

Supplementary Materials

Legal Literacy, AI Risk Perception, and Digital Safety in UAE Universities:

Testing a Trust-Calibrated Vigilance Model

Dataset Documentation, Statistical Summary, Survey Instrument, and Scoring Guide

Analytic sample: $N = 710$
Role distribution: 300 students; 200 faculty members; 210 administrative/professional staff
Data files: `CALTV_dataset.xlsx`; `CALTV_dataset.sav` (same dataset, two formats)
Software documented: IBM SPSS Statistics 29.0; IBM SPSS Amos 29.0

Contents

Part I. Dataset Documentation and Scoring Guide	1
1 Contents of the Supplementary Materials	1
2 Dataset Structure	1
2.1 Variable Dictionary	1
3 Scoring Conventions	2
Part II. Statistical Summary of the Dataset	3
4 Descriptive Statistics	3
5 Reliability Analysis (Cronbach's α)	3
6 Construct-Level Correlations (Pearson)	4
7 Role-Based Comparisons	4
7.1 One-way ANOVA (Students vs. Faculty vs. Administrative/Professional staff)	4
7.2 Welch tests (Students vs. Employees)	4
8 Measurement Model (CFA)	5
8.1 Standardized subscale loadings	5
8.2 Composite reliability and discriminant validity	5
9 Structural Model (SEM)	5
9.1 Direct effects	5
9.2 Standardized indirect effects (bootstrap, 95% CI)	6
9.3 Standardized total effects on digital safety behaviors	6
Part III. Survey Instrument	7
A. Legal Literacy (LL): Compliance Architecture	7
B. AI-Enabled Cyber Risk Perception (RP): Threat Appraisal	8
C. Multi-Layer Trust (T): Calibration Gate	8
D. Vigilance / Verification Norms (V): Translation Layer	9
E. Digital Safety Behaviors (DSB): Outcome Index	10
F. Governance Conditions	10

Part I. Dataset Documentation and Scoring Guide

1 Contents of the Supplementary Materials

The supplementary materials for this article consist of one documentation file (the present PDF) together with two data files, as listed below. The two data files contain the *same* 710 scale-level records and are provided in two formats for convenience; they are not separate datasets.

- **Supplementary File S1** — **CALTV_Supplementary_Materials.pdf** (this document): data dictionary, scoring guide, statistical summary tables, and the full survey instrument.
- **Supplementary File S2** — **CALTV_dataset.xlsx**: the scale-level dataset ($N = 710$) with an accompanying variable-label worksheet.
- **Supplementary File S3** — **CALTV_dataset.sav**: the identical dataset in IBM SPSS Statistics format.

2 Dataset Structure

The scale-level dataset contains one record per respondent. The role variable is coded as 1 = student, 2 = faculty member, and 3 = administrative/professional staff. The dataset contains complete scale-level observations for the focal constructs documented below.

2.1 Variable Dictionary

Table 1: Variable names, labels, and score ranges.

Variable	Label	Coding or range
ID	Respondent identifier	1–710
Role	Institutional role	1 = student; 2 = faculty; 3 = administrative/professional staff
LLK	Objective legal-literacy knowledge	0–6
LL_R	Rights literacy	5–25
LL_O	Obligations literacy	5–25
LL_P	Procedural literacy	6–30
RP_S	Perceived risk severity	5–25
RP_V	Perceived vulnerability	5–25
RP_AI	AI-enabled credibility amplification	6–30
T_inst	Institutional trust	7–35
T_AI	Technology/AI trust	6–30
T_over	Overreliance indicator, scored in the trust-total direction	5–25
V_norm	Normative vigilance	8–40
V_beh	Behavioral vigilance	8–40
DSB_AA	Authentication and access hygiene	5–25
DSB_IH	Information handling and data minimization	6–30
DSB_VRR	Verification, resistance, and reporting	7–35
GC	Governance clarity	6–30
ENF	Enforcement	5–25
LL_total	Overall legal-literacy score	16–86
RP_total	Overall AI risk-perception score	16–80
T_total	Overall trust score	18–90
V_total	Overall vigilance score	16–80
DSB_total	Overall digital-safety-behavior score	18–90
GOV_total	Overall governance-conditions score	11–55

3 Scoring Conventions

- Agreement items use a five-point scale: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree.
- Frequency items use a five-point scale: 1 = never, 2 = rarely, 3 = sometimes, 4 = often, and 5 = always, referring to the preceding eight weeks.
- Objective legal-knowledge items are scored dichotomously: 1 = correct and 0 = incorrect.
- The overreliance items are reverse-keyed before the trust subscale and overall trust score are formed, so that higher stored scores indicate more calibrated trust.
- Construct totals are formed as follows:

$$\begin{aligned}
 LL_{\text{total}} &= LLK + LL_R + LL_O + LL_P, \\
 RP_{\text{total}} &= RP_S + RP_V + RP_{AI}, \\
 T_{\text{total}} &= T_{inst} + T_{AI} + T_{over}, \\
 V_{\text{total}} &= V_{norm} + V_{beh}, \\
 DSB_{\text{total}} &= DSB_{AA} + DSB_{IH} + DSB_{VRR}, \\
 GOV_{\text{total}} &= GC + ENF.
 \end{aligned}$$

Part II. Statistical Summary of the Dataset

4 Descriptive Statistics

Table 2: Descriptive statistics for subscales and construct totals ($N = 710$).

Measure	Range	N	M	SD	Mdn	Skew	Kurt
Legal literacy knowledge (LL-K)	0–6	710	3.75	1.21	4.0	-0.21	-0.07
Rights literacy (LL-R)	5–25	710	17.24	3.73	17.0	-0.07	-0.18
Obligations literacy (LL-O)	5–25	710	17.22	3.67	17.0	-0.08	-0.11
Procedural literacy (LL-P)	6–30	710	20.57	4.38	20.0	-0.08	0.0
Overall legal literacy (LL total)	16–86	710	58.78	11.95	58.0	-0.05	-0.08
Risk severity (RP-S)	5–25	710	17.19	3.61	17.0	-0.13	-0.16
Risk vulnerability (RP-V)	5–25	710	17.11	3.52	17.0	-0.1	-0.13
AI amplifiers (RP-AI)	6–30	710	20.66	4.15	21.0	-0.13	-0.11
Overall AI risk perception (RP total)	16–80	710	54.97	10.66	55.0	-0.11	-0.08
Institutional trust (T_inst)	7–35	710	24.18	5.0	24.0	-0.06	-0.44
Technology/AI trust (T_AI)	6–30	710	20.72	4.26	21.0	-0.08	-0.12
Overreliance (T_over)	5–25	710	17.53	3.15	18.0	-0.14	0.06
Overall trust (T total)	18–90	710	62.43	6.65	63.0	-0.05	-0.36
Normative vigilance (V_norm)	8–40	710	27.61	5.62	28.0	-0.19	-0.18
Behavioral vigilance (V_beh)	8–40	710	27.66	5.48	28.0	-0.1	-0.31
Overall vigilance (V total)	16–80	710	55.27	10.81	56.0	-0.15	-0.25
Adoption/avoidance (DSB-AA)	5–25	710	17.43	3.56	17.0	-0.08	-0.02
Information hygiene (DSB-IH)	6–30	710	20.78	4.1	21.0	-0.1	-0.15
Verification & reporting (DSB-VRR)	7–35	710	24.18	4.77	24.0	-0.07	-0.01
Overall digital safety behaviors (DSB total)	18–90	710	62.38	11.85	62.0	-0.09	-0.05
Governance clarity (GC)	6–30	710	20.77	3.92	21.0	-0.1	-0.15
Enforcement (ENF)	5–25	710	17.25	3.17	17.0	-0.13	-0.17
Overall governance conditions	11–55	710	38.02	6.4	38.0	-0.06	-0.25

Note. Skew = skewness; Kurt = excess (Fisher) kurtosis. All $|\text{skew}| < 1$ and $|\text{kurtosis}| < 1$, indicating approximately normal univariate distributions consistent with maximum-likelihood estimation.

5 Reliability Analysis (Cronbach's α)

Table 3: Internal-consistency reliability across subscale indicators.

Construct	No. of indicators	Cronbach α
Legal literacy (LL-R, LL-O, LL-P)	3	0.974
AI risk perception (RP-S, RP-V, RP-AI)	3	0.938
Trust (T_inst, T_AI, T_over reverse-scored)	3	0.777
Vigilance (V_norm, V_beh)	2	0.946
Digital safety behaviors (DSB-AA, DSB-IH, DSB-VRR)	3	0.942

Note. Overreliance (T_over) was reverse-scored within the trust construct so that higher scores reflect more calibrated trust.

6 Construct-Level Correlations (Pearson)

Table 4: Pearson product-moment correlations among focal constructs ($N = 710$).

	LLK	LL	RP	T	V	DSB	GC	ENF
LLK	1							
LL	0.400**	1						
RP	0.109**	0.300**	1					
T	0.091*	0.263**	0.249**	1				
V	0.133**	0.396**	0.293**	0.373**	1			
DSB	0.162**	0.388**	0.298**	0.214**	0.424**	1		
GC	0.079*	0.268**	0.245**	0.690**	0.287**	0.195**	1	
ENF	0.040	0.187**	0.240**	0.643**	0.281**	0.164**	0.623**	1

Note. LLK = legal-literacy knowledge; LL = legal literacy; RP = AI risk perception; T = trust; V = vigilance; DSB = digital safety behaviors; GC = governance clarity; ENF = enforcement. * $p < 0.05$; ** $p < 0.01$.

7 Role-Based Comparisons

7.1 One-way ANOVA (Students vs. Faculty vs. Administrative/Professional staff)

Table 5: One-way ANOVA of composite constructs by institutional role.

Measure	F (2, 707)	p	η^2
Legal literacy knowledge	0.05	0.952	0.0001
Legal literacy total	0.45	0.637	0.0013
AI risk perception	1.21	0.299	0.0034
Trust	0.42	0.66	0.0012
Vigilance	0.05	0.953	0.0001
Digital safety behaviors	1.16	0.314	0.0033
Governance clarity	0.08	0.924	0.0002
Enforcement	0.76	0.468	0.0021
Overall governance conditions	0.12	0.89	0.0003

Note. η^2 values at or below 0.005 indicate negligible role-based variance in the composite measures.

7.2 Welch tests (Students vs. Employees)

Table 6: Welch two-sample tests comparing students with employees (faculty + staff).

Measure	M (Stud.)	M (Emp.)	Δ	t	df	p	Hedges g
Legal literacy knowledge	3.77	3.75	0.02	0.22	614.8	0.827	0.02
Legal literacy total	58.96	58.65	0.3	0.33	636.8	0.74	0.03
AI risk perception	55.68	54.44	1.24	1.52	620.3	0.129	0.12
Trust	62.7	62.24	0.46	0.9	638.6	0.366	0.07
Vigilance	55.13	55.38	-0.25	-0.3	648.0	0.762	-0.02
Digital safety behaviors	61.73	62.86	-1.13	-1.24	612.3	0.215	-0.1
Governance clarity	20.83	20.72	0.1	0.35	641.5	0.726	0.03

continued on next page

(continued)

Measure	M (Stud.)	M (Emp.)	Δ	t	df	p	Hedges g
Enforcement	17.21	17.28	-0.07	-0.3	659.6	0.761	-0.02
Overall governance conditions	38.04	38.0	0.03	0.07	644.6	0.948	0.0

Note. Δ = Students – Employees. All tests two-tailed.

8 Measurement Model (CFA)

8.1 Standardized subscale loadings

Table 7: Standardized CFA loadings for subscale indicators.

Construct	Standardized loadings
Legal literacy	LL_R=0.97, LL_O=0.97, LL_P=0.96
AI risk perception	RP_S=0.92, RP_V=0.91, RP_AI=0.92
Trust	T_inst=0.79, T_AI=0.72, T_over=-0.75
Vigilance	V_norm=0.95, V_beh=0.95
Digital safety behaviors	DSB_AA=0.93, DSB_IH=0.93, DSB_VRR=0.92

Note. Overreliance (T_over) is retained as a reverse-oriented indicator of trust and therefore carries a negative standardized loading.

8.2 Composite reliability and discriminant validity

Table 8: Composite reliability, average variance extracted, and discriminant-validity evidence.

Construct	k	CR	AVE	$\sqrt{\text{AVE}}$	Largest r
Legal literacy	3	0.977	0.934	0.967	0.396
AI risk perception	3	0.94	0.84	0.917	0.3
Trust	3	0.795	0.564	0.751	0.373
Vigilance	2	0.946	0.897	0.947	0.424
Digital safety behaviors	3	0.95	0.863	0.929	0.424

Note. CR = composite reliability; AVE = average variance extracted. $\sqrt{\text{AVE}}$ exceeds the largest correlation with another focal construct, supporting discriminant validity (Fornell–Larcker).

9 Structural Model (SEM)

Standardized estimates for the trust-calibrated vigilance pathway. The confirmatory latent model and its global fit indices (χ^2 , CFI, TLI, RMSEA) were estimated in IBM SPSS AMOS 29.0 with subscale-level indicators. The tables below summarize the direct, indirect, and total effects.

9.1 Direct effects

Table 9: Standardized direct effects.

Path	β	SE	CR (t)	p
LL $\rightarrow$ T	0.207	0.037	5.54	< 0.001
RP $\rightarrow$ T	0.187	0.037	5.01	< 0.001
T $\rightarrow$ V	0.373	0.035	10.7	< 0.001
V $\rightarrow$ DSB	0.357	0.037	9.68	< 0.001
RP $\rightarrow$ DSB	0.184	0.035	5.22	< 0.001
T $\rightarrow$ DSB	0.035	0.036	0.96	0.338

Note. β = standardized coefficient. Trust has no statistically reliable direct association with digital safety behaviors, indicating that trust operates through vigilance rather than directly.

9.2 Standardized indirect effects (bootstrap, 95% CI)

Table 10: Standardized indirect effects with bootstrap confidence intervals.

Pathway	β_{ind}	Boot SE	95% CI LL	95% CI UL	p
Trust $\rightarrow$ Vigilance $\rightarrow$ DSB	0.133	0.017	0.1	0.167	< 0.001
AI risk perception $\rightarrow$ DSB (indirect)	0.031	0.009	0.015	0.052	< 0.001
Legal literacy $\rightarrow$ DSB (indirect)	0.035	0.011	0.016	0.061	< 0.001

9.3 Standardized total effects on digital safety behaviors

Table 11: Standardized total effects.

Predictor	β_{tot}	Boot SE	95% CI LL	95% CI UL	p
AI risk perception $\rightarrow$ DSB (total)	0.216	0.034	0.148	0.284	< 0.001
Legal literacy $\rightarrow$ DSB (total)	0.035	0.011	0.016	0.061	< 0.001

Note. Indirect and total effects were estimated with 1,000 nonparametric bootstrap resamples on the dataset; percentile 95% confidence intervals are reported.

Part III. Survey Instrument

Instrument coverage. The sections below present the item wording of the CALT-V instrument. The scenario-based legal-knowledge section lists its six item stems.

Response formats. Agreement items (1–5): 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. Frequency items (1–5): 1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always (time frame: last 8 weeks). Knowledge-check items (A/B/C/D): single best answer; 1 = correct, 0 = incorrect.

A. Legal Literacy (LL): Compliance Architecture

Table 12: Rights Literacy (LL-R) — agreement scale 1–5

Code	Item
LL-R1	I understand what counts as “personal data” in a UAE university context (e.g., ID, grades, contact details).
LL-R2	I understand that individuals may have rights regarding access to or correction of their personal data.
LL-R3	I understand that using personal data beyond the stated purpose can create compliance risk.
LL-R4	I understand that consent (when required) should be specific and not assumed.
LL-R5	I know that privacy protections can apply even when data is shared internally within the university.

Table 13: Obligations Literacy (LL-O) — agreement scale 1–5

Code	Item
LL-O1	I know when it is not appropriate to share student/staff data, even for “urgent” requests.
LL-O2	I understand that data should be shared only with authorized persons and for legitimate purposes.
LL-O3	I understand the principle of data minimization (sharing only what is necessary).
LL-O4	I can distinguish between official requests and suspicious requests for credentials or personal details.
LL-O5	I understand that forwarding personal data through informal channels (personal email/apps) can be noncompliant.

Table 14: Procedural Literacy (LL-P) — agreement scale 1–5

Code	Item
LL-P1	I know the official channel(s) to report phishing, impersonation, or suspected data misuse at my university.
LL-P2	I know what information/evidence to include when reporting a suspicious message (e.g., sender address, link).
LL-P3	I know the correct first steps after I suspect my account has been compromised.
LL-P4	I know where to find the university’s official guidance on data protection and cyber safety.
LL-P5	I understand the difference between reporting to IT/security and reporting to an academic/administrative office.
LL-P6	I know what typically happens after an incident report is submitted (acknowledgment, triage, follow-up).

Table 15: Scenario-Based Legal Literacy (LL-K) — knowledge check, A/B/C/D (1 = correct, 0 = incorrect)

Code	Item
LL-K1	Email claims “IT Support” needs your ID + one-time code to restore access. Best action is...
LL-K2	Colleague asks for a grades sheet via personal messaging app “to be quick.” Safest action is...
LL-K3	Student data used for non-course invitations without clear notice. Most compliant approach is...
LL-K4	After clicking a suspicious link, best first action is...
LL-K5	Most helpful evidence in a phishing report is...
LL-K6	Data minimization means...

B. AI-Enabled Cyber Risk Perception (RP): Threat Appraisal

Table 16: Perceived Severity (RP-S) — agreement scale 1–5

Code	Item
RP-S1	AI-enabled deception can cause serious harm in universities (financial, academic, reputational).
RP-S2	AI-generated phishing can lead to harm even when users think they are careful.
RP-S3	Impersonation of staff/leadership through AI is a serious campus risk.
RP-S4	Deepfake-like messages/calls can create real consequences in university processes.
RP-S5	AI increases the potential scale and impact of cyber incidents compared to traditional scams.

Table 17: Perceived Vulnerability (RP-V) — agreement scale 1–5

Code	Item
RP-V1	People in my university are likely targets for AI-enabled scams.
RP-V2	I personally could be targeted due to routine email/LMS/messaging.
RP-V3	Busy periods (registration/exams) increase my susceptibility to manipulation.
RP-V4	University-related financial/administrative messages are a likely route for deception.
RP-V5	I think AI-enabled deception can bypass normal “common sense” warning signs.

Table 18: AI Credibility-at-Scale Amplifiers (RP-AI) — agreement scale 1–5

Code	Item
RP-AI1	AI makes scam messages look official and professional.
RP-AI2	AI can personalize scams using names/roles/tasks in convincing ways.
RP-AI3	AI can generate messages in fluent language that lowers suspicion.
RP-AI4	AI can automate deception at high volume without obvious patterns.
RP-AI5	AI makes it harder to judge authenticity without verification.
RP-AI6	AI enables realistic impersonation (email/text/voice) that can mislead people who normally verify.

C. Multi-Layer Trust (T): Calibration Gate

Table 19: Institutional Trust (T_inst) — agreement scale 1–5

Code	Item
Tinst1	My university provides clear official channels for cyber/security communications.
Tinst2	I believe cyber incidents are handled competently and promptly.
Tinst3	I trust the university to communicate transparently about digital threats.
Tinst4	I believe reporting an incident will be handled fairly and confidentially.
Tinst5	I trust that the university’s data-handling practices are responsible and controlled.
Tinst6	I believe policy enforcement is consistent (rules apply to everyone).
Tinst7	When the university issues cyber guidance, I consider it credible.

Table 20: Technology/AI Trust (T_AI) — agreement scale 1–5

Code	Item
TAI1	AI-based security tools generally improve safety in university systems.
TAI2	I expect automated security warnings to be useful and reliable.
TAI3	AI assistance helps me identify suspicious messages more effectively.
TAI4	I believe AI tools used in my university are deployed responsibly.
TAI5	I think AI systems can reduce human error in cybersecurity decisions.
TAI6	Overall, I feel comfortable using AI-enabled systems when completing university tasks.

Table 21: Overreliance / Trust-without-Checking (T_over) — agreement scale 1–5 (reverse-scored)

Code	Item
Tover1	If a message looks official, I usually do not need to verify it further.
Tover2	If an AI/security tool marks something as safe, I rarely double-check.
Tover3	I trust university-branded messages enough to act immediately.
Tover4	Verification steps are often unnecessary and slow down work.
Tover5	I assume the system will block most threats, so personal checks are less important.

D. Vigilance / Verification Norms (V): Translation Layer

Table 22: Verification Norms (V_norm) — agreement scale 1–5

Code	Item
Vn1	Sensitive requests should be verified through known official channels before acting.
Vn2	Out-of-band confirmation (call/portal) is normal for credentials or payment requests.
Vn3	Urgency (“act now”) is a warning sign that requires extra verification.
Vn4	It is appropriate to pause and verify even if it delays the task.
Vn5	I consider requests for one-time codes/passwords suspicious even when they look official.
Vn6	Checking sender address/domain is a standard step before clicking links.
Vn7	I verify identity before sharing documents that include personal data.
Vn8	Reporting suspicious messages is a normal responsibility in my university community.

Table 23: Behavioral Vigilance (V_beh) — frequency scale 1–5 (last 8 weeks)

Code	Item
Vb1	Verified a suspicious request using an official portal or a known phone number.
Vb2	Checked the sender address/domain carefully before responding.
Vb3	Avoided clicking a link and instead navigated directly to the official site/LMS.
Vb4	Inspected link destinations (hover/preview) before clicking.
Vb5	Captured evidence (screenshots/sender details) before deleting a suspicious message.
Vb6	Reported suspicious messages to the designated IT/security channel.
Vb7	Refused a request for credentials/payment even though it looked official.
Vb8	Warned colleagues/peers through an official or appropriate internal channel.

E. Digital Safety Behaviors (DSB): Outcome Index

Table 24: Authentication and Access Hygiene (DSB-AA) — frequency scale 1–5

Code	Item
DSB-AA1	I use multi-factor authentication where available.
DSB-AA2	I avoid reusing passwords across accounts.
DSB-AA3	I update passwords when there is a security warning or suspicion.
DSB-AA4	I avoid logging into university accounts on shared/public devices.
DSB-AA5	I log out and do not save credentials on browsers/devices I do not fully control.

Table 25: Information Handling and Data Minimization (DSB-IH) — frequency scale 1–5

Code	Item
DSB-IH1	I share sensitive files only via approved university platforms.
DSB-IH2	I avoid sending personal data through personal email or informal messaging apps.
DSB-IH3	I limit shared data to only what is necessary for the task.
DSB-IH4	I check permissions before sharing links/files (view/edit access).
DSB-IH5	I avoid storing sensitive university data on unmanaged personal devices/services.
DSB-IH6	I delete or archive sensitive files appropriately when they are no longer needed.

Table 26: Verification, Resistance, and Reporting (DSB-VRR) — frequency scale 1–5

Code	Item
DSB-VRR1	I verify identity before acting on requests involving credentials, money, or sensitive data.
DSB-VRR2	I treat unexpected attachments as risky unless verified.
DSB-VRR3	I verify “leadership/IT/finance” messages through official channels.
DSB-VRR4	I report suspicious messages using the official reporting channel.
DSB-VRR5	I follow incident guidance promptly after suspected exposure.
DSB-VRR6	I refuse requests for one-time codes/passwords even when the message looks official.
DSB-VRR7	I keep a record of suspicious messages (evidence) when reporting or escalating.

F. Governance Conditions

Table 27: Governance Transparency and Communication Clarity (GC) — agreement scale 1–5

Code	Item
GC1	Official cyber/security messages are easy to recognize (clear provenance cues).
GC2	The university provides clear instructions about what to do when suspicious messages occur.
GC3	Reporting channels are visible and easy to access.
GC4	Cyber guidance is written in practical language (actionable steps).
GC5	The university communicates threat updates in a timely manner.
GC6	I know where to find the most current official cyber/data guidance.

Table 28: Perceived Enforceability and Accountability (ENF) — agreement scale 1–5

Code	Item
ENF1	Data/privacy rules are enforced consistently across the university.
ENF2	Unsafe handling of personal data has clear consequences.
ENF3	People are held accountable for repeated unsafe digital behavior.
ENF4	Enforcement improves compliance and safety behavior on campus.
ENF5	It is clear who is responsible for cyber/data compliance in different units.

G. Background and Control Variables

The survey also included: role (student / faculty / staff / admin); college or discipline; years at the university; age band; gender (optional); digital intensity (average academic hours per day online); prior cyber-incident experience (yes/no; if yes, type); and prior cyber training in the last 12 months (yes/no).