ISACA MELBOURNE CHAPTER

RESEARCH SERIES Vol. 01 / 2025-26

ISACA Melbourne Chapter

VICTORIAN ENTERPRISE BENCHMARK

Digital Trust Capability Index

DTCI — 2025 / 26 Edition

A quantitative benchmark of digital trust maturity across Victorian enterprises — measuring governance, cybersecurity, risk assurance, emerging technology readiness, and people capability.

PERIOD
October 2025 – March 2026

GEOGRAPHY
Victoria, Australia

RESEARCHERS
Dinesh Dino Velusamy & Reshma Devi

Executive Summary

Key findings from the inaugural DTCI Victorian enterprise survey.

Victorian enterprises demonstrate uneven digital trust maturity — operationally strong in cybersecurity and workforce capability, yet materially underdeveloped in AI governance, enterprise-wide trust strategy, and incident readiness. The composite DTCI score of 65.3 out of 100 positions the cohort in the Developing band, signalling a structural gap between operational controls and strategic digital trust leadership.

Headline metrics

49%
only partially embed digital trust principles into enterprise strategy and governance

51%
have no formal or only informal AI governance — the weakest DTCI dimension surveyed

69%
are not fully prepared to respond to a major digital trust incident

57%
lack an enterprise-wide digital trust framework, operating in domain silos or without policy

56%
of the certified workforce is below 25%, or certifications are not tracked at all

74%
anticipate moderate or significant investment increases in digital trust over the next 12 months

Composite DTCI Score · Victorian Enterprises · 2025

65.3 / 100

DEVELOPING

Defined controls in key domains, but governance fragmentation and AI maturity gaps constrain strategic value creation. Clear uplift pathway exists.

Maturity scale: Nascent · Initial · Developing · Advanced · Leading

Dimension scores

DTCI Dimension	Score (out of 5)	Maturity Band
Cybersecurity	3.37	Defined
Emerging Tech Governance	2.53	Nascent–Initial
People Capability	4.00	Proficient
Trust Governance	3.01	Developing
ERM & Risk Integration	3.41	Defined

SECTION 01

Sample Profile

Senior functional leaders across Victorian enterprises, surveyed October 2025 – March 2026.

51%
From large enterprises (1,000+ FTE)

31%
Hold CISO, CIO/CTO, or C-suite roles

52%
Technology & Finance sectors combined

23%
Self-identify as Digitally Developing maturity

Industry distribution

Sector	Share
Technology	26%
Finance	26%
Utilities / Critical Infrastructure	18%
Other	18%
Healthcare	5%
Government	5%
Engineering	3%

Role / function

Role	Share
Cybersecurity Manager	31%
Other / General Management	21%
CISO	13%
CIO / CTO	10%
GRC Lead	10%
CRO / Risk Officer	8%
Internal Auditor	8%

Organisation size (FTE)

Size band	Share
5,000+	33%
1,000 – 4,999	23%
Less than 100	18%
500 – 999	13%
100 – 499	13%

Self-assessed digital maturity

Self-assessment	Share
Digitally Mature (combined)	54%
Digitally Developing	23%
Digital Leader (combined)	21%
Digital Beginner	3%

Sampling note

The sample is skewed toward large enterprises (56% ≥ 1,000 FTE) and technology-adjacent sectors (Technology + Finance = 52%), and toward cybersecurity/GRC functional roles. Findings are indicative for this cohort and should not be interpreted as population-representative. The 2026 longitudinal study is designed to scale to n≥200 with stratified sampling to enable inferential generalisation.

SECTION 02

Trust Governance

Strategic embedding of digital trust principles, framework adoption, and policy maturity. DTCI dimension score: 3.01/5.

49%
only partially embed digital trust principles into enterprise strategy

57%
operate without an enterprise-wide digital trust framework, or in domain silos

Key finding

Trust governance scores in the Developing band (3.01/5), reflecting a structural gap between operational digital trust controls and enterprise-wide strategic embedding. Approximately half of surveyed organisations have only partial integration of digital trust principles into enterprise strategy, and 57% lack a coordinated framework — operating either in domain silos (cybersecurity, privacy, risk handled separately) or without formal policy.

This dimension is the second-weakest DTCI sub-score and represents the highest leverage point for strategic uplift. Closing the trust governance gap requires Board-level mandate, enterprise architecture alignment, and cross-functional accountability — capabilities that ISACA's CGEIT (Certified in the Governance of Enterprise IT) and CDPSE (Certified Data Privacy Solutions Engineer) credentials are designed to develop.

SECTION 03

Cybersecurity Maturity

Operational cybersecurity capability across detection, response, control deployment, and assurance. DTCI dimension score: 3.37/5.

3.37

Cybersecurity dimension score (out of 5) — Defined band

69%

are not fully prepared to respond to a major digital trust incident

Key finding

Cybersecurity is the second-strongest DTCI dimension after People Capability, scoring 3.37/5 in the Defined band. Victorian enterprises have made measurable investment in foundational cybersecurity controls — perimeter defence, identity management, vulnerability management — and these are operating with documented maturity in most surveyed organisations.

However, the 69% incident readiness gap is the most material operational risk indicator in the survey. Organisations have invested in prevention but have under-invested in response capability, tabletop exercises, and crisis communications. ISACA's CISM (Certified Information Security Manager) and CRISC (Certified in Risk and Information Systems Control) credentials directly address the response readiness gap.

SECTION 04

ERM & Risk Integration

Integration of digital trust risk into enterprise risk management frameworks. DTCI dimension score: 3.41/5.

3.41

ERM Integration dimension score — Defined band

—

Strongest non-People dimension; reflects mature risk discipline in financial services and utilities cohorts

Key finding

ERM Integration is the strongest non-People dimension at 3.41/5, reflecting the sample's overrepresentation of financial services, critical infrastructure, and large-enterprise risk functions where ERM discipline is mature and regulatory-driven. Digital trust risk is increasingly recognised as a first-class enterprise risk category alongside financial, operational, and strategic risk.

The risk management uplift opportunity lies in extending mature ERM discipline to emerging risk categories — AI model risk, third-party AI risk, and supply chain digital trust risk — where existing ERM frameworks are not yet calibrated. CRISC and the AAIR (Advanced in AI Risk) credential are positioned for this evolution.

SECTION 05

Emerging Technology Governance

Governance maturity for AI, cloud, IoT, and other emerging technology categories. DTCI dimension score: 2.53/5 — the weakest DTCI dimension.

2.53
Emerging Tech Governance score — Nascent–Initial band

51%
have no formal or only informal AI governance

3.46
Cloud governance maturity (relative strength)

2.46
AI governance maturity (the structural weakness)

Key finding

Emerging Technology Governance is the weakest DTCI dimension at 2.53/5, in the Nascent–Initial band. The structural weakness is concentrated in AI governance: 51% of organisations have no formal or only informal AI governance, despite the majority having deployed or piloted generative AI in production over the prior 12 months.

Given the proliferation of generative AI in customer-facing, advisory, service, and decision support contexts, the absence of formal governance exposes organisations to model bias risk, regulatory non-compliance (EU AI Act implications for Australian multinationals operating globally), and reputational liability. The gap between cloud governance maturity (3.46) and AI governance (2.46) illustrates that organisations successfully applied governance discipline to prior technology generations but have not yet industrialised the equivalent for AI-era systems. ISACA's AAIA (Advanced in AI Audit) and AAIR (Advanced in AI Risk) credentials are directly responsive to this gap.

SECTION 06

People & Capability

Workforce maturity across five digital trust disciplines, certification depth, and self-identified capability gaps. DTCI dimension score: 4.00/5 (with important caveats).

Workforce capability maturity by domain

Scale: Low → Developing → Competent → Proficient → High (practitioner self-assessment)

Domain	Low	Developing	Competent	Proficient
Cybersecurity	—	—	46%	33%
IT Audit	13%	41%	26%	15%
Risk Management	18%	36%	28%	18%
Data Governance	28%	28%	28%	13%
Ethics & Digital Responsibility	23%	31%	26%	15%

Professional certifications (% of workforce certified)

Certification depth	Share
<25% certified	36%
50–74% certified	23%
Not tracked	21%
25–49% certified	10%
75%+ certified	10%

Top workforce capability gaps

Gap	Share citing
Lack of governance awareness	49%
Limited business engagement	28%
Low risk culture	26%
Cyber skills shortage	23%
Limited audit expertise	18%

Key finding — people score 4.00/5: a caveat on interpretation

The people dimension returns the highest DTCI sub-score, but warrants interpretive caution. The surveyed population is dominated by cybersecurity practitioners and GRC professionals — precisely the cohort most likely to self-rate their own capability as Competent or Proficient. The more instructive signal is structural: 57% of organisations either have fewer than 25% of their workforce certified, or do not track certification at all. This suggests that while individual practitioner capability is strong, enterprise-wide capability uplift through structured certification programmes remains an underdeveloped lever.

SECTION 07

Investment Outlook

Forward-looking commitment to digital trust investment over the next 12 months.

74%

anticipate moderate or significant investment increases in digital trust over the next 12 months

—

Investment direction is positive across all surveyed sectors and organisation sizes

Key finding

Forward-looking commitment is strong: 74% of organisations anticipate moderate or significant digital trust investment increases in the next 12 months. This reflects both the maturity gap awareness and the regulatory pressure environment — particularly in the wake of high-profile Australian breaches and the SOCI Act expansion. The investment momentum represents a structural opportunity for the profession, for the certification community, and for the consulting and assurance ecosystem.

SECTION 08

Strategic Recommendations

Priority actions for Victorian enterprises to advance from Developing to Advanced DTCI maturity.

Priority 1 — Industrialise AI governance

The 51% AI governance gap is the most material strategic risk in the dataset. Establish a formal AI governance framework with model inventory, risk classification, and ongoing monitoring. Align with ISO 42001 and the EU AI Act for organisations with global operations. ISACA AAIA and AAIR credentials provide the practitioner foundation. High Priority.

Priority 2 — Close the incident readiness gap

69% incident-readiness exposure should be addressed via tabletop exercises, crisis communications playbooks, and Board-level breach response simulation. CISM-certified leaders should lead this programme. High Priority.

Priority 3 — Establish enterprise digital trust framework

57% of organisations operate without an enterprise-wide digital trust framework. Adopt a coordinated framework (e.g., ISACA Digital Trust Ecosystem Framework) with Board mandate, executive ownership, and cross-functional accountability. Medium-High Priority.

Priority 4 — Scale workforce certification

With 56% of workforces below 25% certified or untracked, a structured certification roadmap (CISA, CISM, CRISC, CDPSE, CGEIT, AAIA, AAIR) tied to role progression should be established. Medium Priority — high long-term ROI.

Priority 5 — Modernise third-party trust management

Extend third-party risk management beyond traditional vendor reviews to include AI supplier risk, cloud governance attestation, and supply chain digital trust assurance. Particularly material for financial services environments. High Priority.

SECTION 09

Methodology & Index Construction

Research design, analytical approach, and known constraints on the current dataset.

Research design

Quantitative, cross-sectional survey using a 23-question structured instrument. Data collected via Microsoft Forms, October 2025 – March 2026. Instrument segmented across seven thematic domains with Likert scale, multiple-choice, and multi-select question formats. Research conducted by Dinesh Dino Velusamy and Reshma Devi, ISACA Melbourne Chapter.

DTCI index construction

Composite DTCI computed as an equal-weighted mean across five dimensions. Dimension scores converted to a 0–100 scale using score ÷ 5 × 100. Composite DTCI is the equal-weighted mean of the five dimension scores on this scale. Future iterations should apply confirmatory factor analysis (CFA) to validate the dimensional structure and differential weighting.

Known limitations

Sample size restricts inferential generalisability. Respondent skew toward cybersecurity/GRC practitioners inflates people capability scores. Sector underrepresentation limits sector-level conclusions. Self-assessed maturity introduces optimism bias.

DTCI computation summary

DTCI Dimension	Survey Qs	Scale	Raw	/100	Rating
Cybersecurity Maturity	Q8a–e	5-pt ordinal	3.37	67.4	Defined
Trust Governance	Q5, Q6	4-pt → norm.	3.01	60.2	Developing
ERM Integration	Q11	5-pt ordinal	3.41	68.2	Defined
Emerging Tech Governance	Q15a–e	5-pt ordinal	2.53	50.6	Nascent–Initial
People Capability	Q17a–e	5-pt ordinal	4.00	80.0	Proficient
Composite DTCI	—	Equal-weighted	3.27	65.3	Developing

Research roadmap — 2026 enhancement priorities

To strengthen DTCI validity and inferential power: (1) Scale to n≥200 per original research design to enable factor analysis and regression-based capability predictor modelling. (2) Apply CFA to validate the five-dimensional construct structure. (3) Stratify sampling by sector and organisation size to enable reliable cross-tabulation. (4) Introduce longitudinal tracking to detect directional maturity change year-on-year. (5) Consider objective validation indicators (audit certifications, regulatory disclosures, incident data) alongside self-assessed scores to address response bias.

ISACA

MELBOURNE CHAPTER

Published by ISACA Melbourne Chapter. Research conducted by Dinesh Dino Velusamy and Reshma Devi, ISACA Melbourne Chapter. This report is based on the inaugural DTCI Victorian enterprise survey and is intended for professional benchmarking and member education purposes. Findings are indicative for this cohort and should not be interpreted as population-representative. For research enquiries or to participate in the 2026 longitudinal study, contact ISACA Melbourne Chapter.