

INTERNET SECURITY ALLIANCE

Decisions for Larry

Seven recommended names + Microsoft referral | 13 October 2026

Recommended: advance four for qualification, hold two, reconcile one existing relationship and pursue one Microsoft referral. These are recommendations for Larry to approve.

Person / company	Decision	Introduction lead	Exact next action
Summer Craze Fowler / Exponent	Advance to qualification	ISA introducer unnamed Email	Larry: name the willing member; confirm Exponent account, eligibility and sponsor. Test the metrics dashboard case.
Leo Simonovich / Siemens Energy	Advance through existing pipeline	Larry / ISA existing-prospect route Email	Larry: establish pipeline stage and contact owner; confirm Siemens Energy representation and funding. Test the secure-design case.
Christopher Porter / Booz Allen Hamilton	Advance to qualification	JR Williamson / Leidos Email	Larry: confirm JR owns the follow-up and timing in the new role. Verify Booz Allen account, sponsor and a current risk-decision case.
Chris Betz / Google Cloud	Advance to qualification	Stephane Lenco / Thales Email	Larry: confirm Lenco contact ownership and introduction consent. Verify Google account, sponsor and AI-governance contribution.
Jack Freund / Freund Advisory Group	Hold membership priority	ISA introducer unnamed Email	Larry: name the member and reconcile current employment. Require a suitable paying organization before restoring priority.
Michael Papay / Rohirrim	Hold; reconcile board feedback	Tracie Grella; JR Williamson Email	Larry: reconcile Tracie relationship lead with JR negative-fit feedback. Require eligible sponsor, scale and role/time confirmation.
Tim McKnight / reported Merck	Reconcile existing ISA relationship	Larry / ISA to designate owner Email	ISA: resolve Merck versus UnitedHealth affiliation, current seat and account treatment. Confirm employer sponsorship before counting a new sponsor.
Igor Tsyganskiy / Microsoft	Referral route only	Attending ISA members unnamed Email	Larry: name the attending members and verify intended Igor contact. Request one suitable Microsoft nominee; qualify one corporate account.

Common release gate

ISA confirms membership, eligibility and introduction owner. Prospect/employer confirms current remit, interest, sponsor approval, time and agreed contribution. Confirmations remain open; a named relationship lead is not an accepted introduction assignment.

1631 next step: after Larry selects the routes, prepare each concise, source-backed pitch and record qualification outcomes. No outreach has been sent.

ISA-recommended prospects

Designed board-membership review | Prepared for Larry Clinton and Joe Corbe | 13 October 2026

Seven recommended names and one Microsoft referral route. Each profile has an authentic sourced headshot and company brand treatment, with prominent contact lines and clickable public routes.

Current decisions

Four names remain priorities for qualification. Jack Freund and Michael Papay remain on hold. Tim McKnight is an existing ISA relationship requiring affiliation and sponsorship reconciliation. Igor Tsyganskiy remains a Microsoft referral contact.

Reading the report

The four retained names use their current top-50 research priorities: Fowler #1, Simonovich #2, Porter #3 and Betz #4. Those research ranks do not establish eligibility, membership approval or a sponsorship commitment. Earlier rankings and affiliations have been superseded.

Qualification still required

Confirm current role, membership and eligibility; name and verify introducers; validate executive interest, company sponsorship and time; agree a specific ISA contribution and separate company and executive benefits. Keep industry, geography and expertise in the first-group decision.

Evidence standard

Public sources and submitted webinar registration matches support research and engagement hypotheses. Registration is not confirmed attendance or an additional substantive sighting. Private commitments, following ISA or Larry, and LinkedIn connections require direct evidence.

Review directory

Person / affiliation	Treatment	Page
Summer Craze Fowler / Exponent	Top 50 research #1; qualification pending	4
Leo Simonovich / Siemens Energy	Top 50 research #2; qualification pending	9
Christopher Porter / Booz Allen Hamilton	Top 50 research #3; qualification pending	15
Chris Betz / Google Cloud / Alphabet	Top 50 research #4; qualification pending	19
Jack Freund / Freund Advisory Group / Acrisure affiliation disputed	Hold	23
Michael Papay / Rohirrim	Hold	26
Tim McKnight / Merck & Co., Inc.	Existing relationship	29
Igor Tsyganskiy / Microsoft	Referral contact only	32

Jack Freund uses the text wordmark published on his own firm website. Tim McKnight carries the official Merck logo with a reported-affiliation flag. All other profiles use published company logos.

Contact information is bold. Published verified email addresses are clickable; unverified addresses are omitted. Links beside factual claims open their source.



#1

Summer Craze Fowler

Corporate Vice President and Principal
Exponent

Current employer biography confirms the role and Philadelphia office; Torc and Motional roles are historical. **Current-role source**

Public business email: sfowler@exponent.com | **Office:** +1-215-594-8855

Public contact source. Named public professional route; delivery/access and personal response are not confirmed. **Source:** www.exponent.com

LinkedIn profile | **Named professional biography / public route**

Work base: Philadelphia office listed by employer. **Employer-listed office; residence and travel availability unconfirmed.**

Recommendation and rationale

First-group qualification. ISA introduction lead; enterprise/scientific operating leadership, testimony, metrics and resilience expertise.

Research rank #1 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 total revenue \$582.0m (\$536.8m before reimbursements); net income \$106.0m; 1,212 employees at January 2, 2026. Listed engineering and scientific consultancy. Annual \$75,000 corporate sponsorship is approximately 0.013% of FY2025 revenue (calculated), but interest and authorization are unconfirmed.

Source: investors.exponent.com

Proposed company benefit: More useful cyber-risk assessments and clearer evidence for investment and recovery decisions.

Proposed executive benefit: Access to directors and peers to test her metrics methods and inform practical oversight guidance.

What This Recruit Could Add to ISA

Create a dashboard linking engineering evidence, residual risk and investment outcomes. **Source:** www.ians.com

Handbook connection: Tool K 66-68; L 69-71. Proposed output and benefits require agreement. **Source:** www.nacdonline.org

Introduction and next decision

ISA-reported willing introducer; name not provided. Larry names Fowler as an introduction priority but does not identify the member. [Source: mail.google.com](mailto:mail.google.com)

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Direct testimony: Written congressional testimony on mission-oriented cyber resilience.

January 2017 - Heinz College Makes Cybersecurity Recommendations That Washington Should Consider Now | Carnegie Mellon University's Heinz College. Advocates clearer cyber-law definitions, federal breach-notification consistency and privacy/security in product design. [Source: www.heinz.cmu.edu](http://www.heinz.cmu.edu)

Historical SEI position. These are policy proposals, not proven legislative outcomes.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	ISA-reported willing introducer; name not provided. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

[ISA public board / meeting baseline](#) | [Bylaws](#) | [Published sponsorship](#)

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Name-matched image on named public biography. [Source: www.exponent.com](http://www.exponent.com)

Company mark: Current employer website brand asset [Source: www.exponent.com](http://www.exponent.com)

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Business outcomes should determine cybersecurity metrics

April 4, 2023 | Direct interview answers published by IANS; historical role descriptions. [Source: www.ians.com](http://www.ians.com)

Fowler identifies two failures: no shared metrics framework and weak translation into business outcomes. She recommends understanding company goals first, explaining outputs and outcomes, disclosing residual risks, and showing why money is being allocated to particular controls. Metrics should serve the audience rather than the security team.

Attribution / limitation: The direct answers are usable. The older Motional role in the article is historical; the current biography footer does not make the original interview new.

2. Operational consequences matter more than vulnerability counts alone

September 15, 2026 | Coauthored Exponent article; collective position. [Source: www.exponent.com](http://www.exponent.com)

The authors recommend starting with adverse operating conditions and tracing the systems, safeguards and operator actions that can produce or prevent them. Identical controller vulnerabilities can yield different consequences in different plants. They also question whether primary and backup systems share credentials, workstations or remote-access infrastructure.

Attribution / limitation: Fowler is one of five listed authors. Do not attribute every sentence exclusively to her. The findings concern water utilities; broader relevance is interpretation.

3. Baseline source

April 2, 2026 | Coauthored Exponent article; collective position. [Source: www.exponent.com](http://www.exponent.com)

The authors warn against restoring systems so quickly that logs or other evidence are overwritten. They recommend explicit response roles, recovery criteria and tested backups. Long-term resilience should include early threat modeling, updateability, software-dependency transparency, independent testing and postmarket monitoring.

Attribution / limitation: Fowler is one of four authors. These are shared published recommendations, not an isolated personal interview or proof of agreement with ISA.

4. Security culture should enable safe work and shared responsibility

November 12, 2021 | Direct answers in Living Security interview transcript. [Source: www.livingsecurity.com](http://www.livingsecurity.com)

Fowler describes embedding safety in job descriptions and everyday responsibility, using team-level cyber ambassadors and ongoing communication, and treating supplier assessment according to the importance of the product or service. She also identifies data access, third-party relationships and supply-chain integrity as concerns.

Attribution / limitation: Argo AI is the historical setting. The transcript identifies individual speakers; do not assign interviewer Drew Rose's observations to Fowler. This interview is counted once.

5. Social engineering needs policy, training and technical safeguards together

June 9, 2021; publisher shows update October 6, 2026 | Article attributed to Fowler by IANS; update authorship unspecified.
Source: www.ians.com

The article recommends measures across departments, including independent approval of elevated access, known-channel verification of changed bank instructions, a second approver for transfers, and social-engineering tests. Its premise is that human-centered attacks require policy and technology controls as well as training.

Attribution / limitation: The original author attribution is Fowler. IANS does not identify who made the 2026 changes or distinguish updated text; do not present all current wording as a fresh 2026 statement by her.

6. Assess cybersecurity spending against planned and actual performance

March 15, 2018 | Single-author SEI article. Source: www.sei.cmu.edu

Fowler proposes adapting earned-value concepts to compare spending, planned scope, actual events and successful handling. Her examples distinguish failed expenditure, accepted risk that materializes, unforeseen impact, residual risk averted and unnecessary spending. She presents the model as an invitation to develop better indicators.

Attribution / limitation: This is a proposed measurement approach, not proof that the metrics became a validated standard. The article's old spending and crime projections are not used.

7. Start cyber-risk analysis with mission impact and critical assets

July 25, 2018 | Written congressional testimony under Fowler's name. Source: docs.house.gov

Fowler argues that agencies must manage attack consequences as well as threats. She favors identifying mission objectives, critical services and assets before working backward to threats. Her resilience approach integrates security, continuity, disaster recovery and IT operations; she also identifies legacy IT and workforce gaps.

Attribution / limitation: Reviewed written testimony, especially pages 1-3. This establishes historical congressional participation and her position then; it does not establish present policy access or endorsement of current ISA legislation.

8. Enterprise risk leadership translates board goals into operational decisions

May 24, 2018 | SEI podcast transcript; Fowler and Ari Lightman have separate turns. Source: www.sei.cmu.edu

In her own answers, Fowler describes a chief risk officer who looks across operational units, translates board and executive goals into business-unit execution, monitors risk and reports decisions requiring leadership attention. She emphasizes operating within risk appetite and communication across different types of risk.

Attribution / limitation: The publication date is confirmed by the SEI episode listing. Pages 2-3 of the transcript distinguish her answers from Lightman's; this is not sole authorship of the whole conversation.

9. Prepare to adapt before disruption rather than only recovering afterward

February 27, 2017 | Single-author SEI article. Source: www.sei.cmu.edu

Fowler proposes organizations that anticipate disruption and adapt before it happens. She describes scenario exercises as an early capability and proposes expanding toward continuous exercises based on real-world indicators. The discussion builds on operational resilience while calling for more proactive adaptation.

Attribution / limitation: The article describes an emerging research direction in 2017. Do not recast its historical AI examples or aspirations as proof of modern agentic-AI capabilities.

10. Workforce development should combine role-specific training and applied exercises

PDF dated December 2016; SEI publication listing February 23, 2017 | Coauthored SEI report; collective project account. **Source:** www.sei.cmu.edu

The report documents a USPS-SEI academy pilot with management and technical tracks, virtual and in-person learning, mentorship and tailored capstone exercises. It describes training existing staff and a two-year postgraduation service commitment. The paper addresses workforce needs revealed by a breach.

Attribution / limitation: Fowler is one of four authors. The report PDF title/date differ from the library listing. USPS's CISO Academy is distinct from ISA's proposed Virtual Cyber Academy; this does not prove support for ISA's model.

Prior ISA webinar engagement - supplied roster

Matched in ISA Webinar Attendees.xlsx, attendees.csv, row 288. Exact LinkedIn URL and supplied name/title reviewed; categorized FINAL v3 and v5 corroborate the row.

Supplied title: Corporate VP and Cybersecurity Principal | Brentwood Bank Board Member | The Forte Group Member | IANS Faculty | Co-host on Business Security Weekly Podcast

Supplied organization: Blank; current employer assessed separately. Registration does not establish current ISA membership, sponsorship interest or event attendance.

Individual webinar dates, repeat registrations, attendance and questions are not included in this source. Not counted toward ten substantive sightings.



#2

Leo Simonovich

VP and Global Head, Industrial Cyber and Digital Security
Siemens Energy

Current contributor biography identifies Siemens Energy industrial-cyber leadership; this is an operating executive role, not a director-only profile. [Current-role source](#)

Direct business email and telephone: not publicly verified.

[LinkedIn profile](#) | [Named professional biography / public route](#)

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

First-group qualification. ISA nominee; House-record comments, industrial policy, secure design and energy economics.

Research rank #2 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 revenue EUR39.1bn, issuer release. Siemens Energy is separate from Siemens AG; do not substitute Siemens AG financials. [Source: www.siemens-energy.com](http://www.siemens-energy.com)

Proposed company benefit: Stronger oversight of power assets, supplier dependencies and security choices across asset lifecycles.

Proposed executive benefit: A policy and peer forum for advancing his industrial-security economics and secure-design priorities.

What This Recruit Could Add to ISA

Develop a capital-project case comparing secure design, retrofit expense and energy disruption. [Source: www.utilitydive.com](http://www.utilitydive.com)

Handbook connection: Tool H 57-59; B 37-40; K 66-68. Proposed output and benefits require agreement. [Source: www.nacdonline.org](http://www.nacdonline.org)

Introduction and next decision

Larry / ISA existing-prospect route. Larry identified Simonovich as a prospective member before the September board meeting; reconcile existing pipeline stage. [Source: mail.google.com](mailto:)

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Own energy-policy remarks on public-private resilience, modernization incentives and AI infrastructure standards.

March 14, 2018 - Leo Simonovich: written comments on DOE modernization and cybersecurity. Makes the case for industry-government collaboration and a shared Charter of Trust for the industrial digital economy. [Source: docs.house.gov](https://docs.house.gov)

Written submitted comments verified; oral witness testimony is not established. Body describes historical Siemens; header uses Siemens Energy. Current employer scale is separate.

2018-11-07 - Driving security in an unsecure world - NIST conference presentation. Simonovich's presentation links industrial cyber risk to safety and production and outlines Charter of Trust principles, supplier requirements, certification and shared initiatives. [Source: www.nist.gov](https://www.nist.gov)

Historical Siemens presentation. Corporate principles and quoted colleagues remain corporate or separately attributed; no claim of regulatory adoption.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	Larry / ISA existing-prospect route. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

[ISA public board / meeting baseline](#) | [Bylaws](#) | [Published sponsorship](#)

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Portrait embedded beside named Leo Simonovich foreword, page 1. Cropped from authentic named portrait to focus on face and shoulders. **Source:** assets.siemens-energy.com

Company mark: Exact asset observed on named public source **Source:** www.siemens-energy.com

Attributable commentary and evidence ledger

11 / 10 substantive sightings recorded. Depth target met.

1. Building security into energy infrastructure by design is lower cost and more effective | Utility Dive

January 12, 2026 | Authored industry article [Source: www.utilitydive.com](http://www.utilitydive.com)

Argues security should be designed into energy infrastructure before construction, avoiding expensive retrofits and protecting reliability.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

2. Minutes to Exploit-Months to Recover

August 3, 2026 | Authored industry article [Source: www.powermag.com](http://www.powermag.com)

Contrasts rapid exploitation with long industrial recovery; urges asset lifecycle planning and compensating controls for aging systems.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

3. Energy leaders need to prepare for AI-powered cyber threats | World Economic Forum

July 24, 2026 | WEF article coauthored with Filipe Beato [Source: www.weforum.org](http://www.weforum.org)

Calls for energy asset visibility and prioritized remediation as AI accelerates threats; automation must support human expertise.

Attribution / limitation: Joint position; do not attribute every sentence to Simonovich alone.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

4. Cybersecurity for both data centres and their energy systems | World Economic Forum

May 5, 2026 | WEF article coauthored with Filipe Beato [Source: www.weforum.org](http://www.weforum.org)

Treats data-center resilience as a dependency problem spanning power, backup, cooling and physical access rather than IT systems alone.

Attribution / limitation: Joint analysis; no evidence of an ISA commitment.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

5. Why we need to power cyber resilience in the energy sector | World Economic Forum

May 9, 2025 | WEF article coauthored with Kesang Tashi Ukyab [Source: www.weforum.org](http://www.weforum.org)

Advocates collaboration across the energy ecosystem because suppliers and operators share cyber dependencies and reliability consequences.

Attribution / limitation: Coauthored; distinguish Siemens Energy from Siemens AG.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

6. The new cyber-threats to utilities: a Q&A with two experts | World Economic Forum

2020-05-22 | Speaker-labeled Q&A Source: www.weforum.org

Links IT/OT convergence with operational shutdown and safety consequences and calls for utility and equipment-manufacturer partnerships.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Sector expertise tied to physical business consequences.

7. AI can protect all energy firms from cyberattack. Here's how | World Economic Forum

2020-11-16 | Self-authored WEF article Source: www.weforum.org

Argues that weak links endanger the interconnected energy ecosystem and that detection must be feasible for smaller operators as well as large companies.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Economic feasibility and systemic resilience.

8. To minimize AI's cyber risks to energy infrastructure, start with the design phase | Utility Dive

2024-10-31 | Self-authored industry article Source: www.utilitydive.com

Discusses AI-related energy regulation and standards, industry cooperation and secure infrastructure design before future operating and compliance costs are locked in.

Attribution / limitation: Published position; no ISA interest or policy outcome is inferred.

ISA relevance: Specific policy and investment-design discussion.

9. Securing the energy and critical infrastructure sectors from cyberattacks - Atlantic Council

2021-12-13 event | Host recap with own attributed policy remarks Source: www.atlanticcouncil.org

Emphasizes sustained investment, public-private resilience partnerships and scenario preparation; identifies uncertainty in policies and funding for upgrading old equipment.

Attribution / limitation: Host recap; other panelists' views are excluded.

ISA relevance: Policy incentives and management decisions for industrial modernization.

10. EnergySource Innovation Stream: Artificial Intelligence-based monitoring for securing industrial IoT and the energy transition from cyberattacks - Atlantic Council

2021-10-04 event | Host recap with own attributed policy remarks Source: www.atlanticcouncil.org

Rejects treating technology adoption as a compliance exercise and urges investors to consider cyber exposure across the energy ecosystem.

Attribution / limitation: Host recap; other panelists' views are excluded.

ISA relevance: Economic incentives and practical adoption policy.

11. Driving security in an unsecure world - NIST conference presentation

2018-11-07 | Named government-hosted presentation **Source:** www.nist.gov

Simonovich's presentation links industrial cyber risk to safety and production and outlines Charter of Trust principles, supplier requirements, certification and shared initiatives.

Attribution / limitation: Historical Siemens presentation. Corporate principles and quoted colleagues remain corporate or separately attributed; no claim of regulatory adoption.

ISA relevance: Business-facing governance, practical controls or policy participation; ISA interest remains unconfirmed.



Booz Allen

#3

Christopher Porter

Global Chief Information Security Officer
Booz Allen Hamilton

Current FAIR roster identifies Booz Allen CISO; JR directly confirms the recent transition. Prior Fannie Mae examples remain historical. [Current-role source](#)

Direct business email and telephone: not publicly verified.

[LinkedIn profile](#) | [Named professional biography](#) / [public route](#)

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

First-group qualification. ISA introduction lead; active major-firm CISO with FAIR/VERIS and decision-oriented governance expertise.

Research rank #3 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

Booz Allen's May 22, 2026 earnings release reports FY2026 revenue of \$11.2bn and 31,500 employees at March 31, 2026. \$75,000 is approximately 0.00067% of annual revenue. Fiscal-year figures are used, not calendar-year estimates. [Source: investors.boozallen.com](#)

Proposed company benefit: Clearer investment, risk-acceptance and workforce decisions grounded in current Booz Allen priorities.

Proposed executive benefit: Peer validation and director engagement for his quantitative-risk and workforce approaches.

What This Recruit Could Add to ISA

Present a decision case showing how quantified loss changes investment, data handling and risk acceptance. [Source: thecyberwire.com](#)

Handbook connection: Tool K 66-68; L 69-71. Proposed output and benefits require agreement. [Source: www.nacdonline.org](#)

Introduction and next decision

JR Williamson, Leidos. Direct first-person follow-up plan; not a completed introduction. Allow time in new Booz Allen role. [Source: mail.google.com](#)

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Own FAIR remarks on risk appetite, enterprise governance and regulator communication; no verified testimony for this identity.

No additional authoritative policy-history evidence was established in the deeper check. This is an evidence gap, not proof of no policy involvement.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	JR Williamson, Leidos. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

ISA public board / meeting baseline | Bylaws | Published sponsorship

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Name-matched image on named public biography. Source: www.fairinstitute.org

Company mark: Current employer website brand asset Source: www.boozallen.com

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Baseline source

October 29, 2024 | Direct CyberWire interview transcript [Source: the cyberwire.com](https://the cyberwire.com)

Explains how data, coding, economic and behavioral skills can help cyber teams and discusses business ownership of security.

Attribution / limitation: Fannie Mae tenure. Statements by interviewer Simone Petrella are not attributed to Porter.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

2. Meet a Member: Christopher Porter

June 13, 2019 | FAIR Institute interview/podcast [Source: www.fairinstitute.org](https://www.fairinstitute.org)

Connects cyber loss to business revenue and downtime, prioritizes the security portfolio and describes business acceptance of financial risk.

Attribution / limitation: Historical examples; not current Booz Allen company policy.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

3. RSA 2020 FAIR program report

February 27, 2020 | Organizer's report of a conference presentation [Source: www.fairinstitute.org](https://www.fairinstitute.org)

The Porter section describes contractual changes around sensitive data and changes to cyber-insurance decisions arising from risk analysis.

Attribution / limitation: Publisher summary, not a sole-authored article. Other speakers' examples are excluded.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

4. Cyber regulators and good governance

November 22, 2024 | FAIR organizer's joint-session report [Source: www.fairinstitute.org](https://www.fairinstitute.org)

Reports a session involving Porter and James Lam on structured governance and communicating risk to regulators. Porter's attributed concluding point links better risk understanding to regulator discussions.

Attribution / limitation: Joint session; not every claim or named framework is Porter's.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

5. Feats of Strength: Chris Porter interview

June 2018 | Direct K logix magazine interview, printed pp. 20-21 [Source: www.klogixsecurity.com](https://www.klogixsecurity.com)

Describes reducing attack surface, improving visibility and using business language and transparency in leadership communication.

Attribution / limitation: Use the Porter interview only. Other interviews and Q&A in the same issue are not additional independent source items.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

6. Fannie Mae CISO calls for more data on security incidents | TechTarget

2018-08-01 | Original interview [Source: www.techtarget.com](https://www.techtarget.com)

Connects economic and psychological decision-making, incident data and organizational tradeoffs with cyber-risk management.

Attribution / limitation: Historical Fannie Mae role; current Booz Allen remit is separate. Only Porter-attributed remarks are used.

ISA relevance: Business-risk communication and evidence for investment decisions.

7. The security ratings game grades third-party vendors | TechTarget

2016-09-01 | Original attributed interview [Source: www.techtarget.com](https://www.techtarget.com)

Explains why periodic questionnaires miss changes in supplier risk and describes continuous ratings as one input rather than a complete solution.

Attribution / limitation: Historical Fannie Mae role; current Booz Allen remit is separate. Only Porter-attributed remarks are used.

ISA relevance: Third-party governance and proportionate assurance.

8. SANS WhatWorks: Supply Chain and Partner Security - Christopher Porter Q&A

Historical deputy-CISO period; exact publication date not established | SANS interviewer Q&A [Source: cdn.featuredcustomers.com](https://cdn.featuredcustomers.com)

Distinguishes vendor checklist compliance from assessing whether a partner has a functioning security program and the capability to manage risk.

Attribution / limitation: Historical Fannie Mae role; current Booz Allen remit is separate. Only Porter-attributed remarks are used.

ISA relevance: Practical supplier-assurance case for ISA guidance.

9. FAIRCON19 Video: CISOs from Fannie Mae, Highmark Health, Department of Energy, and Premise Health Talk FAIR Cyber Risk Quantification

2019-11-06 | Organizer report with own attributed remarks [Source: www.fairinstitute.org](https://www.fairinstitute.org)

Describes using financial loss estimates to make business owners confront the consequences of accepting a critical vulnerability.

Attribution / limitation: Historical Fannie Mae role; current Booz Allen remit is separate. Only Porter-attributed remarks are used.

ISA relevance: Risk acceptance, accountable owners and board decisions.

10. FAIRCON2020 Panel: How FAIR Can Help Better Integrate Cyber Risk with ERM (Video)

2020-10-29 | Organizer report with own attributed remarks [Source: www.fairinstitute.org](https://www.fairinstitute.org)

Explains the challenge of translating quantitative FAIR analyses into qualitative COSO oversight and using quantified risk appetite to clarify board reporting.

Attribution / limitation: Historical Fannie Mae role; current Booz Allen remit is separate. Only Porter-attributed remarks are used.

ISA relevance: Integration of enterprise risk management with cyber governance.



#4

Chris Betz

Chief Information Security Officer, Google Cloud

Google Cloud / Alphabet

Employer introduction and current authored posts confirm Google Cloud CISO; AWS role references are historical. **Current-role source**

Direct business email and telephone: not publicly verified.

LinkedIn profile | Named professional biography / public route

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

First-group qualification. ISA nominee; current cloud CISO with AI governance and director-focused contribution case.

Research rank #4 - ISA core recommendations. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

FY2025 Alphabet revenue \$402.836bn; 190,820 employees. Parent-group capacity, not a dedicated Google Cloud membership allocation. **Source:** www.sec.gov

Proposed company benefit: Clearer assurance of AI controls, shared responsibility and safe release decisions.

Proposed executive benefit: An opportunity to shape AI oversight guidance and compare operating lessons with senior peers.

What This Recruit Could Add to ISA

Build an AI launch and defense case with human approval, validation and measurable remediation outcomes. **Source:** cloud.google.com

Handbook connection: Tool E 48-50; F 51-53; K 66-68. Proposed output and benefits require agreement. **Source:** www.nacdonline.org

Introduction and next decision

Stephane Lenco, Thales. Direct first-person relationship and planned Chicago encounter; introduction consent/owner and current ISA sponsor status to confirm. **Source:** mail.google.com

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Own AI-governance and board-accountability articles plus discussion of public-private security collaboration; formal policymaking or testimony remains unverified.

No additional authoritative policy-history evidence was established in the deeper check. This is an evidence gap, not proof of no policy involvement.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Operating practitioner fit supported by research. ISA acceptance and employer designation pending.
Board feedback / introducer	Stephane Lenco, Thales. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

ISA public board / meeting baseline | Bylaws | Published sponsorship

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Exact asset observed on named public source. Source: cloud.google.com

Company mark: Authentic Google Cloud mark recovered from established brief Source: cloud.google.com

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Cloud CISO Perspectives: The 4 lessons that guided AI Threat Defense | Google Cloud Blog

June 16, 2026 | Authored company article [Source: cloud.google.com](https://cloud.google.com)

Describes preparing, scanning, prioritizing, remediating and improving defenses around business context rather than treating AI as a stand-alone purchase.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

2. Cloud CISO Perspectives: How Google Cloud Security uses AI internally | Google Cloud Blog

June 29, 2026 | Company article coauthored with Ruchi Shah [Source: cloud.google.com](https://cloud.google.com)

Describes internal AI-assisted launch reviews and exploit reproduction, with validation and human intervention for higher-risk decisions.

Attribution / limitation: Company self-report, not independently measured product assurance; coauthored.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

3. Cloud CISO Perspectives: Why AI Threat Defense is the new boardroom baseline | Google Cloud Blog

July 31, 2026 | Company article coauthored with Alicja Cade [Source: cloud.google.com](https://cloud.google.com)

Sets out board questions about business enablement, remediation speed, consolidated tools, contextual prioritization and safeguards for AI.

Attribution / limitation: Joint argument; performance claims remain company-reported.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

4. Cloud CISO Perspectives: Sticking to security fundamentals in the AI era | Google Cloud Blog

August 21, 2026 | Authored company article [Source: cloud.google.com](https://cloud.google.com)

Argues AI should reinforce identity controls and layered defense; higher-risk actions need human review and business leadership remains essential.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

5. Google Cloud's New CISO Chris Betz on Integrating AI in Cyber Defenses

July 7, 2026 | Direct published interview [Source: www.infosecurity-magazine.com](https://www.infosecurity-magazine.com)

Discusses AI-driven threat defense and the value of security collaboration across the public and private sectors.

Attribution / limitation: Interview establishes priorities, not a commitment to ISA or independently verified outcomes.

ISA relevance: ISA governance and management contribution; see the prior individual assessment.

6. AWS Security Profile: Chris Betz, CISO of AWS | AWS Security Blog

2023-11-21 | Company-hosted Q&A [Source: aws.amazon.com](https://aws.amazon.com)

Describes customer trust, shared responsibility and reducing security complexity from the perspective of a former cloud customer.

Attribution / limitation: Historical AWS role; current Google Cloud affiliation is separate. Company claims are not independently audited.

ISA relevance: Clear provider/customer responsibilities and business value.

7. How the unique culture of security at AWS makes a difference | AWS Security Blog

2024-04-17 | Self-authored company article [Source: aws.amazon.com](https://aws.amazon.com)

Treats security as a business imperative supported by leadership access, service ownership and a culture that learns from errors.

Attribution / limitation: Historical AWS role; current Google Cloud affiliation is separate. Company claims are not independently audited.

ISA relevance: Management accountability and practical governance.

8. Introducing the AWS Trust Center | AWS Security Blog

2025-02-14 | Self-authored company article [Source: aws.amazon.com](https://aws.amazon.com)

Explains how a public trust center makes security practices, compliance programs and data-protection controls easier for customers to inspect.

Attribution / limitation: Historical AWS role; current Google Cloud affiliation is separate. Company claims are not independently audited.

ISA relevance: Evidence-based supplier assurance and transparency.

9. AWS CISO: In AI gold rush, folks forget application security

2024-05-13 | Original direct interview [Source: www.theregister.com](https://www.theregister.com)

Warns that rushing AI products to market can leave conventional application security behind; distinguishes training, model and application layers.

Attribution / limitation: Historical AWS role; current Google Cloud affiliation is separate. Company claims are not independently audited.

ISA relevance: AI launch governance and allocation of responsibility.

10. AWS CISO On Cybersecurity 'Baked Into' Chips, Security Services And Marketplace

2025; exact date not exposed | Original direct interview [Source: www.crn.com](https://www.crn.com)

Describes built-in infrastructure security, a shared customer foundation and partners' complementary capabilities rather than a single complete security solution.

Attribution / limitation: Historical AWS role; current Google Cloud affiliation is separate. Company claims are not independently audited.

ISA relevance: Secure design and ecosystem responsibility.

HOLD



Freund Advisory

Jack Freund

Founder, Freund Advisory Group; Acrisure role requires reconciliation

Freund Advisory Group / Acrisure affiliation disputed

Own advisory firm is current public evidence; IANS still lists Acrisure. Sponsor and employment reconciliation remain open. Website uses a text wordmark; no separate graphic logo was found. [Affiliation source](#)

CONTACT | Direct business email and telephone: not verified.

[LinkedIn profile](#) | [Public professional contact route](#)

Recommendation and next decision

Confirm present employment directly. Identify a suitable current paying organization before restoring membership priority. ISA-recommended introduction remains recorded.

ISA relationship and introduction

ISA feedback identifies a willing board-member introduction; member name and relationship confirmation pending.

Image and brand provenance

Authentic published headshot. IANS portrait; employer text may be outdated. [Portrait source](#)

Brand: Own website text wordmark, reproduced as text. [Brand source](#)

Jack Freund | Company and ISA contribution

Freund Advisory Group is an independent advisory practice. Current revenue, staffing and an eligible corporate sponsor are unverified. Acrisure historical scale cannot support a current funding case. [Source](#)

Specific proposed contribution

A worked example linking one business objective to loss scenarios, validated financial risk measures, investment choices and residual risk; an AI vendor-risk scenario is a secondary option.

Proposed executive benefit

Test his quantitative risk communication with directors and senior security peers; validate whether this supports his current professional priorities.

Proposed company benefit

A current sponsoring organization could test a business-loss scenario and AI vendor-risk decision against ISA director questions. Identify the sponsor and its specific objective before proposing membership.

ISA connections

Risk measurement must change an actual business decision

Tool K, “Board-Level Cybersecurity Metrics,” pp. 66-68, addresses financial exposure, risk appetite and spending alignment. Tool L, “Example Cybersecurity Board Reporting,” pp. 69-71, provides a reporting structure. Propose a worked decision, rather than a generic metrics presentation.

The published ISA/NACD webinar schedule includes metrics on November 19, 2026; confirm delivery and dates.

Scope the scenario around the business objective

Use Tools K and L to define a business-specific loss scenario and report expected exposure and residual risk in terms directors can evaluate. This draws on his published risk-analysis expertise. Validate its usefulness to an eligible current sponsoring organization; neither current Acrisure employment nor Acrisure sponsorship is established. His FAIR-related work is not an ISA endorsement.

A possible board contribution is a scenario that explains which control or insurance decision changes when the loss estimate changes.

Frontier AI requires more specific vendor oversight

Tool E, pp. 48-50, and Tool H, “Board Oversight of Third-Party and Supply Chain Cyber Risk,” pp. 57-59, give concrete questions on access, vendor responsibilities and dependencies. Test a scenario involving model change, data handling and vendor outage.

Only the public IANS excerpt was reviewed; the full report is gated. The published schedule lists AI on October 20 and third-party risk on September 15, 2026; replay availability is unverified.

Jack Freund | Substantive public sightings

5 reviewed items. These sources retain their dates and limits; no ten-item completion claim is made.

01 | Baseline source

June 11, 2026 | Single-author public IANS excerpt

Identifies model changes, sensitive input handling, concentration and unreliable outputs as issues that ordinary vendor-risk reviews may miss. [Open source](#)

Limit: Full report is gated; findings here are limited to the public excerpt.

02 | Why cybersecurity needs more than good intentions

April 7, 2025 | Single-author ISACA article

Advocates transparent, empirically validated risk models, enterprise-risk integration and investment decisions aligned to risk appetite. [Open source](#)

Limit: This is the author's argument; it does not prove adoption at Acrisure.

03 | From measurement to management

September 1, 2024 | Single-author ISACA Journal article

Connects financial risk analysis to budgets, insurance, capital allocation and ongoing operating costs. Risk appetite and funding should be evaluated together. [Open source](#)

Limit: The article's employer attribution is historical; no current Acrisure policy is inferred.

04 | Improve cyber-risk measurement through scenario scoping

February 23, 2021 | Authored NACD partner-content article

Starts with a business objective, scopes loss events and controls, then relates the analysis to enterprise risk and decisions. [Open source](#)

Limit: Published in a VisibleRisk partner-content context; affiliation is historical.

05 | Problems with using record count as a proxy for risk

September 14, 2020 | Single-author ISACA article

Explains why record counts miss business value and argues for financial loss ranges and the organization's tolerance for those losses. [Open source](#)

Limit: Historical viewpoint; no claim of Acrisure adoption or ISA endorsement.

HOLD



Michael Papay

Chief Information Security Officer and Chair, Advisory Board

Rohirrim

Western Alliance biography supports the Rohirrim role. Bank directorship does not establish membership purchasing authority.

[Affiliation source](#)

CONTACT | Direct business email and telephone: not verified.

LinkedIn profile | Public professional contact route

Recommendation and next decision

Hold until a recent statement and an authorized paying entity are established. Prefer a board-level introduction over assumed bank sponsorship.

ISA relationship and introduction

Tracie Grella directly knows Papay; JR Williamson directly reports recent conversation and poor current fit. Hold and reconcile with Larry before any approach.

JR Williamson directly reports fractional Rohirrim work of about one day weekly and considers Papay unsuitable at this stage. Larry's October 9 aggregate list still preserves a possible introduction. Reconcile the disagreement before any approach. [Board feedback](#)

Image and brand provenance

Authentic published headshot. Western Alliance director biography portrait. [Portrait source](#)

Brand: Official Rohirrim logo. [Brand source](#)

Michael Papay | Company and ISA contribution

A company-issued announcement reports a \$15m Series A in December 2023. Current revenue and employee count have not been verified. Funding is a scale indicator, not annual revenue or proof of capacity for \$75,000 sponsorship. [Source](#)

Specific proposed contribution

A practical AI governance discussion linking organizational data control to the board questions in Tool E; a workforce-policy discussion drawing on his congressional testimony.

Proposed executive benefit

Compare enterprise AI and workforce governance approaches with directors and policy peers; validate his interest and capacity.

Proposed company benefit

Rohirrim could test how its enterprise AI data controls address directors' questions about access, vendor oversight and business accountability. That is a proposed benefit, not evidence that Rohirrim would sponsor participation.

ISA connections

Organizational control of enterprise AI

Tool E, "Discussion Guide for Board Decisions on AI," pp. 48-50: examine AI access, unapproved use, vendors and accountability. A useful contribution would explain what directors should ask about sensitive proposal data, permissions and fallback arrangements.

The published webinar schedule includes an AI session on October 20, 2026. Confirm date and availability before outreach.

Workforce development across the career pipeline

ISA's Virtual Cybersecurity National Service Academy proposal offers tuition support linked to five years of government service. ISA publicly endorsed the Cyber PIVOTT Act; the House Homeland Security Committee reported advancement in February 2025. Discuss how job requirements and training could support this service pipeline.

The academy is a proposal. Committee advancement is not enactment. Inclusion of ISA's exact proposal in a national strategy still requires a specific documentary citation.

Security leadership and productive deployment

Tool J, "Building a Relationship Between the Board and CISO," pp. 63-65, offers a basis for discussing leadership communication and business decisions. Tool F, pp. 51-53, separately addresses retained responsibility for cloud security.

The 2011 cloud interview is historical; do not portray it as a statement about Rohirrim's present architecture.

Michael Papay | Substantive public sightings

5 reviewed items. These sources retain their dates and limits; no ten-item completion claim is made.

01 | Rohirrim advisory board appointment

February 26, 2024 | Company-issued release with direct attributed comments

Proposal burden, organization-controlled AI and security are the specific concerns raised. The release establishes his advisory appointment at that time; the newer Western Alliance biography establishes the CISO role. [Open source](#)

Limit: Vendor promotional context; product claims are not independently validated.

02 | House hearing on developing the cybersecurity workforce

September 7, 2017 | Prepared and oral congressional testimony; counted as one item

Calls for a continuous education and training pipeline, broader participation, and coordinated industry/government effort. The relevant speaker is Michael Papay, then at Northrop Grumman. [Open source](#)

Limit: Historical position. Other witnesses' statements must not be attributed to Papay.

03 | Baseline source

September 7, 2011 | Direct interview

Discusses building security into cloud services, adapting defenses to changing threats and cooperation across organizations. [Open source](#)

Limit: Older role and technology context; evidence of a documented viewpoint, not current company policy.

04 | Corporate information security leadership

February 19, 2014 | Northrop Grumman release with direct attributed comments

Emphasizes cooperation between CISO and CIO to introduce capabilities securely while supporting productivity. [Open source](#)

Limit: Company announcement about a conference appearance; limited depth beyond the attributed comments.

05 | Western Alliance board appointment

December 11, 2025 | Bank release with direct attributed comments

Expresses interest in applying technology and cybersecurity experience to the bank's growth and stakeholder goals. [Open source](#)

Limit: Limited-depth board-interest statement. It does not establish bank sponsorship, Rohirrim revenue or ISA interest.

EXISTING ISA RELATIONSHIP



Tim McKnight

Reported SVP, IT Risk Management & Security and CISO

Merck & Co., Inc.

Merck is a reported affiliation. ISA still lists UnitedHealth and his former ISA chairmanship; corporate sponsorship and current representation require reconciliation. [Affiliation source](#)

CONTACT | Direct business email and telephone: not verified.

Public professional contact route

Recommendation and next decision

ISA publicly lists McKnight and identifies him as a former chair, under UnitedHealth Group. Reconcile Merck affiliation, board seat and corporate sponsorship internally before any new membership approach.

ISA relationship and introduction

Established ISA relationship: ISA publicly lists McKnight as a board member and identifies his previous chairmanship. ISA must designate the current contact owner; no introduction assignment is confirmed. [ISA board source](#)

Larry's October 9 direction names Merck; May 2026 reporting also names Merck. Public ISA page and handbook retain UnitedHealth affiliation. Employer confirmation and account transfer/new-sponsor treatment are unresolved. [Board feedback](#)

Image and brand provenance

Authentic published headshot. ISA board portrait. [Portrait source](#)

Brand: Official Merck & Co. logo; reported affiliation, not confirmation. [Brand source](#)

Tim McKnight | Company and ISA contribution

FY2025 worldwide sales \$65.0bn, Merck & Co. company results. Merck & Co. is distinct from Merck KGaA.

Source

Specific proposed contribution

Patient-focused continuity, distributed security ownership and board assurance of business applications.

Proposed executive benefit

Compare patient-focused resilience and distributed security ownership with ISA peers; confirm current role and existing relationship.

Proposed company benefit

Proposed: Patient-focused continuity, distributed security ownership and board assurance of business applications. Validate company usefulness and sponsorship interest.

ISA connections

Security ownership extends into business units

Tool J, pp. 63-65; Tool G, pp. 54-56. Discuss how distributed ownership can support a patient-focused business continuity case.

Existing ISA relationship must be reconciled before any new-account approach; three reviewed commentary sources, not five.

Protect applications during transformation

Tool F, pp. 51-53; Tool H, pp. 57-59. Explore retained responsibilities and business dependencies in an enterprise application change.

Proposed connection, not an endorsement or confirmed ISA contribution.

Tim McKnight | Substantive public sightings

3 reviewed items. These sources retain their dates and limits; no ten-item completion claim is made.

01 | Merck Appoints Tim McKnight as SVP, IT Risk Management & Security and Chief Information Security Officer - CDO Magazine

May 18, 2026 | Secondary appointment report with attributed comments

The reported appointment quotes his emphasis on patient-focused mission, resilience and innovation. [Open source](#)

Limit: Limited depth and primary employer confirmation still needed; ISA already lists him as a board member.

02 | Preventing The Next Log4j With A Solid Security Culture

January 20, 2022 | Attributed comments in SAP-sponsored article

Discusses shared security goals, business information security officers and security culture rather than relying solely on a central security function. [Open source](#)

Limit: Historical SAP role and promotional setting; not Merck policy.

03 | Onapsis Appoints Tim McKnight to Board of Directors - Onapsis

April 4, 2024 | Company release with direct attributed comments

Connects business-application protection to visibility and governance during enterprise transformation. [Open source](#)

Limit: Appointment announcement is limited commentary; outside director role is not an assumed sponsor.

MICROSOFT REFERRAL CONTACT



Igor Tsyganskiy

Global CISO; added responsibility for Microsoft Research

Microsoft

His public announcement says he took responsibility for Microsoft Research in addition to his Global CISO responsibilities. Confirm intended contact and present remit before a referral request. [Own announcement](#)

CONTACT | Direct business email and telephone: not verified.

[LinkedIn profile](#) | [Public professional post](#)

ISA direction

Ask the designated ISA members to request one suitable Microsoft management nominee through their intended Igor contact. Microsoft remains one account; this is a referral route, not an eighth qualified board candidate.

Required confirmation

Name the introducing ISA members, verify their relationship and intended contact, reconcile existing Microsoft membership, and confirm the nominee, executive interest, eligibility, company sponsor and approval route.

Image and brand provenance

Headshot cropped from the right-hand portrait in the March 11, 2026 GeekWire article, identified as Igor and credited to LinkedIn. No synthetic image. [Portrait source](#)

Official Microsoft logo. [Logo source](#)