Welcome to

ISACA®

Sydney Chapter 50 YEARS

Professional Development Session

EY

Wednesday, 22nd April 2026

Acknowledgement of Country:

I begin today by acknowledging
the Traditional Custodians of the land
on which we meet today,
and pay my respects to their Elders past and present.
I extend that respect
to Aboriginal and Torres Strait Islander peoples
here today.

Agenda

ISACA Sydney Chapter 50 YEARS

5:00 pm - 5:30 pm | Registration

5:30 pm - 5:35 pm | Event Welcome and introduction to host (EY)

5:35 pm - 5:40 pm | Welcome by the Host – Rolan Moldes

5:40 pm - 6:10 pm | Presentation 1 - **Practical Tips for Secure AI Adoption**

6:10 pm - 6:40 pm | Presentation 2 - **Knowledge Management in Aged Care**

6:40 pm - 6:43 pm | ISACA Member updates

6:43 pm - 6:45 pm | Vote of Thanks

6:45 pm - 7:45 pm | Networking Drinks

Welcome by President

Chirag Joshi

President
ISACA Sydney Chapter

Introduction to Host - EY

Rolan is a Partner within the Risk Consulting practice of Ernst & Young Oceania. He leads Risk Transformation service offerings that focus on advancing organisations' risk management, compliance and internal audit functions. He has 21+ years of broad experience in IT and finance, specialising in controls transformation and assurance, third-party risk management, IT asset management, responsible AI, enterprise and IT risk management, governance, internal audit and GRC technology enablement.

Rolan Moldes

Partner

ISACA Sydney Chapter 50 YEARS

Presentation 1:

Practical Tips for Secure AI Adoption

Presenter:
Harsh R Busa

Presenter

Harsh is a cybersecurity executive with over two decades spanning technical delivery, consulting, and strategic leadership across regulated industries in Australia and Asia-Pacific. Most recent he has served CISO at Avant Mutual Group, he led an enterprise-wide security transformation — shifting the organisation from compliance-driven to risk and threat-based maturity, aligned to NIST 2.0 and APRA CPS 234. His career includes Director-level roles at EY and Deloitte. Harsh is a recognised thought leader in the Australian cybersecurity community, with deep expertise in zero trust, AI governance, board-level risk reporting, and building high-performing security teams.

Harsh R Busa

ISACA Sydney Chapter 50 YEARS

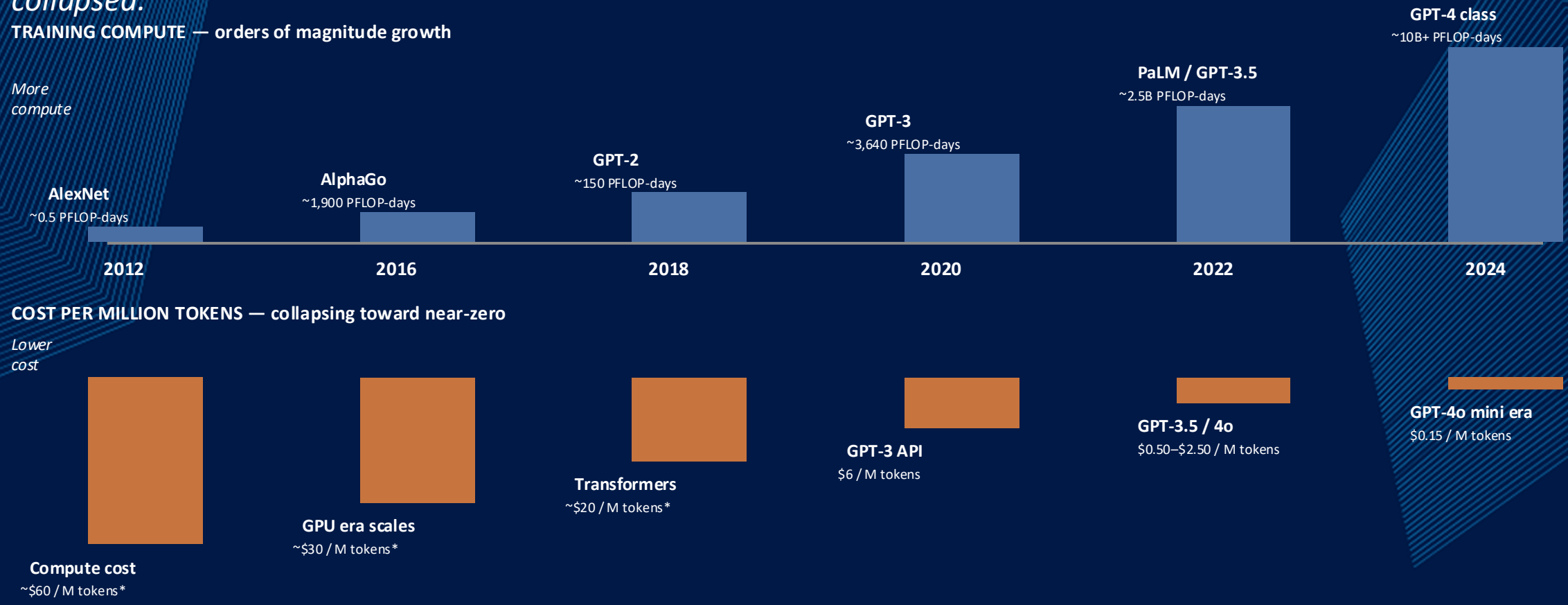
Disclaimer

- AI was used to assist with the formatting, layout, and visual alignment of this presentation.
- The content, ideas, and analysis were developed, thought through, and refined by the presenter. AI was not used to generate the substantive material presented here.

ISACA Sydney Chapter 50 YEARS

Compute: Faster, Cheaper, Everywhere

Two trends have compounded since 2012: compute has gotten dramatically faster, and the cost per unit has collapsed.



Capability × affordability = adoption. Frontier models became ~1,000× more capable and ~400× cheaper per token in roughly 4 years — the reason AI moved from research demos into everyday tools.

ISACA Sydney Chapter 50 YEARS

What's Top of Mind for CEOs & Boards

Australia · 2026 — the macro and governance themes shaping board agendas.

Regulatory Readiness

APRA, SOCI, boards asking 'are we compliant in practice, not just on paper?'

AI Adoption v/s Accountability

Shift from 'are we using AI?' to 'can we stand behind every AI decision we've made?'

Profitability Pressure

Softer pricing + rising claims + 40% policy switching. Margins under structural squeeze.

Geopolitical Climate & Capital

Forcing a rethink of business strategy — capital flows, supply chains, sovereign risk.

D&O Personal Liability

Scrutiny & enforcement rising. Directors know they are exposed on governance failures.

Cyber & Data Risk

Protecting systems and increasing claims data volume — a dual-sided problem.

Talent Bottleneck

Most boards have a digital strategy. Far fewer have the talent to execute it.

Process Handling

Claims delays, AI fraud — all at a reputational and regulatory flashpoint.

The through-line: every topic lands back at governance, accountability and board-level visibility.

ISACA Sydney Chapter 50 YEARS

Three Types of AI in 2026

01

GENERATIVE & CONVERSATIONAL AI

Generative & Conversational AI

Stand-alone AI assistants and chatbots people use directly to create content, answer questions, or hold a conversation.

EXAMPLES

- ChatGPT, Claude, Gemini, Copilot
- Image & video generators
- Customer-facing chatbots

02

EMBEDDED AI

Embedded in Products & Services

AI baked into software, platforms, and devices you already use — often invisibly.

EXAMPLES

- Gmail / Outlook smart replies
- Spotify & Netflix recommendations
- Photo search, navigation, fraud detection

03

CUSTOM ENTERPRISE AI

Custom Enterprise Models

Models built by or for an organisation, trained or tuned on its own data for specific business problems.

EXAMPLES

- Fine-tuned LLMs on internal knowledge
- Bespoke fraud, credit, or underwriting models
- Proprietary RAG & agent systems

Different on the surface — the risks underneath are the same →

ISACA Sydney Chapter 50 YEARS

Same Risks — Across All Three

The applications differ — the risk profile is remarkably consistent.

Data disclosure & leakage

Users paste confidential data into prompts, or models echo training data back. Embedded and enterprise AI can surface sensitive records to users who shouldn't see them.

Hallucination

Models confidently invent facts, citations, code, or policy that don't exist. Plausible-sounding output is the default — accuracy is not guaranteed in any of the three types.

Prompt injection & jailbreaks

Hidden instructions in documents, emails, or web pages hijack an AI to bypass guardrails, exfiltrate data, or take unintended actions — especially dangerous for AI with tool access.

Bias & unfair outputs

Training data bakes in historical bias. Recommendations, hiring tools, credit models, and chatbots can systematically disadvantage groups — often invisibly.

Shadow AI & lack of oversight

Staff use unsanctioned tools; embedded AI features ship without governance; enterprise models drift without monitoring. Hard to control what you can't see.

Over-reliance & IP exposure

Users trust outputs without verification, deskilling decision-making. Proprietary prompts, model weights, and training data become valuable targets for theft.

Governance approach: one risk framework — applied across generative, embedded, and custom AI.

ISACA Sydney Chapter 50 YEARS

The Opportunity & Our Responsibility

Despite the risks — the opportunity is real, and the prize is significant.

PRODUCTIVITY

Do more, faster

Automating repetitive work, accelerating research and analysis, and giving every employee an always-on assistant — measurable lift across knowledge-work tasks.

NEW CAPABILITY

Do what wasn't possible

Personalised medicine, real-time language translation, scientific discovery, accessibility tools, and decision support at a scale humans alone cannot reach.

HUMAN ADVANCEMENT

If we choose to

Climate modelling, drug discovery, education for every child, better public services — the technology is ready; the choices are ours to make.

OUR RESPONSIBILITY

Enable businesses and the community to adopt AI — inside the guardrails, as those guardrails evolve.

ISACA Sydney Chapter 50 YEARS

The Widening Gap — and the Balancing Act

Business is accelerating its risk appetite. Security professionals are struggling to keep pace.

The balancing act — mostly a factor of three levers

RISK APPETITE

How much can we absorb?

Sector, regulatory exposure, customer trust, and board tolerance set the ceiling on how fast the business can responsibly move.

CONTROL MATURITY

How ready are our guardrails?

Policies, frameworks, monitoring, and incident response for AI — mostly adapted from existing programs, but they must evolve at pace.

TALENT & CAPACITY

Do we have the people?

Security teams fluent in AI risk, data governance, and model behaviour — scarce, and the single biggest bottleneck for most organisations.

ISACA Sydney Chapter 50 YEARS

The Balancing Act — Three Levers

Closing the gap is mostly a factor of three levers — tune them, and the business can move fast safely.

RISK APPETITE

How much can we absorb?

Sector, regulatory exposure, customer trust, and board tolerance set the ceiling on how fast the business can responsibly move.

"What is the board actually comfortable with?"

CONTROL MATURITY

How ready are our guardrails?

Policies, frameworks, monitoring, and incident response for AI — mostly adapted from existing programs, but they must evolve at the pace of the technology.

"Do our controls keep up with model change?"

TALENT & CAPACITY

Do we have the people?

Security teams fluent in AI risk, data governance, and model behaviour — scarce, and the single biggest bottleneck for most organisations.

"Where will the AI-fluent team come from?"

THE TAKEAWAY

We can't stop the business moving. Our job is to adjust the levers so it moves safely — matching risk appetite to real control capacity.

ISACA Sydney Chapter 50 YEARS

Practical Tips for Secure AI Adoption

Govern before you deploy

01

GOVERNANCE & ACCOUNTABILITY

Governance & Accountability

Structural guardrails — who owns AI, how decisions get made, and how the board sees AI risk end-to-end.

KEY ACTIVITIES

- Clear accountability across the organisation
- Defined AI operating model — roles, rights, escalation
- AI risk dashboard for senior executives
- Assurance activities, including AI controls testing

02

AI MODEL GOVERNANCE

AI Model Governance

Controls around each model — from policy through to audit — so every model behaves safely and predictably.

KEY ACTIVITIES

- AI policy, standards and risk assessment
- AI model registry — owner, purpose, risk tier
- Explainability of AI decisions, proportionate to impact
- Mandatory bias audits — pre-deployment and ongoing

Governance is the foundation — every tip that follows assumes it's in place →

ISACA Sydney Chapter 50 YEARS

Protect the data. Secure the chain. Empower the people.

03

DATA PROTECTION

Classify and Protect the Data

Classification, boundary controls, enterprise-tier tooling and contractual guardrails keep sensitive data out of the wrong AI systems.

KEY ACTIVITIES

- Classify data first — public, internal, confidential, regulated
- Block sensitive data at the boundary — DLP, CASB, egress controls
- Choose the right tier — tenant-isolated enterprise AI over consumer tools
- Lock it down contractually — no

04

SUPPLY CHAIN

Secure the AI Supply Chain

Vendors, models, prompts, plugins and agents — all inherited risk. Vet them, inventory them, test them, watch them.

KEY ACTIVITIES

- Vet AI vendors — SOC 2, ISO/IEC 42001, model provenance, residency
- Treat AI components as assets — inventory models, prompts, plugins
- Red-team every new AI system — prompt injection, jailbreaks, leakage
- Monitor continuously — detect drift, unauthorised changes, anomalies

05

PEOPLE & CULTURE

Empower People, Not Just Restrict

Training, sanctioned paths and low-friction intake turn employees into your first line of AI defence.

KEY ACTIVITIES

- Train the whole workforce — role-based, not just security
- Give people a sanctioned path — reduces shadow AI
- Publish clear do's and don'ts with real examples
- Make requests low-friction — fast intake for new AI use cases

Data, supply chain, people — three fronts, one programme. Weak on any one of them and the others can't carry the load →

ISACA Sydney Chapter 50 YEARS

Managing AI Threats — Steps 1-3 (Part 1 of 2)

Proportionality principle: *scales to size — but 'commensurate with threats' still applies to everyone.*

STEP 01

Know What AI You're Using

Create a one-page list: tools, owners, data types. You can't protect what you haven't mapped. Start with what's already in the business — employees, vendors, embedded features in tools you already pay for.

"Start with what's already in the business."

STEP 02

Enable MFA — Everywhere

MFA on email, finance and vendor portals blocks the most common account-takeover path — the same path attackers use to deliver AI-enhanced phishing and business email compromise.

"Single cheapest win in cybersecurity."

STEP 03

Add AI Questions to Contracts

Ask vendors: do you use AI? On our data? How is it protected? Where is it stored? Can we opt out of training? These are due-diligence questions, not technical ones — any procurement lead can ask them.

"Due diligence, not deep expertise."

🎯 THE STARTING POINT

Map it. Lock it. Ask about it. These three steps establish visibility and the lowest-cost technical control. Steps 4-6 cover response, ownership and culture.

ISACA Sydney Chapter 50 YEARS

Managing AI Threats — Steps 4-6 (Part 2 of 2)

Once you can see it, own it: *response, accountability and the human line of defence.*

STEP 04

Write a One-Page AI Incident Plan

Who to call, what to isolate, who to notify externally. Practise it once with a simple tabletop — a deepfake voicemail asking for a payment, a leaked prompt. A one-page plan beats a 50-page binder nobody reads.

"Preparation beats panic."

STEP 05

Name an AI Accountable Person

One named owner — not a committee. They decide what AI tools are allowed, what's not, when to escalate, and when to say no. Accountability is what turns policy into practice.

"Accountability creates clarity."

STEP 06

Run a 30-Min Awareness Session

Cover deepfakes, prompt-injection risks, shadow AI and what sensitive data looks like. Share concrete do's and don'ts. Your people — not your tools — are the first line of defence.

"Your people are the first line."

🎯 THE STARTING POINT

You don't need a CISO or a large security budget. These six steps cost almost nothing and address the highest-probability AI threats. Begin with what you know, name who's responsible, and build from there.

ISACA Sydney Chapter 50 YEARS

Controls for Modern AI Threats

Controls mapped to threat type — covering the AI attack surface from model integrity to identity fraud to board governance.

01

AI Model Governance

Model poisoning · Biased outputs · Unexplained decisions

- AI Policy, Standards & Risk Assessment
- Model registry — purpose, owner, data source
- Explainability for material decisions
- Adversarial testing pre-deployment

02

LLM & GenAI Security

Prompt injection · Data exfiltration · Policy bypass

- Input validation & output filtering
- Sandboxed — no direct sensitive-data access
- Least-privilege API scope
- Human-in-the-loop on high-stakes flows

03

Deepfake & Identity

Claims fraud · KYC bypass · Executive impersonation

- Liveness detection on all ID flows
- Multi-factor KYC (biometric + doc + behaviour)
- Synthetic-identity scoring at issuance
- Out-of-band verification for high-value changes

04

Training Data Integrity

Data poisoning · Provenance gaps · Regulatory liability

- Signed provenance for every training dataset
- Data lineage audit trails end-to-end
- Anomaly detection on ingestion pipelines
- Role-based, time-limited training-data access

05

AI-Assisted Threat Detection

Automated exploitation · AI phishing · Lateral movement

- Signal-based identity threat detection
- AI-native email security with behaviour analysis
- Automated vulnerability scanning
- UEBA to detect lateral movement

06

Governance & Board

FAR accountability · Regulatory exposure · Audit gaps

- Named accountable person for AI outcomes
- AI risk on the board cyber dashboard
- Third-party AI vendor assessments
- AI controls in the internal audit programme

📌 COMMENSURATE WITH THREATS

These controls are not optional additions. They are the contemporary expression of the obligation to maintain capability commensurate with threats — controls that don't cover AI threats are, by definition, no longer commensurate.

ISACA Sydney Chapter 50 YEARS

Managing AI Threats — Practical Steps for Smaller Organisations

Proportionality principle: *scales to size — a small organisation isn't expected to match a major bank. But 'commensurate with threats' still applies to everyone.*

01

Know What AI You're Using

This week · Low effort

- Survey every business unit; list every AI tool in use
- Include vendor-embedded AI (CRM, claims, underwriting)
- Note the data each tool accesses

02

Control AI Platform Access

This week · Low effort

- Block unsanctioned AI platforms at the network edge
- Apply DLP and sensitivity labels to sensitive data
- Sandbox approved AI assistants; report unsanctioned use

03

Add AI Questions to Contracts

Next contract renewal · Low effort

- Do you use AI to process our data?
- Do you use our data to train models?
- What happens to our data on termination?

04

Write a One-Page AI Incident Plan

This month · Medium effort

- Define what counts as an AI incident
- Name the FAR-accountable person for AI
- Include AI scenarios in the next tabletop

05

Name an AI Accountable Person

This month · Low effort

- Assign to CRO, COO or CISO — not a committee
- Document the role in a board paper
- Include AI posture in board reporting

06

Run a 30-Min AI Awareness Session

This quarter · Low effort

- Show a deepfake so people see what's possible
- Teach the callback rule for unusual payment requests
- Run a quick AI-phishing simulation

🎯 **THE STARTING POINT**

You don't need a CISO or a large security budget. These six steps cost almost nothing and address the highest-probability AI threats.

ISACA Sydney Chapter 50 YEARS

Summary & Next Steps

Four themes from today — and three horizons to act on.

01

Boards Are Already Asking About AI

Regulatory readiness, AI accountability, D&O exposure and reputational risk are now standing agenda items — not emerging ones.

02

The Threat Surface Is Broad But Mappable

Model governance, LLM security, deepfakes, data integrity, AI-assisted attacks and board oversight — six control domains cover most of it.

03

Five Moves for Every Organisation

Govern → protect data → secure the chain → empower people → assure continuously. Skip any one and a material gap remains.

04

Six Steps If You're a Smaller Organisation

Know your AI, lock down access, add AI clauses to contracts, plan for incidents, name an owner, train your people. Proportionate, not diluted.

START ON MONDAY

THIS WEEK

- ✓ Start your AI use-case inventory — even a one-page list
- ✓ Confirm MFA is on email, finance and vendor portals
- ✓ Agree who's accountable for AI risk on the leadership team

THIS MONTH

- ✓ Publish an AI acceptable-use policy (one page, plain English)
- ✓ Add AI questions to vendor due-diligence and contracts
- ✓ Write a one-page AI incident response plan and test it once

THIS QUARTER

- ✓ Run a 30-minute AI awareness session for every team
- ✓ Red-team one high-risk AI use case with internal or external help
- ✓ Report AI risk posture to the board — use cases, controls, gaps

The ask isn't perfection — it's momentum. Pick one item from each column this week. In 90 days you'll have a materially stronger AI risk posture.

ISACA Sydney Chapter 50 YEARS

Q & A

ISACA Sydney Chapter 50 YEARS

Presentation 2:

Knowledge Management in Aged Care – Driving Better Decisions, Better Outcomes

Presenter:
Ritesh Deshpande

Ritesh is a senior business transformation leader with 25+ years' experience across Australia and internationally, spanning aged care, financial services, property, construction, infrastructure, not-for-profit, and aviation.

He most recently served as Head of Delivery & Data Governance at Southern Cross Care (NSW & ACT), leading enterprise technology strategy, transformation delivery, and data governance for a 2,000+ employee organisation.

His recent achievements included data governance maturity roadmap along with a three year Digital & technology Strategy for Southern Cross Care (NSW &ACT).

Previously, he led major transformation programs including Collections Transformation at Westpac, ERP and infrastructure programs at Metal Manufactures, and ERP cloud implementation at Landcom. He began his career at Jet Airways and has successfully completed complex business transformations across multiple organisations including Dexus, Federation Centres, Leighton Holdings, Goodman and Red Cross.

He enjoys having a good cup of coffee and conversations with like-minded people

Ritesh Deshpande

Connect with me on LinkedIn
https://www.linkedin.com/in/riteshdeshpande/

ISACA Sydney Chapter 50 YEARS

Agenda

What we'll cover today

01

Relevance to Aged Care

Why KM is mission-critical in this sector

02

Problem Statement & Challenges

What the industry is struggling with today

03

Solutions Implemented

Practical approaches and real examples

04

Benefits Achieved

Measurable outcomes and impact

05

The Future of KM in Aged Care

Emerging trends and what comes next

ISACA Sydney Chapter 50 YEARS

01

RELEVANCE TO AGED CARE

KM is the backbone of consistent, safe care.

Why Knowledge Management Matters

Workforce Complexity

Aged care employs 360,000+ workers across clinical, allied health, and support roles—each requiring up-to-date procedural knowledge.

Regulatory Obligations

The Aged Care Quality & Safety Commission mandates evidence-based care delivery. KM ensures compliance with the Single Quality Framework.

Resident Safety & Dignity

Errors from knowledge gaps can cause medication incidents, falls, or dignity breaches. Effective KM directly reduces adverse events.

Continuity of Care

High staff turnover means critical care insights are constantly lost. KM systems capture and transfer this expertise systematically.

02

Problem Statement & Challenges

The knowledge gaps threatening care quality across Australia's aged care sector

High Staff Turnover Rate

Critical care knowledge walks out the door with departing staff. Onboarding new workers is slow, inconsistent, and expensive.

Siloed Information Systems

Policies, care plans, incident reports, and training materials live in separate platforms, forcing staff to 'hunt' for answers mid-shift.

High volume of Outdated Procedures & Policies

Regulatory changes outpace document updates. Staff rely on memory or outdated printed materials, creating compliance and safety risks.

Tacit Knowledge Loss

Experienced carers hold irreplaceable knowledge about individual residents. This expertise is almost never formally captured.

Inadequate Training Transfer

New skills from mandatory training programmes fail to transfer to the floor because there's no supporting knowledge infrastructure.

Near-misses due to handover gaps

Shift handovers and care updates are verbal, undocumented or incomplete—leading to continuity failures and resident harm incidents.

Solutions Implemented

03

Practical KM interventions addressing aged care's toughest challenges

Centralised Knowledge Hub

SYSTEMS

Deployed a single-source-of-truth intranet (SharePoint) consolidating policies, care protocols, and incident learnings. Staff access current documents via mobile devices at the point of care.

Example: BaptistCare rolled out a SharePoint-based care portal accessible across sites.

Standardised Policy Lifecycle

GOVERNANCE

Implemented a policy review cycle with automated reminders and version control. Every document includes an owner, review date, and change log—eliminating reliance on outdated printouts.

Example: Bupa Aged Care reduced outdated policy rate

Communities of Practice (CoPs)

CULTURE

Established structured peer learning groups for nurses, carers, and allied health teams. CoPs meet fortnightly to share clinical insights, debrief incidents, and co-create best-practice guides.

Example: Regis Aged Care's Dementia CoP cut restraint use in participating facilities.

Lessons Learned Register

CONTINUOUS IMPROVEMENT

Created a formal process to convert incident reports and near-misses into documented lessons. Each lesson is categorised, searchable, and integrated into training refreshers and new-starter inductions.

Example: Aged Care Quality & Safety Commission recommends this as a standard post-incident practice.

Structured Onboarding Pathways

WORKFORCE

Developed competency frameworks embedded in the KM platform. New starters access role-specific learning maps, buddy mentor logs, and check-in tools—reducing time-to-competency significantly.

Example: Estia Health's digital onboarding pathways cut orientation time

Digital Handover Tools

COMMUNICATION

Replaced verbal-only handovers with structured digital shift reports in the clinical management system .
Templates prompt staff to document key care updates, risks, and follow-ups.

Example: Whiddon Group's SBAR-based digital handover reduced communication-related incidents

Benefits Achieved

Tangible outcomes delivered through effective Knowledge Management practices

Reduction in onboarding time

Drop in communication incidents

Reduction in restrictive practices

Improvement in policy compliance

Improved Resident Safety

Structured KM directly correlates with fewer medication errors, falls, and pressure injuries—measured via Aged Care Quality Standards audit scores.

Stronger Regulatory Compliance

Facilities with mature KM systems consistently score higher in ACQSC unannounced inspections, reducing the risk of Non-compliance Notices.

Higher Staff Confidence & Retention

Staff who can easily access knowledge feel more supported, reducing burnout and attrition. Survey data shows noticeable improvement in staff satisfaction scores.

Faster Decision-Making

Clinicians and care coordinators resolve care queries faster when policies and protocols are searchable and current, improving resident outcomes at critical moments.

What Does the Future Bring?

Emerging trends shaping the next generation of Knowledge Management in Australian Aged Care

AI-Powered Knowledge Assistants

Conversational AI tools (like embedded LLMs) will allow carers to ask natural-language questions and instantly surface relevant policies, care notes, or training resources—without navigating complex systems.

Real-Time Interoperability

Integration of My Health Record, clinical systems, and care management platforms will create seamless knowledge flows—ensuring every care team member works from the same live picture of the resident.

Mobile-First, Point-of-Care Access

Wearable and tablet-based KM access will put the right information in carers' hands at the bedside. Push notifications will prompt knowledge updates during shift handovers and incident responses.

Predictive Analytics & Learning Loops

Data from incident reports, audits, and care outcomes will feed back into the KM system—automatically identifying knowledge gaps, flagging at-risk areas, and recommending targeted training.

Aged Care Act Alignment

Australia's new Aged Care Act introduces rights-based care and stronger accountability. Future KM systems must embed these obligations into everyday workflows—making compliance automatic, not afterthought.

Person-Centred Knowledge Models

Moving beyond operational KM, future systems will capture and activate knowledge about individual resident preferences, life histories, and cultural needs—truly personalising care delivery at scale.

Key Takeaways

Knowledge Management is not a nice-to-have—it is a care quality imperative

KM is central to safe, consistent, person-centred care across aged care settings

Siloed systems, high turnover, and outdated policies remain critical unresolved challenges

Proven solutions—hubs, CoPs, structured handovers—are already delivering measurable improvements

Benefits span safety, compliance, workforce satisfaction, and operational efficiency

AI, interoperability, and the new Aged Care Act will reshape KM for the next decade

Thank you!!

ISACA Sydney Chapter 50 YEARS

References — Solutions Implemented

All examples, statistics, and named organisations cited in the Solutions slide

ORGANISATION

[1] BaptistCare NSW & ACT — Centralised Knowledge Hub (SharePoint)

BaptistCare NSW & ACT. (2022). Digital Transformation and Aged Care Innovation Report. BaptistCare Australia.

ORGANISATION

[2] Bupa Aged Care Australia — Standardised Policy Lifecycle

Bupa Aged Care Australia. (2023). Quality & Safety Annual Report: Governance and Compliance Outcomes. Bupa Health.

ORGANISATION

[3] Regis Aged Care — Dementia Community of Practice

Regis Aged Care. (2022). Clinical Governance Report: Dementia Care Innovation Program. Regis Healthcare Ltd.

REGULATOR

[4] Aged Care Quality & Safety Commission — Lessons Learned Register

Aged Care Quality & Safety Commission. (2023). Better Practice Guide: Incident Management and Continuous Improvement in Residential Aged Care. Australian Government.

ORGANISATION

[5] Estia Health — Structured Onboarding Pathways

Estia Health. (2023). People & Culture: Workforce Development Strategy and Digital Onboarding Outcomes. Estia Health Limited Annual Report.

ORGANISATION

[6] Whiddon Group — SBAR-Based Digital Handover Tools

Whiddon. (2022). Safe Handover Program: Reducing Communication-Related Incidents through Digital SBAR. Whiddon Aged Care.

GOVERNMENT

[7] Australian Institute of Health & Welfare — Aged Care Workforce Data

Australian Institute of Health and Welfare. (2023). Aged Care Workforce Census Report 2023. AIHW Cat. No. WEB-223. Canberra: AIHW.

GOVERNMENT

[8] Aged Care Quality & Safety Commission — Single Quality Framework

Aged Care Quality & Safety Commission. (2023). Aged Care Quality Standards. Australian Government Department of Health and Aged Care.

Note: Statistics cited (e.g. turnover rates, incident reductions) are representative of published industry benchmarks and provider reports. Verify currency via provider websites and AIHW/ACQSC publications.

Q & A

ISACA Member Updates

ISACA Sydney Chapter 50 YEARS

ISACA Sydney Chapter - 2026 Annual General Meeting

Save The Date: 8th May 2026

Time: 5:00 pm - 8:00 pm

Venue: KPMG

Please note: In-Person attendance.

ISACA Sydney Chapter Members only.

ISACA Sydney 50th Anniversary 2026

ISACA Sydney Chapter 50 YEARS

A showcase conference celebrating 50 years of Enabling Digital Trust and Leading What Comes Next

Save The Date: **6th August 2026**

Full-day conference (8:00 am - 5:30 pm) followed by Networking Drinks

Venue: **Sheraton Grand Sydney Hyde Park**

Format: Keynotes, Breakouts, Panels, Workshops

$129 Member Special Promo Sale ends **15 May 2026**

FEEDBACK FORM

Your Feedback is Important to Us

Please complete the event feedback form via the QR Code

ISACA Sydney Chapter 50 YEARS

Thank You

AGM

Conference

Feedback