ISSN 2356-5462
https://journals.telkomuniversity.ac.id/ijoict

Intl. Journal on ICT
Vol. 12, No. 1, Jun 2026. pp. 78-91
doi.org/10.21108/ijoict.v12i1.10605

Developing a CIS Framework-Based Training Syllabus for Venture Capital Firms: A Competency-Driven Approach

Jandika Triindra Burhan[1*], Farisya Setiadi[2], Rio Guntur Utomo[3]

[1-3]*School Of Computing, Telkom University*
Jl. Telekomunikasi No. 1, Sukapura Kec, Dayeuhkolot Kabupaten Bandung, Jawa Barat 40257

[*]jandika.triindra@gmail.com

Abstract

The purpose of this study is to develop and validate a role-based cybersecurity training syllabus for Venture Capital (VC) firms using the CIS Critical Security Controls v8.1 (Implementation Group 1) and an Outcome-Based Education (OBE) approach grounded in a cybersecurity-adapted Training Needs Assessment (TNA) framework. A mixed-method design was employed. In the qualitative phase, interviews with IT personnel and senior management were conducted to identify dominant cybersecurity risks in VC environments. In the quantitative phase, a structured survey was distributed to VC employees to assess the relevance, clarity, and applicability of the proposed syllabus. Content validity was evaluated through expert judgment using the Content Validity Ratio (CVR), while employee acceptance and internal consistency were examined using Cronbach's Alpha. The results show that the most critical risks in VC firms are low security awareness, phishing threats, and compliance-related vulnerabilities. Three CIS IG1 controls—Security Awareness Training, Malware Defenses, and Incident Response Management—were prioritized as core content. The final syllabus integrates these controls into role-specific learning outcomes and assessment strategies aligned with OBE principles. Validation results indicate strong expert agreement and high employee acceptance, supporting the syllabus as relevant, understandable, and suitable for implementation in VC firms.

Keywords: Cybersecurity Training, CIS Controls, Venture Capital, Risk Mitigation, Outcome-Based Education (OBE), Training Need Assessment (TNA), Content Validity Ratio, Cronbach's Alpha.

I. INTRODUCTION

THE rapid digital transformation in financial and investment sectors has increased organizational dependency on digital infrastructure and cloud-based collaboration. This reliance also expands exposure to cybersecurity threats such as phishing [1], ransomware [2], and social engineering attacks that exploit human and procedural weaknesses [3]. In practice, these threats are particularly impactful when daily operations depend on fast, trust-based information exchange and when security responsibilities are distributed across non-specialist roles. As a result, cybersecurity readiness in investment-oriented organizations needs to be approached not only as a technical safeguard, but also as an operational discipline supported by consistent workforce capability development.

Venture capital (VC) firms represent a context where cybersecurity risk is amplified by organizational constraints. Although VC firms handle sensitive investment and business information, they often operate with lean IT capacity and limited dedicated cybersecurity resources, resembling small and medium-sized enterprises (SMEs) in terms of workforce structure and governance maturity [4], [5]. Studies on SMEs consistently report

Received on 28 Jan 2026. Revised on 31 Mar 2026. Accepted and Published on 26 Jun 2026.

practical barriers such as limited technical expertise, constrained budgets, and uneven policy enforcement, which collectively hinder adoption of mature cybersecurity governance practices and increase vulnerability to recurring cyber incidents [4], [5], [6]. These constraints shape an environment where security controls may exist in fragmented form, implementation becomes ad-hoc, and employee awareness remains inconsistent across functions.

VC firms differ from conventional SMEs or general service organizations because their daily operations depend heavily on rapid, trust-based exchange of highly sensitive external information during deal sourcing, due diligence, portfolio monitoring, and investor coordination activities. VC firms routinely handle confidential artifacts such as startup financial reports, cap tables, investment agreements, product roadmaps, and investor-related documents through cloud-based collaboration platforms, shared drives, and email communication [7]. These interactions often involve multiple external parties, including founders, co-investors, legal advisors, and limited partners (LPs), creating a cybersecurity environment characterized by high-frequency data sharing, distributed access points, and elevated confidentiality requirements. Within the Indonesian context, particularly in VC firms operating under SOE-linked or regulated investment ecosystems, cybersecurity readiness also carries governance and compliance implications because organizations are expected to maintain stronger protection of sensitive digital assets and investor-related information [8].

In resource-constrained organizations, adopting comprehensive cybersecurity management frameworks can be difficult, not because their guidance is irrelevant, but because implementation requires sustained governance overhead and specialized roles that smaller teams rarely possess. Empirical work on SME cybersecurity management highlights the continuing gap between framework-level expectations and operational feasibility, motivating the need for approaches that are incremental, actionable, and compatible with limited staffing [6], [9]. Without such feasibility, cybersecurity initiatives tend to remain at the policy level rather than being translated into day-to-day behaviors, leaving human-factor vulnerabilities—such as unsafe handling of digital access, weak security practices, and delayed reporting—insufficiently addressed.

One practical implication is that organizational capability development becomes more realistic when approached through structured internal upskilling rather than through cybersecurity headcount expansion. This orientation is aligned with the broader SME literature that positions scalable governance models and operationally grounded controls as necessary for environments with limited security specialization [6], [9]. A workforce-focused approach is also supported by evidence that compliance behavior and violation patterns are strongly linked to organizational practices and employee conduct, implying that strengthening awareness and role accountability can improve security posture in a measurable way [10]. Therefore, a structured training syllabus can function as an operational mechanism to standardize essential competencies, support onboarding and continuity, and clarify role responsibilities in daily security practices.

Several cybersecurity governance frameworks have been widely adopted to strengthen organizational security posture, including NIST Cybersecurity Framework (NIST CSF), ISO/IEC 27001, COBIT, and SME-oriented risk management models [6], [11]. NIST CSF and ISO/IEC 27001 provide comprehensive governance structures and risk-management guidance; however, their implementation often requires extensive documentation, mature governance processes, and dedicated cybersecurity personnel, which may exceed the operational capacity of lean organizations such as VC firms [6]. Similarly, COBIT emphasizes enterprise-wide governance and control alignment, but its implementation complexity may limit practical adoption in organizations with constrained technical resources and shared operational responsibilities [11]. Recent SME-oriented cybersecurity studies therefore increasingly emphasize scalable, modular, and operationally feasible approaches that can be implemented incrementally without requiring large-scale organizational restructuring [6], [9].

To ensure feasibility under limited capacity, this study positions the CIS Critical Security Controls v8.1 Implementation Group 1 (IG1) as a baseline control set suitable for organizations with constrained resources, and uses it as the technical backbone for training design [12]. CIS IG1 is relevant because it supports a prioritized, prescriptive, and implementable set of safeguards that can be mapped directly into practical training content. Evidence from applied cybersecurity auditing work indicates that CIS-aligned approaches can support organizational readiness when integrated with complementary governance perspectives [11]. In parallel, cybersecurity awareness training models emphasize that training programs should not remain generic, but should strengthen job-relevant skills and behaviors that reflect operational duties and risk exposure [10], [13].

Based on this logic, the study develops a role-based cybersecurity training syllabus tailored for VC firms by translating prioritized CIS IG1 safeguards into structured training modules. The syllabus is designed to reduce

exposure to key human-factor vulnerabilities while remaining realistic under lean staffing conditions, and it is validated using expert judgment and employee evaluation to ensure content relevance and practical acceptability. In addition, the study recognizes that cybersecurity incidents can influence investor-related perceptions and interest in a firm, reinforcing the strategic importance of improving cybersecurity readiness within investment-oriented environments [8]. The resulting contribution is a validated training model that aligns foundational CIS controls with the operational realities of VC firms and supports organizational readiness for cybersecurity risk mitigation.

This study contributes theoretically by extending the discussion on cybersecurity governance in VC environments through the integration of CIS IG1, competency-based learning, and organizational cybersecurity readiness. Methodologically, the study contributes by combining Training Needs Analysis (TNA), thematic risk analysis, CIS control prioritization, role-based mapping, and OBE principles into a structured mixed-method development framework. Practically, the study provides a validated cybersecurity training syllabus designed specifically for lean VC organizations operating under resource constraints, governance requirements, and multi-functional operational structures.

II. LITERATURE REVIEW

The cybersecurity risk landscape relevant to VC firms is shaped by both the evolution of external threats and VC-specific operational exposure. Phishing remains a dominant entry vector that exploits human and procedural weaknesses [1], ransomware continues to disrupt organizations through encryption and extortion [2], and social engineering expands exposure by targeting trust-based interactions rather than purely technical vulnerabilities [3]. VC work amplifies these risks because deal sourcing and due diligence require frequent exchange of high-sensitivity artifacts (e.g., pitch decks, cap tables, financial models, and roadmaps) through email, cloud drives, and shared data rooms [7]. The time-critical and relationship-driven nature of these exchanges elevates confidentiality and access-control risks and positions cybersecurity as an operational assurance mechanism embedded in investment workflows [7]. Cyber incidents may also generate reputational and relational consequences, including impacts on investor interest, extending beyond technical recovery considerations [8].

Despite handling sensitive information, VC firms commonly exhibit cybersecurity maturity patterns similar to resource-constrained small and medium-sized enterprises (SMEs) due to lean staffing and limited dedicated security capacity [4], [5]. SME-oriented evidence consistently highlights constraints such as limited in-house expertise, budget limitations, and unclear governance responsibilities, which hinder adoption of mature frameworks and weaken consistent enforcement of security practices [4], [5], [6]. In practice, this gap often manifests as fragmented controls, uneven policy adherence, and difficulty translating high-level guidance into repeatable day-to-day behaviors [4], [5].

To address feasibility limitations, recent literature increasingly emphasizes simplified and implementable cybersecurity governance approaches. Meta-analytic evidence indicates that effective SME risk management requires aligning information-security systems with organizational capability through pragmatic, scalable practices rather than high-overhead frameworks [6]. Operationally grounded models such as CyberTOMP seek to manage asset-focused cybersecurity across levels of execution, yet complexity can remain challenging for non-specialist environments [9]. Complementary SME-oriented contributions propose specialized risk assessment tools and cost-effective governance models that prioritize practicality, contextual fit, and implementable strategies under limited resources [14], [15].

Within this constraint, the CIS Controls v8.1—particularly IG1—provide an actionable baseline for organizations with limited cybersecurity capacity [12]. CIS IG1 offers a prescriptive, prioritized set of safeguards that supports incremental implementation and translation into concrete organizational practices [12]. Applied work suggests that CIS-aligned assessments can be strengthened by integrating complementary governance perspectives (e.g., NIST structures and COBIT-based control thinking) to support readiness assessment and improvement planning [11]. For VC firms, implementability is essential because controls must be executable across roles that may not include dedicated security specialists; accordingly, CIS IG1 is positioned as both operationally feasible and "training-friendly," enabling safeguards to be mapped into role-specific competencies and daily work practices [11], [12], [13].

Because high-impact incidents in resource-constrained settings frequently involve human-factor vulnerabilities, the literature emphasizes training, awareness, and compliance behavior as key determinants of cybersecurity posture. Awareness and compliance studies indicate that security outcomes are closely tied to organizational practices and employee conduct, supporting capability development as a governance mechanism rather than an optional educational add-on [10], [13]. Intelligence-sharing research similarly highlights difficulties in translating cybersecurity concepts into actionable steps, reinforcing the need for structured, role-relevant learning that enables consistent implementation capability [16].

Role and competency frameworks provide additional grounding for accountability-based training design. The European Cybersecurity Skills Framework (ECSF) supports role definitions and capability expectations for cybersecurity functions [17], while Indonesia's national ICT occupation map provides auditable role–competency alignment through standardized occupational units [18]. CyBOK further contributes a structured body of cybersecurity knowledge areas to support curriculum framing and content categorization [19]. To ensure training translates into measurable capability outcomes, Outcome-Based Education (OBE) emphasizes explicit learning outcomes and assessment evidence rather than content coverage [20]. Measurability can be strengthened using the revised Bloom's taxonomy to formulate outcomes across levels of cognitive demand [21], while constructive alignment ensures consistency between outcomes, learning activities, and assessment tasks [22]. Adult learning principles further support scenario-based, problem-centered learning that aligns with real work responsibilities and constraints in professional settings [23].

Human-factor vulnerabilities in cybersecurity are closely associated with inconsistent security behavior, varying levels of employee awareness, and the absence of standardized operational practices across organizational roles [10], [13]. In lean VC environments, employees frequently manage sensitive digital interactions, including document sharing, investor communication, and access-related activities, without formal cybersecurity specialization. Consequently, cybersecurity risks may persist even when governance policies or technical safeguards are already established, because operational implementation remains dependent on individual behavior and organizational culture [10]. Prior studies therefore emphasize that competency-based and role-oriented training approaches are necessary to reinforce consistent cybersecurity practices and strengthen organizational readiness in resource-constrained environments [13].

Synthesizing these streams, three gaps remain salient for VC-oriented cybersecurity training design. First, most SME-oriented models are not explicitly tailored to VC operational characteristics, particularly confidentiality demands and trust-based, time-critical multi-party information exchange [7], [8]. Second, many studies emphasize frameworks and risk assessment, yet fewer translate controls into a competency-based syllabus with measurable outcomes and aligned assessment evidence [14], [15], [20]. Third, while CIS IG1 provides an implementable baseline for resource-constrained organizations [9], limited guidance exists on systematically mapping prioritized safeguards to VC job roles and structuring them into an outcome-based syllabus aligned with role accountability, governance needs, and workforce feasibility [18], [24].

Compared with broader cybersecurity governance frameworks such as NIST CSF, ISO/IEC 27001, and COBIT, CIS IG1 provides a more operationally focused and prioritized baseline that is easier to translate into daily security practices and competency-based learning activities for lean organizations [12], [18] . While larger frameworks emphasize extensive governance structures, documentation processes, and enterprise-wide risk management, CIS IG1 concentrates on essential safeguards with high impact and lower implementation complexity, particularly for organizations with limited cybersecurity personnel and constrained operational resources [12]. This characteristic makes CIS IG1 more suitable for addressing human-factor vulnerabilities in VC environments, where cybersecurity implementation must remain practical, scalable, and aligned with multi-functional organizational roles.

Existing studies on cybersecurity governance primarily focus on technical framework implementation, organizational audits, or general awareness programs within SMEs and large enterprises [6], [12]. Other studies discuss cybersecurity awareness practices and OBE principles, yet fewer explicitly translate cybersecurity controls into competency-based syllabus structures with measurable outcomes and aligned assessment evidence [13], [17]. In the VC context, limited research specifically addresses how cybersecurity controls can be operationalized into role-based learning outcomes aligned with lean organizational structures, governance responsibilities, and resource constraints. Therefore, this study extends prior approaches by integrating CIS IG1, TNA, and OBE principles into a validated cybersecurity training syllabus specifically tailored for VC operational environments. Unlike prior studies that primarily emphasize technical implementation or general awareness initiatives, this study integrates CIS IG1 prioritization, role-based mapping, TNA adaptation, and

OBE principles into a VC-oriented competency-based cybersecurity training syllabus with measurable organizational learning outcomes.

III. RESEARCH METHOD

A. Research Design

This study applied an exploratory sequential mixed-method design to develop and validate a CIS IG1-based cybersecurity training syllabus for VC firms, combining qualitative exploration of contextual risks with quantitative control prioritization and acceptance assessment for triangulation [21]. TNA was adapted to VC operations through organizational, task, and role analyses: organizational analysis identified VC-specific cyber risks and governance challenges; task analysis prioritized CIS Controls v8.1 (IG1) based on perceived importance and implementation difficulty; and role analysis mapped prioritized controls to VC job roles using Indonesia's national ICT occupation framework (KOMDIGI) [9], [23]. Extending conventional TNA, OBE was used to translate prioritized needs into measurable learning outcomes, aligned assessments, and training modules, positioning the syllabus as a role-based competency mechanism rather than a one-off awareness activity [15], [17].

TABLE I
RESEARCH DESIGN OVERVIEW

Element	Description
Approach	Mixed Method
Type of Design	Exploratory (Sequential)
Sampling Method	Probability Sampling (Survey) & Purposive Sampling (Interview)
Data Collection Method	Quantitative: Survey Qualitative: Interview & Expert Feedback
Target Audience	IT Team, Senior Management, and Stakeholders in VC firms
Data Collection Procedures	Quantitative: Reliability and Validity Test Qualitative: Thematic Analysis
Data Analysis Strategy	Quantitative: Content Validity Ratio Qualitative: Thematic coding, categorizing insight and aligning with CIS Controls.

Table I provides an overview of the adopted research design, which applies an exploratory sequential mixed-method approach to support both contextual understanding and empirical validation [12]. Surveys provide the quantitative component, while interviews and expert feedback refine syllabus relevance. The design targets key VC role groups (IT teams, senior management, and general employees) and integrates quantitative assessment (e.g., CVR) with qualitative coding aligned to CIS controls to ensure the syllabus is methodologically sound and feasible for lean VC environments.

B. Research Process

The research process comprised six interconnected phases forming a sequential yet iterative pathway. It started with problem understanding (preliminary findings, research objectives/problem statement, and literature review), progressed to design outputs (risk identification, CIS control prioritization, and role mapping), and concluded with validation through expert judgment and end-user evaluation. This structure ensured that each phase addressed the research questions and that outputs from earlier phases directly informed subsequent steps.

TABLE II
RESEARCH PHASES, METHODS, AND OUTPUTS

Phase	Main Activity	Method/Approach	Key Output
Phase 1	Identification of VC cybersecurity risks	Interviews and thematic analysis	Key cybersecurity risk themes
Phase 2	Prioritization of CIS IG1 controls	Stakeholder survey and quartile analysis	Prioritized CIS controls
Phase 3	Mapping CIS controls to organizational roles	KOMDIGI occupation mapping	Role–control alignment
Phase 4	Development of cybersecurity training syllabus	OBE-based syllabus design	Initial syllabus structure
Phase 5	Expert validation and refinement	CVR analysis and expert feedback	Refined and validated syllabus
Phase 6	Employee acceptance and feasibility evaluation	Cronbach's Alpha reliability analysis	Acceptance and feasibility findings

Table II operationalizes the study framework by explicitly linking each research phase with its corresponding methods and outputs, thereby maintaining alignment between CIS Controls, OBE principles, VC operational constraints, and the final validated syllabus. Early exploration through interviews and document review identified common VC realities—including lean technical staffing, shared responsibilities, inconsistent cybersecurity practices, phishing exposure, and weak access-control behavior—which refined the problem definition toward a structured, role-based, and resource-feasible cybersecurity training syllabus for VC environments.

C. Instrumentation and Data Collection

Instrumentation and data collection followed the exploratory sequential mixed-method design, where qualitative findings informed quantitative prioritization and validation. Instruments were derived from the research objectives, VC context, and prioritized CIS IG1 controls to directly support syllabus development and evaluation [15], [21]. Qualitative data were collected through semi-structured interviews with IT personnel and senior management to capture cybersecurity challenges, risk perceptions, and current practices; thematic patterns (e.g., phishing exposure, low awareness, weak controls, and governance gaps) were used to shape the survey and training content [22], [25]. Quantitative data were gathered using two questionnaires: (1) a CIS-oriented prioritization survey measuring perceived importance, implementation level, and implementation difficulty of CIS IG1 controls via Likert-type items [26]; and (2) a post-expert-review syllabus validation survey assessing clarity, role relevance, practicality, and usefulness, adapted from prior structured cybersecurity questionnaire studies to fit VC roles and CIS IG1 objectives [27], [28]. For end-user acceptance, after a readability test, the final online questionnaire was administered to employees of one of Indonesia's top three VC firms; 48 of 56 invited participants completed responses. Items were aligned with Program Learning Outcomes (PLOs) to evaluate perceived relevance, clarity, and applicability of the syllabus.

Although data were collected from individual employees and organizational representatives, the proposed framework and syllabus function as organizational-level interventions. Employee insights informed the identification of cybersecurity realities, barriers, and role-specific needs, which were synthesized into outputs such as competency mapping, policy-aligned learning outcomes, and training recommendations. The study engaged multiple VC firms during risk assessment, with feasibility evaluation conducted in one of Indonesia's top three VC firms within an SOE-linked ecosystem

D. Data Analysis

1) Quantitative Analysis: Quantitative data were analyzed using descriptive statistics and prioritization procedures (ranking and quartile computation) to identify high-priority CIS controls. These results informed syllabus construction and were cross-checked with qualitative insights for contextual fit. For syllabus validation, Content Validity Ratio (CVR) was used to quantify expert and employee agreement on the relevance, clarity, and applicability of syllabus components, following recent methodological guidance for instrument evaluation [29]. Reliability of the acceptance instrument was assessed using Cronbach's Alpha across PLO constructs, where acceptable-to-good values indicated internal consistency [30].

2) Qualitative Analysis: Interview data were analyzed using thematic coding to identify key cybersecurity challenges and organizational constraints. Emergent themes were mapped to CIS Controls to ensure alignment between practitioner needs and the prioritized safeguards, supporting syllabus content and structure.

3) Integration of Findings: Quantitative and qualitative results were integrated through triangulation to cross-validate statistical prioritization with thematic evidence, strengthening credibility and ensuring operational relevance for VC settings.

IV. RESULTS AND DISCUSSION

A. Phase 1 – Identification of Key Cybersecurity Risks in VC Firms

Phase 1 focuses on identifying the primary cybersecurity risks and challenges faced by VC firms through semi-structured interviews with IT teams, senior management, and selected staff from investment and operations divisions. Interviews were complemented by internal cybersecurity documents and secondary industry references, then coded using thematic analysis and visualized to support risk prioritization.

Fig. 1 Tree Map Thematic Coding

Fig. 4 visualizes the frequency and relationship among coded themes from interview transcripts. The largest thematic clusters relate to data protection (9 references), awareness of cybersecurity importance (9 references), and the need for basic cybersecurity awareness programs (8 references). Other frequently mentioned risks include phishing attacks, data leaks, and compliance obligations from parent companies or external auditors. These findings indicate that VC firms experience more challenges related to awareness and governance than to infrastructure or technical configurations.

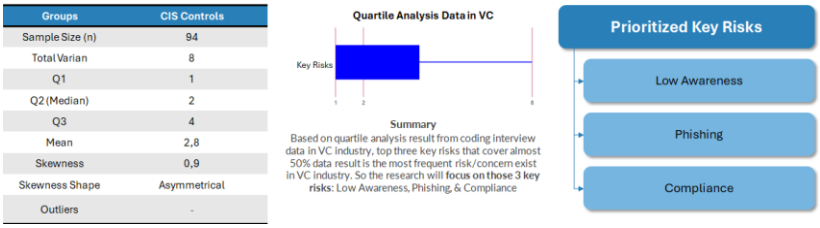


Fig. 2 Quartile Analysis Data in VC Industry and Prioritized Key Risk

Fig. 5 presents quartile analysis applied to the frequency distribution of eight risk variants. The results show Q2 (Median) = 2, Q3 = 4, Mean = 2.8, and skewness = 0.9, indicating an asymmetrical distribution dominated by specific recurring risks. The top quartile (Q3–Q4) covers nearly 50% of total coded data and concentrates on three primary risk categories: Low Awareness, Phishing, and Compliance. The integrated interpretation highlights that low awareness reflects insufficient understanding of cybersecurity principles and weak engagement with awareness initiatives; phishing vulnerability reflects recurring incidents and unsafe email practices; and compliance gaps reflect difficulties in maintaining alignment with cybersecurity audits, data protection regulations, and external stakeholder requirements.

B. Phase 2 – Survey and Prioritization of CIS Controls

Phase 2 aims to validate and quantify Phase 1 findings through a structured stakeholder survey distributed online to participants across multiple industries, including VC firms and SMEs. A total of 128 participants were invited, and 96 valid responses were collected; responses were then filtered to the VC context, resulting in 28 complete responses from multiple VC firms.

Fig. 6 summarizes VC-filtered responses to the survey question, “Which of the following cybersecurity controls is the hardest to implement in your company?” The figure is intended as an explanatory visual summary

of perceived implementation difficulty (Survey Question Q31). Survey results show varied maturity across the 18 CIS controls: controls related to asset inventory and secure configuration were generally rated as implemented, while controls involving human awareness, malware protection, and incident response were consistently perceived as the hardest to implement. These findings reinforce the need for role-based cybersecurity capability development, particularly in awareness, malware defense, and incident-response practices, which later became the primary focus areas of the proposed syllabus.

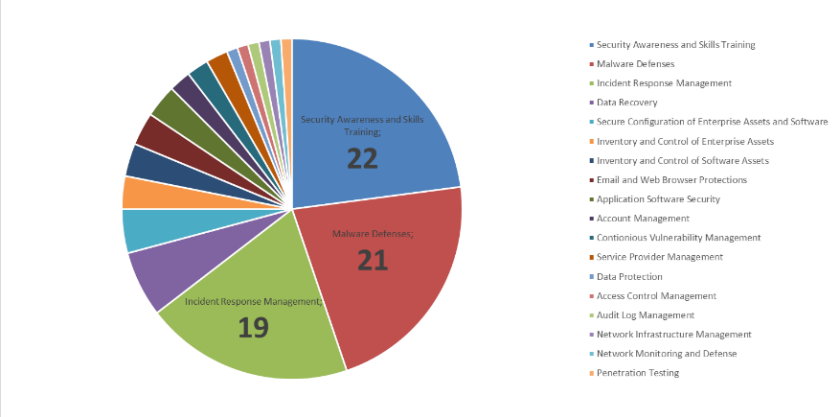
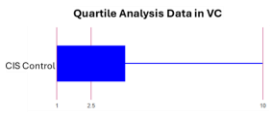


Fig. 3 Survey Result of the Hardest-to-Implement CIS Controls v8.1 (IG1) within VC Firms

Groups	CIS Controls
Sample Size (n)	96
Total Varian	18
Q1	1
Q2 (Median)	2,5
Q3	4
Mean	3,1
Skewness	1,3
Skewness Shape	Asymmetrical
Outliers	11, 11, 12, 12, 13, 14, 15, 16, 17, 18



Summary

Based on quartile analysis result from survey data in VC industry, top three controls that cover almost 65% survey result is the hardest to implement in VC industry. So the research will **focus on those 3 controls:** Security Awareness and Skills Training, Malware Defenses, & Incident Response Management

Fig. 4 Quartile Analysis Data in VC Industry and Prioritized CIS Controls v8.1 (IG1)

Fig. 7 reports quartile distribution to evaluate frequency of each control's difficulty rating. The analysis indicates 18 control variants with Q2 (Median) = 2.5, Q3 = 4, Mean = 3.1, and skewness = 1.3, confirming an asymmetrical distribution in which a small subset of controls is cited disproportionately as difficult. Based on quartile segmentation, approximately 65% of survey responses clustered around three controls in the upper quartile (Q3–Q4), establishing the priority set for syllabus development.

TABLE III
PRIORITIZED CIS CONTROLS V8.1 (IG1)

Priority Rank	CIS Controls	Category	Description
1	Controls 14	Security Awareness and Skills Training	Ensures employees receive ongoing, role-specific cybersecurity education and practical skills.
2	Controls 10	Malware Defenses	Focuses on detecting, preventing, and responding to malware through automated tools and user vigilance.
3	Controls 17	Incident Response Management	Establishes capabilities for detecting, reporting, and mitigating incidents while ensuring compliance and recovery.

Table II presents the top three prioritized controls: Control 14 (Security Awareness and Skills Training), Control 10 (Malware Defenses), and Control 17 (Incident Response Management), including their categories and descriptions. The thesis interpretation confirms that this prioritization validates Phase 1 findings and directly aligns with key risks identified earlier—Low Awareness, Phishing Vulnerability, and Compliance Gaps—therefore establishing an empirical basis for focused training design. The prioritization results indicate that VC cybersecurity challenges are strongly associated with human-factor exposure, operational awareness gaps, and response preparedness rather than solely technical infrastructure limitations.

C. *Phase 3 – Mapping CIS Controls to Organizational Roles*

Phase 3 translates the three prioritized CIS controls into actionable responsibilities across VC roles by adopting the ICT Occupation Map published by KOMDIGI (2023), ensuring alignment with nationally recognized job functions. Each control was decomposed into sub-safeguards and matched to suitable occupational categories (e.g., Cybersecurity Analyst, System Administrator, Information Security Awareness Officer, Incident Response Team Manager). The mapping also accounts for lean and multi-functional VC teams, where safeguards may overlap between IT and senior management responsibilities.

TABLE IV
CONDENSED CIS IG1–ROLE–COMPETENCY MAPPING

CIS IG1 Control	Primary Role(s)	Competency Outputs (concise)	Policy/SOP Artifacts (concise)
Control 14: Security Awareness and Skills Training	Senior Management, IT/Admin	Identify phishing/social engineering cues; apply safe handling for deal documents; follow reporting/escalation procedures; demonstrate basic secure behaviour compliance	Security Awareness Policy; Phishing Reporting SOP; Acceptable Use & Email/Cloud Sharing Guidelines; Onboarding security checklist
Control 10: Malware Defenses	IT/Admin	Configure endpoint protection (AV/EDR) baseline; patch/update cadence; safe software installation and macro controls; respond to suspected malware per playbook	Endpoint Protection Standard; Patch & Update SOP; Software Installation Policy; Malware Response Playbook
Control 17: Incident Response Management	Senior Management, IT/Admin	Classify incidents; execute notification workflow; preserve evidence at basic level; coordinate containment and recovery; conduct post-incident review and improvements	Incident Response Policy; IR Roles & RACI; Incident Triage & Escalation SOP; Post-Incident Review Template; Contact tree / communication plan

In this study, prioritized CIS IG1 controls were mapped to organizational roles and translated into competency outputs and supporting governance artifacts to ensure feasibility in a lean VC context; detailed mapping covered CIS sub-safeguards 14.1–14.8, 10.1–10.3, and 17.1–17.3 and is summarized at control-level for publication compactness [12], [20], [21].

D. *Phase 4 – Development of CIS Framework-Based Training Syllabus*

Phase 4 develops the initial CIS IG1-based training syllabus by translating the prioritized controls into role-based modules within an OBE structure. The syllabus integrates anti-malware management, security awareness, and incident response competencies into a single curriculum framework, organized into two role categories: IT Team modules and Senior Management modules.

TABLE V
HIGH-LEVEL ROLE-BASED OBE SYLLABUS

Module / CIS IG1 Control	Target Role	CLO (single-line; Sub-CLO merged)	Assessment (single-line)	Hours
M1 – Security Awareness & Skills (CIS 14)	All staff; Senior Mgmt; IT/Admin	Demonstrate secure handling of VC deal artifacts by recognizing phishing/social engineering cues, applying safe email/cloud sharing practices, and executing the reporting/escalation workflow in routine operations.	Scenario-based quiz + phishing simulation response + short SOP compliance checklist	3 Hours
M2 – Malware Defenses (CIS 10)	IT/Admin; Power users	Apply malware prevention controls by configuring baseline endpoint protection, enforcing safe software/macro practices, and performing patch/update routines aligned with operational constraints.	Hands-on configuration checklist + case-based incident identification exercise	3 Hours
M3 – Incident Response Management (CIS 17)	Senior Mgmt; IT/Admin	Execute a basic incident response process by classifying incidents, conducting triage/escalation, supporting containment/recovery steps, and completing a post-incident review to propose improvements.	Tabletop exercise + IR form completion (triage log, comms, PIR template)	4 Hours

To meet page constraints while preserving the OBE logic, the final syllabus is presented as a high-level role-based structure where sub-outcomes are consolidated into a single measurable CLO per module. Each CLO is constructively aligned with scenario-based assessments and operational artifacts to provide evidence of role performance rather than content exposure [23]–[26].

E. Phase 5 – Expert Validation and Feedback Analysis

Phase 5 evaluates the draft syllabus through structured expert judgment to ensure relevance, clarity, and alignment with VC operational realities. Four cybersecurity experts meeting Indonesian National Qualifications Framework (KKNI) Level 7 or higher participated, with complementary backgrounds spanning cybersecurity consulting, IT governance and control implementation, and curriculum development. This composition was applied to reduce validation bias by ensuring technical, governance, and educational review perspectives.

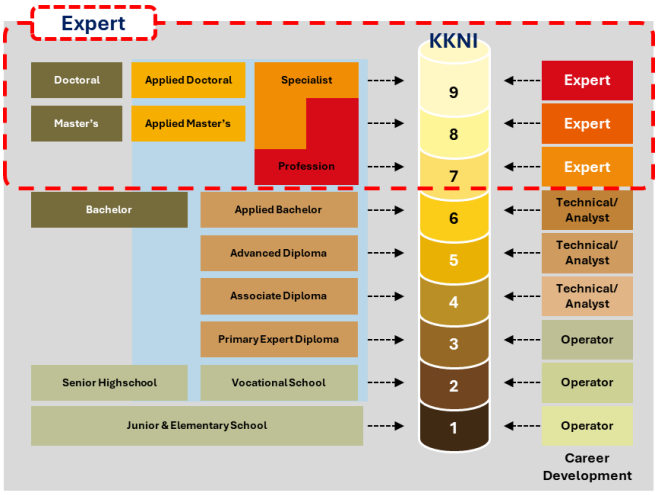


Fig. 5 Expert Definition based on Indonesia KKNI

Fig. 8 presents the expert definition and eligibility framing used for validation, emphasizing KKNI Level 7 (or equivalent) as a minimum requirement and highlighting the complementary expertise composition supporting credibility of expert judgment.

TABLE VI
CVR RESULT OF SYLLABUS ITEMS

	Expert1	Expert2	Expert3	Expert4	n_e	N	CVR
Alignment with CIS Controls	3	3	2	3	3	4	0,5
Mapping with KOMDIGI Occupation Map	3	2	3	3	3	4	0,5
Relevance of Function Role Responsibilities	2	3	3	3	3	4	0,5
Program Learning Outcomes (PLO)	3	3	3	3	4	4	1
Course Learning Outcomes (CLO)	3	3	3	2	3	4	0,5
Learning Objectives (Sub-CLO)	3	3	3	2	3	4	0,5
Assessment Method	3	3	3	3	4	4	1
Training Hours Allocation	3	2	3	3	3	4	0,5
PLO, CLO, and Sub CLO Coherence	3	3	3	3	4	4	1
Technical Feasibility in VC Environment	3	3	3	3	4	4	1
Relevance to VC Organization Context	3	3	3	3	4	4	1
Clarify of Language and Structure	3	3	3	3	4	4	1
Learning Domain Balance	3	2	3	3	3	4	0,5
Innovation and Practicality	3	3	3	3	4	4	1
Overall Necessity	3	3	3	3	4	4	1

Each item was rated as essential, useful but not essential, or not necessary, and CVR values were calculated using Lawshe's formula. All syllabus items achieved positive CVR values, with several reaching the maximum CVR score, indicating strong agreement among experts regarding item necessity. Items with lower but positive CVR values were interpreted as relevant but requiring refinement in wording, scope, or instructional emphasis rather than elimination. These results indicate that the proposed syllabus components were considered substantively relevant and necessary by the expert panel, supporting the content validity of the developed training structure [29]. The CVR results demonstrate strong expert agreement regarding the relevance, structural coherence, and practical applicability of the proposed syllabus components within VC operational contexts.

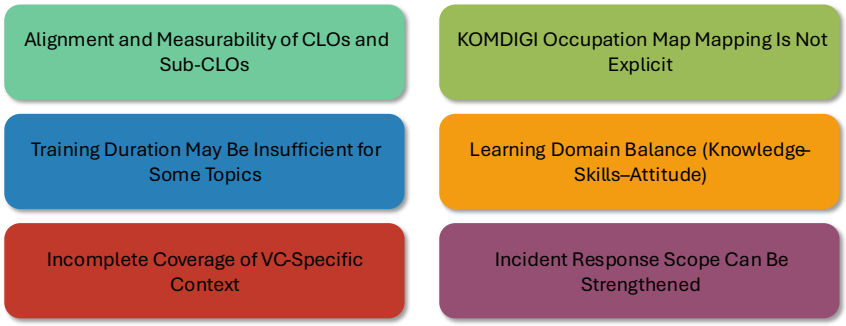


Fig. 6 Summarize of Expert Feedback

Fig. 9 synthesizes qualitative expert feedback into six dominant themes: (1) measurability limitations in some CLOs/Sub-CLOs, requiring reformulation into observable behaviors; (2) KOMDIGI mapping not sufficiently explicit, requiring clearer occupational-code linkage; (3) training duration concerns, particularly for awareness and incident response modules; (4) need for stronger balance across learning domains, including attitude/behavior indicators; (5) incomplete coverage of VC-specific operational contexts (outsourced IT risks, investment/analyst functions, crisis communication, secure handling of confidential deal information); and (6) recommendations to strengthen incident response scope through realistic scenarios, decision exercises, and readiness assessments.

F. Phase 6 – VC Employee Acceptance and Feasibility Evaluation

Phase 6 evaluates employee-level acceptance, feasibility, and internal consistency after expert validation and syllabus refinement. A readability test was conducted prior to distribution, resulting in minor wording adjustments to reduce ambiguity. The finalized questionnaire was distributed online to employees of one of the top three VC firms in Indonesia, selected due to high investment activity and governance maturity (117 investments, 46 as lead investor, 14 exits including five IPOs) within an SOE ecosystem with higher regulatory and compliance requirements. Of 56 invited participants, 48 completed the survey.

TABLE VII
CRONBACH'S ALPHA INTERPRETATION SCALE

Criteria (Value)	Interpretation
< 0,50	Unacceptable
> 0,50	Poor
> 0,60	Questionable
> 0,70	Acceptable
> 0,80	Good
> 0,90	Excellent
> 0,95	Too High

Cronbach's Alpha values below 0.70 indicate insufficient internal consistency and suggest that measurement items may require revision. Values from 0.70 to 0.95 indicate acceptable-to-good reliability, while values above 0.95 are considered problematic due to potential item redundancy.

All evaluated PLOs achieved Cronbach's Alpha values above 0.77, indicating acceptable to good internal consistency. Several PLOs (10.2, 10.3, 14.1, 14.2, 14.3, 14.5, 14.7, and 17.1) achieved good reliability ($\alpha > 0.80$), while remaining PLOs achieved acceptable reliability ($\alpha \geq 0.70$). No construct fell below the acceptable threshold and no alpha exceeded 0.95, indicating that items are neither inconsistent nor redundant. The obtained Cronbach's Alpha values, which predominantly fall within the acceptable-to-good range, indicate consistent participant responses across PLO dimensions and support the internal reliability of the proposed syllabus evaluation instrument [30].

TABLE VIII
EMPLOYEE ACCEPTANCE RESULT WITH CRONBACH'S ALPHA METHOD

PLO	CA Score	CA Interpretation
PLO 10.1 – Endpoint Security Policy and Device Control	0,77762	Acceptable
PLO 10.2 – Endpoint Protection Implementation	0,83121	Good
PLO 10.3 – Endpoint Maintenance and Updates	0,83455	Good
PLO 14.1 – Phishing and Social Engineering Awareness	0,86469	Good
PLO 14.2 – Secure Authentication Practices	0,82269	Good
PLO 14.3 – Secure Data Handling and Privacy	0,84919	Good
PLO 14.4 – Preventing Unintentional Data Exposure	0,77500	Acceptable
PLO 14.5 – Incident Recognition and Reporting	0,82853	Good
PLO 14.6 – Identifying Missing Security Updates	0,78175	Acceptable
PLO 14.7 – Secure Network Connectivity	0,82240	Good
PLO 17.1 – Incident Communication and Coordination	0,83110	Good
PLO 17.2 – Incident Reporting Processes	0,76759	Acceptable
PLO 14.8 – Cybersecurity Awareness Program Governance	0,81470	Good
PLO 17.3 – Incident Leadership and Business Continuity	0,78804	Acceptable

The validated syllabus also provides a practical foundation for future implementation within VC organizational environments. Potential implementation strategies may include pre–post competency assessments, phishing simulation exercises, incident-response drills, and periodic behavioral evaluation to measure improvements in cybersecurity awareness and operational readiness over time. Because the syllabus is structured using role-based learning outcomes and governance-aligned competency mapping, organizations may also integrate the training into internal compliance programs, onboarding activities, and continuous security-awareness initiatives to strengthen long-term cybersecurity culture and accountability.

V. CONCLUSION

This study concludes that cybersecurity capability development in VC firms requires a contextual, role-based, and resource-aware approach rather than generic training. Findings show that CIS Controls v8.1 IG1 can be translated into practical training outcomes through role mapping and OBE, reducing gaps between governance expectations and daily practices in lean VC environments. Combining expert judgment and employee evaluation provides a credible basis for assessing contextual appropriateness. Positive validation and consistent employee responses confirm that the proposed syllabus is conceptually sound and practically usable, offering a validated model that integrates governance, technical controls, and human behavior to strengthen cybersecurity readiness in resource-constrained investment organizations.

VC firms are recommended to adopt the syllabus as a foundational training framework by prioritizing role-specific modules on awareness, malware prevention, and incident response, and integrating training outcomes into broader risk management and compliance mechanisms. Industry associations and regulators may also consider this model as a reference for standardized training guidance for investment-driven or SME-oriented organizations due to its scalable, resource-aware design. Future research should strengthen empirical evidence through implementation-based studies (e.g., pre–post tests, longitudinal observation, phishing simulations, and incident-reporting indicators), expand external validity by replication across different VC types and governance models, and improve methodological robustness by comparing alternative prioritization methods (e.g., AHP) and validation techniques (e.g., Delphi, Cohen's Kappa, or Krippendorff's Alpha) to refine decision-making and confidence in syllabus evaluation.

REFERENCES

[1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, no. March, pp. 1–23, 2021, doi: 10.3389/fcomp.2021.563060.

[2] H. T. Neprash *et al.*, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," *JAMA Heal. Forum*, vol. 3, no. 12, p. E224873, 2022, doi: 10.1001/jamahealthforum.2022.4873.

[3] W. Syafitri, Z. Shukur, U. M. I. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention : A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[4] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cyber security of Small-to-Medium businesses : Challenges , research focus and recommendations A Survey on the Cyber Security of Small-to-Medium Businesses : Challenges , Research Focus and Recommendations," *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[5] M. Antunes, M. Maximiano, and R. Gomes, "Information Security and Cybersecurity Management : A Case Study with SMEs in Portugal," *J. Cybersecurity Priv.*, vol. 1, no. 2, pp. 219–238, 2021.

[6] K. AL-Dosari and N. Fetais, "Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach," *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173629.

[7] F. Kolini and L. Janczewski, "Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review," *Commun. Assoc. Inf. Syst.*, vol. 50, no. 1, pp. 86–121, 2022, doi: 10.17705/1CAIS.05004.

[8] K. C. Demek and S. E. Kaplan, "Cybersecurity breaches and investors' interest in the firm as an investment," *Int. J. Account. Inf. Syst.*, 2023, doi: 10.1016/j.accinf.2023.100616.

[9] D. D. Manuel, J. Carmona-Murillo, D. Cortes-Polo, and F. J. Rodriguez-Perez, "CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels," *IEEE Access*, vol. 10, no. November, pp. 122454–122485, 2022, doi: 10.1109/ACCESS.2022.3223440.

[10] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review," *Soc. Sci.*, vol. 11, no. 9, 2022, doi: 10.3390/socsci11090386.

[11] V. Fadila, N. Mutiah, and R. P. Sari, "Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 8, no. 2, p. 271, 2023, doi: 10.24114/cess.v8i2.43257.

[12] Center for Internet Security (CIS), "CIS Critical Security Controls v8.1: Implementation Groups," 2024.

[13] P. Nair, "Enhancing Cybersecurity Awareness Training through the NIST Framework," *IJARCCE*, 2023, doi: 10.17148/ijarcce.2023.121203.

[14] ENISA, *European Cybersecurity Skills Framework (ECSF) User Manual*. 2022.

[15] Kominfo, "Peta Okupasi TIK Nasional. Kementerian Komunikasi dan Informatika Republik Indonesia," 2023.

[16] CyBOK, "Introduction to CyBOK Knowledge Areas," *Cyber Secur. Body Knowl.*, p. 22, 2021, [Online]. Available: www.cybok.org

[17] R. M. Harden, "Outcome-based education: The future is today," *Med. Teach.*, vol. 29, no. 7, pp. 625–629, 2007, doi: 10.1080/01421590701729930.

[18] L. W. Anderson and D. R. Krathwohl, "Lorin W. Anderson, David R. Krathwohl - A taxonomy for learning teaching and assessing: a revision of Bloom`s taxonomy of educational objetives - Complete edition," *Longman*, 2001.

[19] J. Biggs, "Enhancing teaching through constructive alignment Thinking about teaching and learning," *High. Educ.*, vol. 32, no. 347, pp. 347–364, 1996.

[20] M. S. Knowles, E. F. Holton, P. A. Robinson, and C. Caraccioli, *THE ADULT LEARNER: The Definitive Classic in Adult Education and Human Resource Development, TENTH EDITION*. 2024. doi: 10.4324/9781003387671.

[21] J. W. Creswell and V. L. P. Clark, *Designing and Conducting Mixed Methods Research.* Sage Publications, 2018.
[22] S. Kvale, "Doing Interviews: Conducting an Interview," *Methods*, 2007.
[23] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, 2006, doi: 10.1191/1478088706qp063oa.
[24] K. S. Issa, *Factors Affecting The Adoption Of Electronic Procurement Among Public Procuring Entities In Tanzania. A case of TANESCO.* 2020.
[25] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.
[26] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert Scale: Explored and Explained," *Br. J. Appl. Sci. Technol.*, vol. 7, no. 4, pp. 396–403, 2015, doi: 10.9734/bjast/2015/14975.
[27] F. Gioulekas *et al.*, "A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures," *Healthcare*, vol. 10, no. 327, pp. 1–19, 2022.
[28] S. Landolt, J. Hirschel, T. Schlienger, W. Businger, and A. M. Zbinden, "Assessing and Comparing Information Security in Swiss Hospitals," *Interact. J. Med. Res.*, vol. 1, no. 2, p. e11, 2012, doi: 10.2196/ijmr.2137.
[29] M. Romero Jeldres, E. Díaz Costa, and T. Faouzi Nadim, "A review of Lawshe's method for calculating content validity in the social sciences," *Front. Educ.*, vol. 8, no. November, pp. 1–8, 2023, doi: 10.3389/feduc.2023.1271335.
[30] D. George and P. Mallery, *IBM SPSS Statistics 29 Step by Step*. 2024. doi: 10.4324/9781032622156.