 landscape shows **depth in cryptography but shallow coverage in storage-specific assurance**. Elevating *Information Storage Security* closes a high-impact, frequently audited gap (key custody, sanitization, masking) and improves the *defense-in-depth* story across KA1, KA5 (systems), KA7 (program management), and KA8 (privacy/law). Practically, this raises HIOF/VT from *Evolving* toward *Operational* in KA1 and consolidates NTNU's KA1 leadership.

5.4 Cross-institution lift opportunities

The maturity matrix points to explicit peer-learning paths: NTNU can lift KA6 (Human Security) from *Initial* by leveraging HIOF's *Operational* coverage; HIOF can raise KA5 (System Security) with input from NTNU/VT; VT can consolidate KA8's *Sustainable* status while seeking support from HIOF/NTNU to elevate KA2/KA4 toward *Sustainable*.

6 Qualitative Discussion: Case Study

Numeric indicators were complemented by narrative evaluation of website transparency, IT versus OT emphasis, and emerging needs such as ethics, privacy, and human factors

6.1 Website transparency and course documentation

Course-catalogue usability varies markedly. NTNU's site offers the most structured, versioned course pages (history, learning outcomes, workload, assessments, timetable), HIOF provides clear semester-grouped pages with detailed sections (learning outcomes, workload, evaluation, literature), while VT's catalogue tends to shorter heterogeneous descriptions with detail for some courses but less uniformity. These differences affect how easily external reviewers can verify mappings and triangulate KU coverage.

6.2 IT vs. OT orientation and security emphasis

All three institutions emphasize IT-centric security, with OT/critical-infrastructure elements present but uneven. For instance, NTNU lists courses spanning management, risk, systems, networks, and ethical hacking (e.g., IMT4113/4115/4129; TTM4536), HIOF anchors core topics around information/data security (ITL27019, ITF15019, ITF25019), and VT contributes both foundational security (ACIS 4684; CS/ECE 5560; BIT 4614) and policy/technology linkages (GIA 5454; UAP 5564).

6.3 Interdisciplinarity, policy, and ethics reach

VT exemplifies breadth beyond CS/EE through business (BIT 46xx series) and School of Public & International Affairs offerings (e.g., SPIA 4374, GIA/PAPA courses), arguing for multi-department pipelines to meet workforce needs. The analysis also highlights ethics topics (e.g., autonomy/robot ethics, ethical hacking, normative frameworks) as part of societal security literacy that programmes should surface explicitly.

6.4 Actionable focus areas

Two clusters merit near-term attention across universities: (i) human-centred security (identity management; usable security/privacy; awareness/behavioural privacy) where HIOF's practice can inform peers, and (ii) system-lifecycle KUs (system access/control/retirement) to avoid architectural blind spots in safety-critical domains. Targeted course modules or cross-listed electives can close these gaps efficiently.

7 Conclusions and Future Work Directions

This study presented a transparent, standards-aligned methodology for evaluating cybersecurity curricula across institutions by mapping courses to CSEC2017 knowledge units and interpreting coverage through a maturity rubric. The approach highlights curricular strengths, gaps, and peer-learning opportunities in a way that is replicable and scalable to broader contexts. Several limitations should be noted. First, coverage metrics were not weighted by course credits. While this simplifies cross-institutional comparison, it may obscure the relative intensity of coverage, particularly given structural differences between Norway and US degree programs. Second, courses that mentioned cybersecurity topics without assessable learning outcomes were excluded from mapping. This avoided artificially inflating coverage but may understate peripheral or emerging areas. Third, the reliability of coding is shaped by the coders' backgrounds. We recommend establishing a pool of four to five coders, balancing engineering and social science expertise, to strengthen validity. Finally, course descriptions may not fully represent actual delivery, the maturity rubric inherits thresholds from a single reference model, and the findings reflect only three universities, which limits generalizability. Relatedly, the comparison includes only three universities. This constrains the breadth of inference but provides a useful proof of concept for the method. Expanding the analysis to more institutions, ideally all Norwegian universities, would improve external validity and practical value. Future work should extend the framework in several directions. Automated KU mapping using natural-language processing could reduce manual effort and coder subjectivity. Maturity assessment could be broadened to include teaching quality and student learning outcomes, not just coverage. Expanding the institutional sample would also support stronger generalization and cross-regional benchmarking. In addition, aligning analyses with established references would strengthen validity and comparability: relate curricula to the NICE Workforce Framework for Cybersecurity [13], update mapping to the 2020 ACM Cybersecurity Curriculum Guidelines [14], and incorporate the ECSO Minimum Reference Curriculum [15].

Acknowledgments. The authors would like to thank our colleagues, Vasileios Gkioulos, Ahmed Walid Amro, and Mary Ann Lundteigen at NTNU, Ricardo Colomo-Palacios at HiØ, and Nathan Lau at Virginia Tech for providing course information through the shared template and their support. This research is funded by the Research Council of Norway (RCN) in the INTPART program, under the project "Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway-US Partnership (RECYCIN)", with the project number #309911.

References

[1] Francois Goupil et al. "Towards Understanding the Skill Gap in Cybersecurity". In: *Proceedings of the 27th Annual Conference on Innovation and*

Technology in Computer Science Education (ITiCSE '22). New York, NY, USA: ACM, 2022. DOI: 10.1145/1122445.1122456.

[2] Jan Vykopal et al. "Cybersecurity Study Programs: What's in a Name?" In: *Proceedings of the 56th ACM Technical Symposium on Computer Science Education (SIGCSE TS 2025)*. Pittsburgh, PA, USA, 2025. DOI: 10.1145/3641554.3701976.

[3] Mathew Erickson and Philip Kim. "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning". In: *Issues in Information Systems* 22.4 (2021), pp. 9–20. DOI: 10.48009/4_iis_2021_9-21.

[4] Norwegian University of Science and Technology (NTNU). *Norwegian University of Science and Technology Home Page*. https://www.ntnu.edu/. Accessed: 2025-09-17. 2025.

[5] Østfold University College (HIOF). *Østfold University College Home Page*. https://www.hiof.no/english/. Accessed: 2025-09-17. 2025.

[6] Virginia Tech (VT). *Virginia Tech Home Page*. https://www.vt.edu/. Accessed: 2025-09-17. 2025.

[7] RECYCIN Working Group. *Gap Analysis with 3 Universities: Internal Dataset*. Technical Report. Unpublished. 2023.

[8] ACM and IEEE Computer Society. *Cyber Security Curricula 2017: Curriculum Guidelines for Cybersecurity Degree Programs*. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf. Accessed: 2025-06-20. 2017.

[9] Stephen Marshall and Geoff Mitchell. "An e-learning maturity model". In: *Proceedings of the 19th Annual Conference of the Australian Society for Computers in Learning in Tertiary Education, Auckland, New Zealand*. 2002, pp. 8–11.

[10] Mauricio Solar, Jorge Sabattin, and Victor Parada. "A maturity model for assessing the use of ICT in school education". In: *Journal of Educational Technology & Society* 16.1 (2013), pp. 206–218.

[11] Gordon R Middleton. "A maturity model for intelligence training and education". In: *American Intelligence Journal* 25.2 (2007), pp. 33–45.

[12] Working Knowledge CSP. *Community of Practice Maturity Model*. https://workingknowledge-csp.com/wp-content/uploads/CoP_Maturity_Model_v1.pdf. Accessed: 2025-06-20. 2014.

[13] National Initiative for Cybersecurity Education (NICE). *NICE Workforce Framework for Cybersecurity (NICE Framework)*. https://niccs.cisa.gov/tools/nice-framework. NIST/CISA. 2020.

[14] ACM CCECC. *Cybersecurity Curricular Guidance for Associate-Degree Programs (2020)*. https://ccecc.acm.org/guidance/cybersecurity. Association for Computing Machinery, 2020.

[15] European Cyber Security Organisation (ECSO). *Minimum Reference Curriculum for Cybersecurity, Version 3.0*. Tech. rep. ECSO, 2022. URL: https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf.