THE CISO SUMMIT

INSIDER THREAT:
REDUCING THE RISK WITH OPERATIONAL REGULATORY COMPLIANCE

ISRAEL D. ESQ
Founder & Lead Consultant (Information Security Architects Ltd)
Member, EC-Council BETA Testing Committee

SPEAKER PROFILE

DESMOND ISRAEL ESQ.

Lawyer and Data Privacy/Information Security Practitioner

Founder & Lead Consultant, Information Security Architects Ltd (Rapid7 Gold Partner)
Lecturer, Ghana Institute of Management and Public Administration (GIMPA) School of Law
Consulting Partner, Legal Afrique Unlimited, Ghana
Non-Executive Director, Zerone AnalytiQs, British Columbia, Canada
Member, EC-Council's Beta Testing Committee, United States

Memberships:

Ghana Bar Association (GBA)
International Information System Security Certification Consortium (ISC2)
International Association of Privacy Professionals (IAPP)
Institute of ICT Professional Ghana (IIPGH)
Internet Society-SIG(Cybersecurity & Online Safety)
Exam Development Volunteer, ISC2

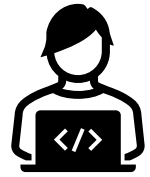
Certifications:
Verified Certicate (Cyberwar, Surveillance and Security)
CISSP, CIPM, CCT, CC

20 Years of Industry Experience

desmond.israel@gmail.com | Linkedin.com/in/desmondisrael | @desmond_israel | +233244284133

PLAN FOR TODAY

- Statistics
- Basis of Insider Threat
- The Insider Threat Risk Spectrum
- Convergence of Cyber & Regulatory Compliance
- Practical Strategies for Risk Mitigation
- **Future Outlook:** Emerging Technologies & Insider Threats
- Conclusion & Wake-Up Call



LEARNING OBJECTIVES

Implement a Holistic Insider Threat Strategy

Integrate Regulatory Compliance into Insider Threat Mitigation

STATISTICS ON INSIDER THREAT

Insider threats account for **over 60% of data breaches** with increasing year-on-year costs.

The **average cost per insider incident** now exceeds **$15 million**

70% are caused by negligence, but **malicious insiders** cause the most financial damage.

“In the past year(s), organizations have seen several serious data breaches committed at the hands of insiders.” — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

STATISTICS ON INSIDER THREAT

The charts on this page illustrate data captured within the CERT Insider Threat Incident Repository.

Insider Threat Incident Types

Figure 2: Insider Threat Incident Types (n=1314)

Estimated Financial Impact

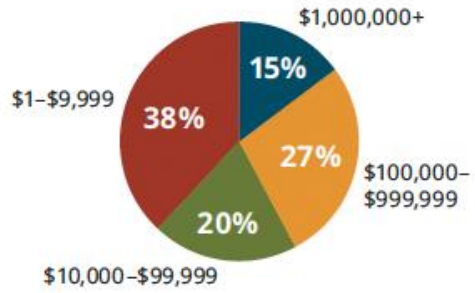


Figure 3: Estimated Financial Impact (n=1179)

Victim Organization Industry Type

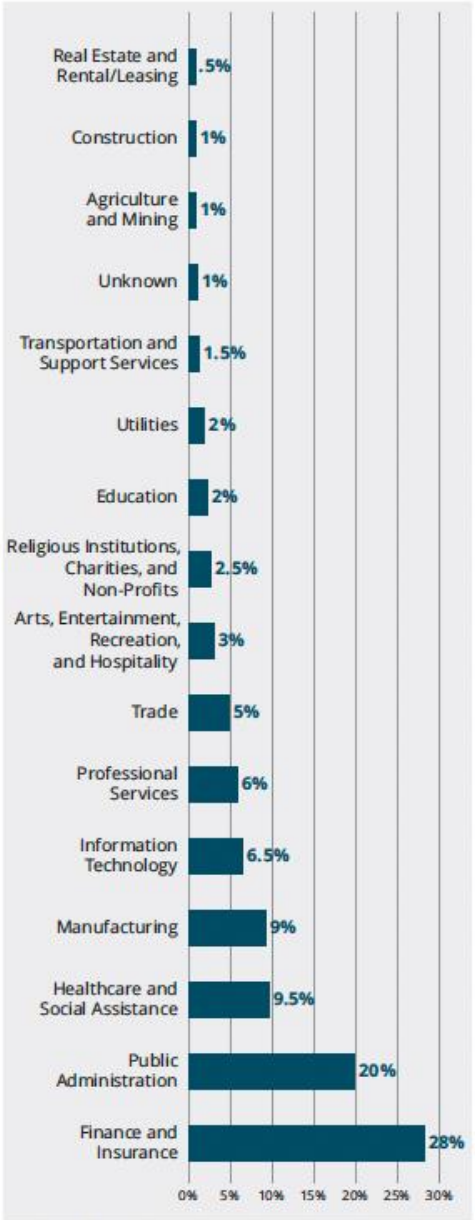


Figure 8: Victim Organization Industry Type (n=1515)

Top Five Stressors

	Incidents
1. Termination	375
2. Resignation	245
3. Internal Position Change	55
4. Organization M&A Activity	43
5. Emerging Financial Problems	33

Figure 4: Top Five Stressors Across Insider Threat Incidents

Top Five Concerning Behaviors

	Incidents
1. Went to Work for a Competitor	89
2. Disgruntled	57
3. Suspicious Foreign Travel	55
4. Financial Conflict of Interest	53
5. Physical Property Theft	50

Figure 5: Top Five Concerning Behaviors Across Insider Threat Incidents

Top Five Data Exfiltration Methods Observed

	Incidents
1. Email	141
2. Removable Media	90
3. Paper	80
4. Web	61
5. Verbal	42

Figure 6: Top Five Data Exfiltration Methods Observed Across Insider Threat Incidents

Top Five Sabotage Methods Observed

	Incidents
1. Critical Data Modified	135
2. Critical Data Deleted	91
3. Denial of Service Attack—General	79
4. Malicious Code Inserted	42
5. Social Engineering	35

Figure 7: Top Five Sabotage Methods Observed Across Insider Threat Incidents

"Anticipate and manage negative issues in the work environment. Adopt positive incentives to align the workforce with the organization."
— *Common Sense Guide*, Insider Risk Management Program

BASIS OF INSIDER THREATS

“To ensure protection of intellectual property… systems and data… and respond in a consistent, timely, and quality manner…” — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

Categories

- Negligent
- Malicious
- Compromise

Intent vs. access vs. impact: the insider risk trichotomy

Human, behavioural, and technical elements converge to create insider risk.

THE INSIDER THREAT RISK SPECTRUM

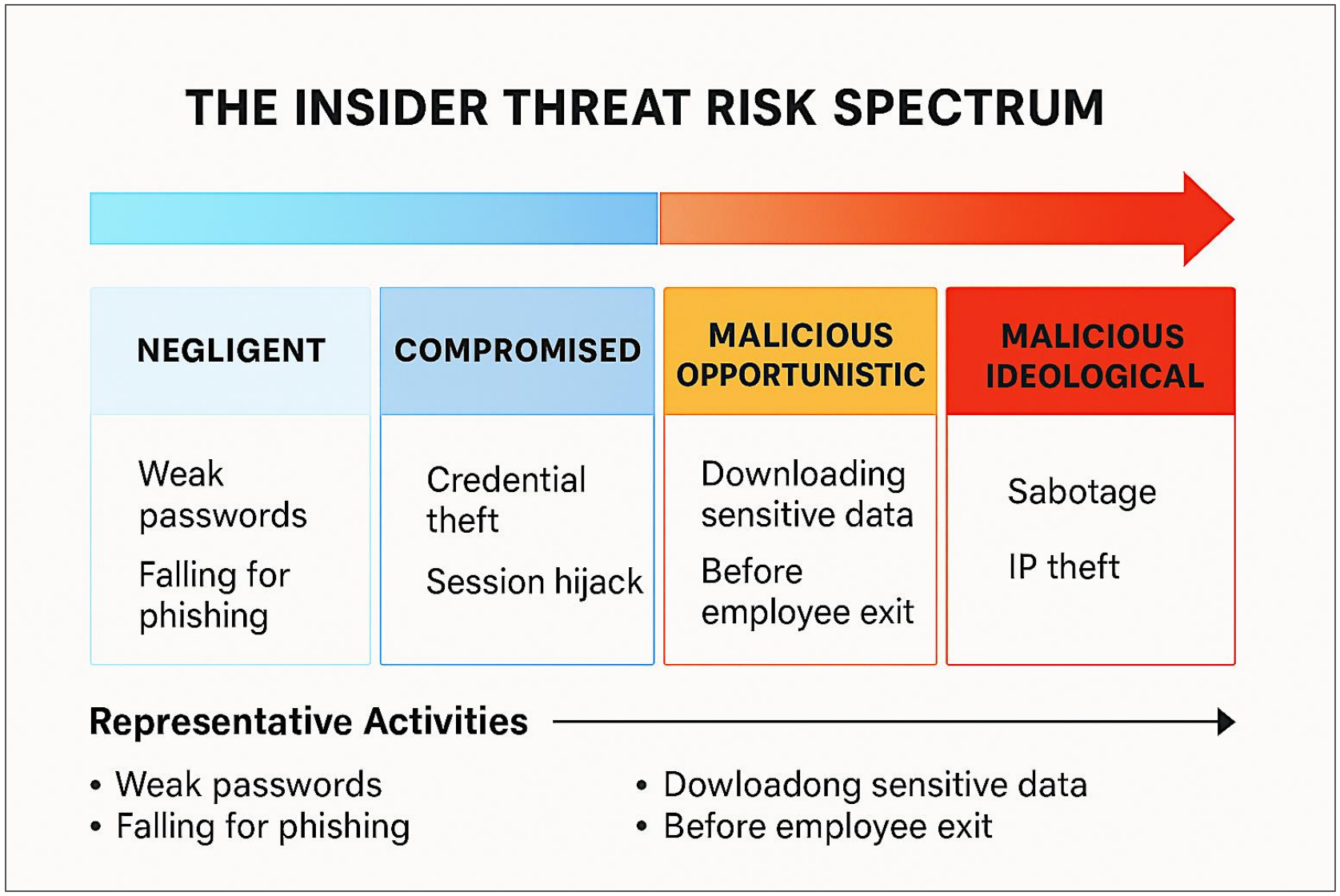
Build a **threat-intent-impact** spectrum from inadvertent behaviour to ideological sabotage.

Include real-world examples of each risk level.

Assess each type using a **severity score** (impact × likelihood × detectability).

"Create a high-level view of information that can prioritize alerts and observables based on severity." — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

THE INSIDER THREAT RISK SPECTRUM



CONVERGENCE OF CYBER & REGULATORY COMPLIANCE

The intersection of insider risk controls and compliance mandates (industry standards, legal, policies etc)

Privacy, **legal defensibility**, and internal audit alignment.

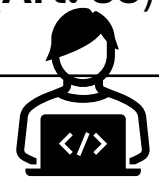
Compliance is not the ceiling—it's the foundation.

"Documentation of metrics and improvement activities may be relevant to regulators."— *Measuring the Effectiveness of a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

"Ensure that all Insider Threat Program actions meet legal mandates and protect the rights and privacy of employees." — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

CONVERGENCE OF CYBER & REGULATORY COMPLIANCE

	NIST SP 800-53 Rev.5	NIST CF	NIST PF	CIS v7	Privacy Regulations (GDPR/DPA2012)
Mappings	**CM-2** Baseline Configuration **CM-8** Information System Component Inventory **PM-5** Information System Inventory **PM-8** Critical Infrastructure Plan **RA-2** Security Categorization	ID AM ID RA ID RM PR DS PR MA	ID.IM-P ID.BE-P ID.DE-P CT.DM-P CT.DP-P	Control 1 Control 2	Processing of special categories of personal data (**Art. 9, Sec. 96**) Security of processing (**Art. 32, Sec. 28**) Data protection impact assessment (**Art. 35**)



PRACTICAL STRATEGIES FOR RISK MITIGATION

A. Governance & Policy Foundation

Insider threat charter, response plan, data ownership matrix.

Stakeholder mapping: legal, HR, ethics, risk, operations.

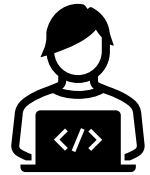
B. Insider Risk Management Program Evaluation (IRMPE) – Evaluating and Maturing the Program

Use the **IRMPE self-assessment** to evaluate maturity (MIL scale 0–5). Covers domains: **Program Management**, **Personnel & Training**, and **Data Collection & Analysis**.

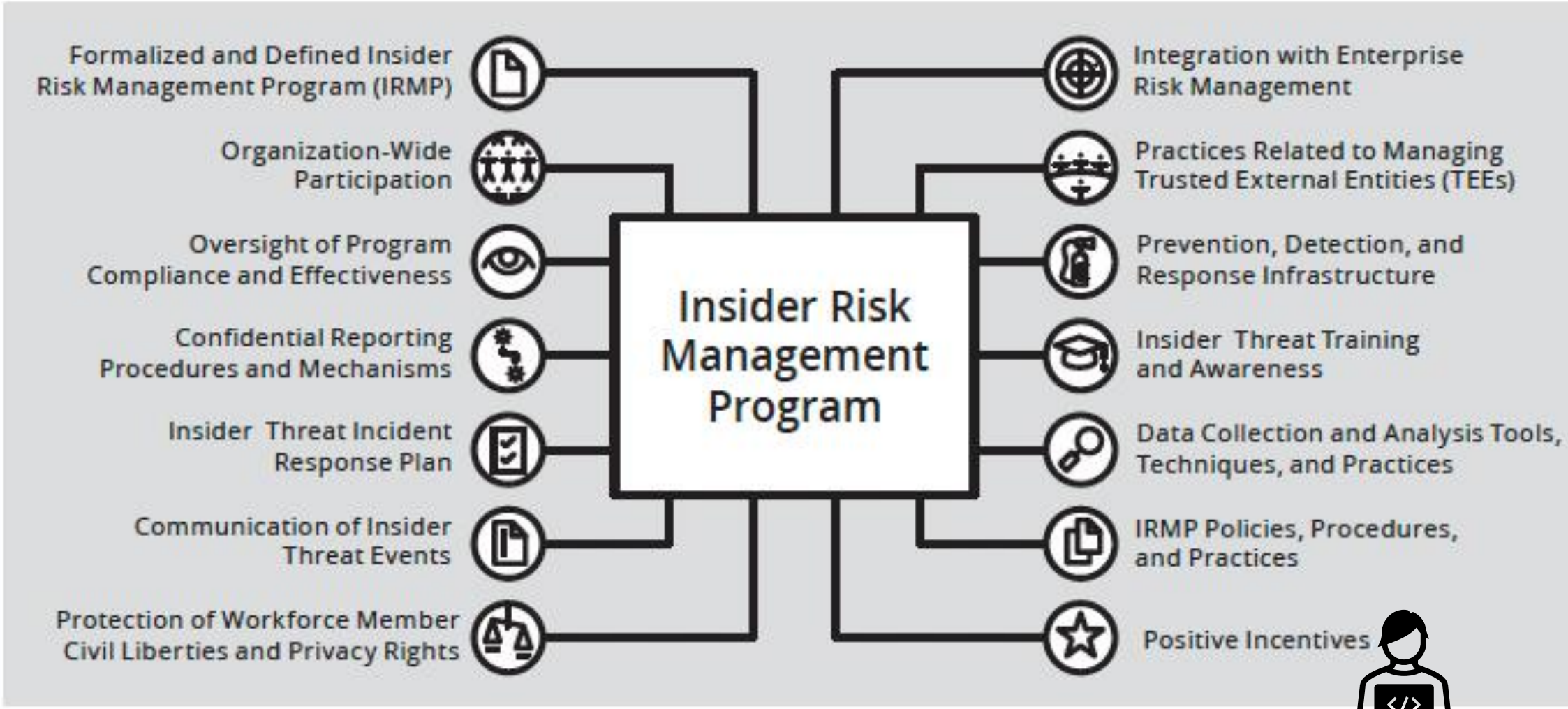
C. Technology Controls

UEBA, **SIEM**, **DLP**, **IAM**, and **behavioural analytics** integrated via a **centralized threat hub**.

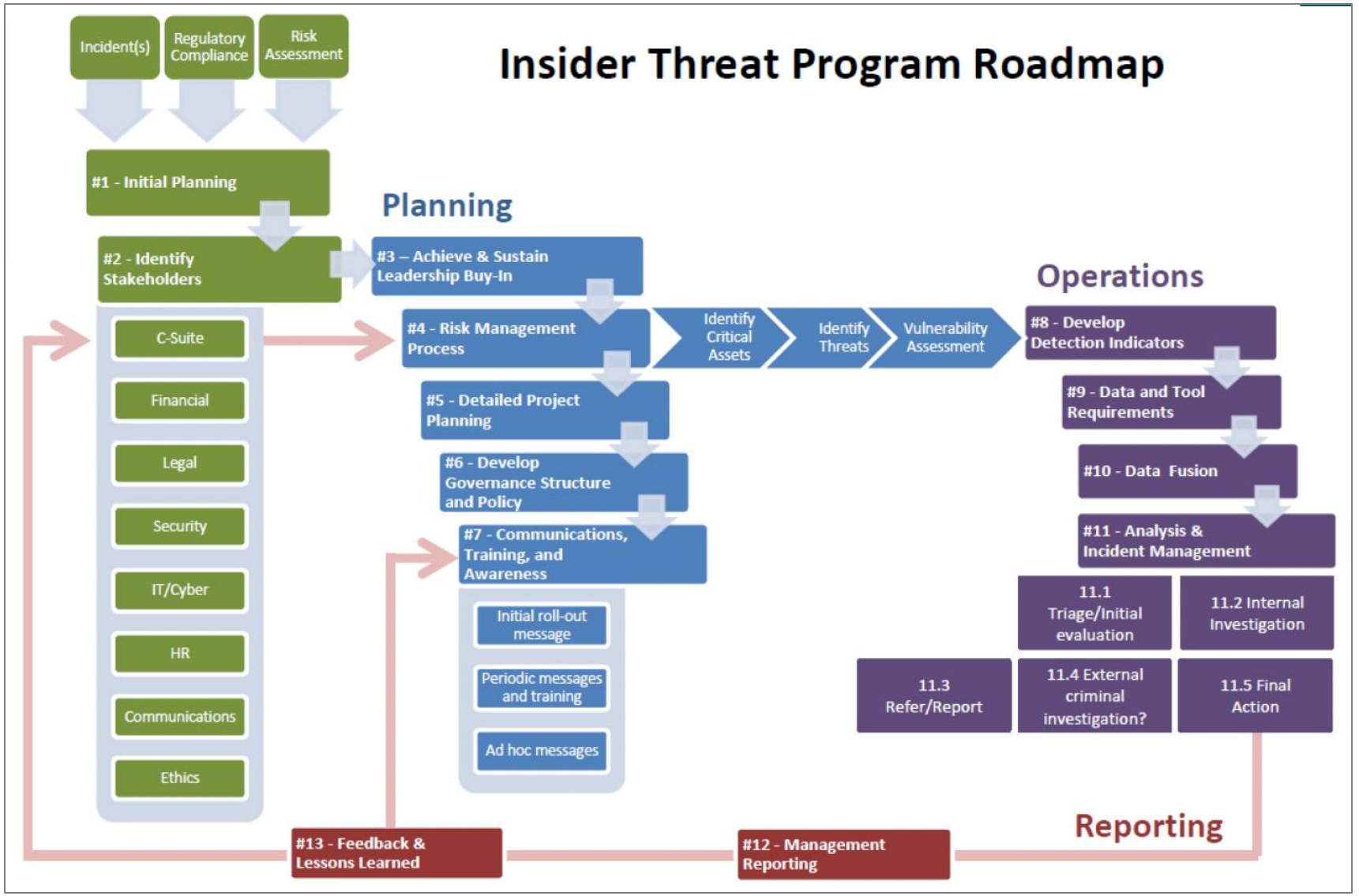
"Insider Threat Policy, Concept of Operations (CONOPS), Communications Plan..."— *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*



PRACTICAL STRATEGIES FOR RISK MITIGATION



PRACTICAL STRATEGIES FOR RISK MITIGATION



"Work with legal counsel and privacy officers in the development of the Insider Threat Program… ensure actions meet legal mandates and protect the rights and privacy of employees." — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

ISRAEL D. ESQ

THE CISO SUMMIT

FUTURE OUTLOOK: EMERGING TECHNOLOGIES & INSIDER THREATS

AI-enabled social engineering, deepfake impersonation, synthetic insider activity.

Risks from decentralized workforces and BYOD environments.

Next-gen monitoring: privacy-aware ML, sentiment analysis, biometric patterns.

“Machine Learning, Data Science – configure the systems that process massive amounts of data.” — *Designing and Implementing a Cyber Insider Threat Mitigation Program (Randall Trzeciak, 2024)*

CONCLUSION & WAKE-UP CALL

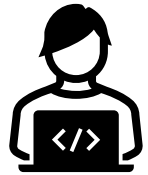
- Insider threats are **not just security problems—they're leadership problems**.
- Regulatory compliance is **the floor, not the ceilin**
- Build programs that are **measurable, resilient, an trusted** by the workforce.

Final Message

- **Run an IRMPE assessment** this quarter.
- **Formalize your insider threat charter** and review your tech stack.
- **Educate your executive suite** on the real cost of neglecting internal risks.

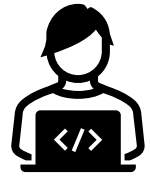
Call to Action

"Security isn't just about protection—it's about trust and resilience." — *Israel D. ESQ (Speaker, CISO SUMMIT 2025)*

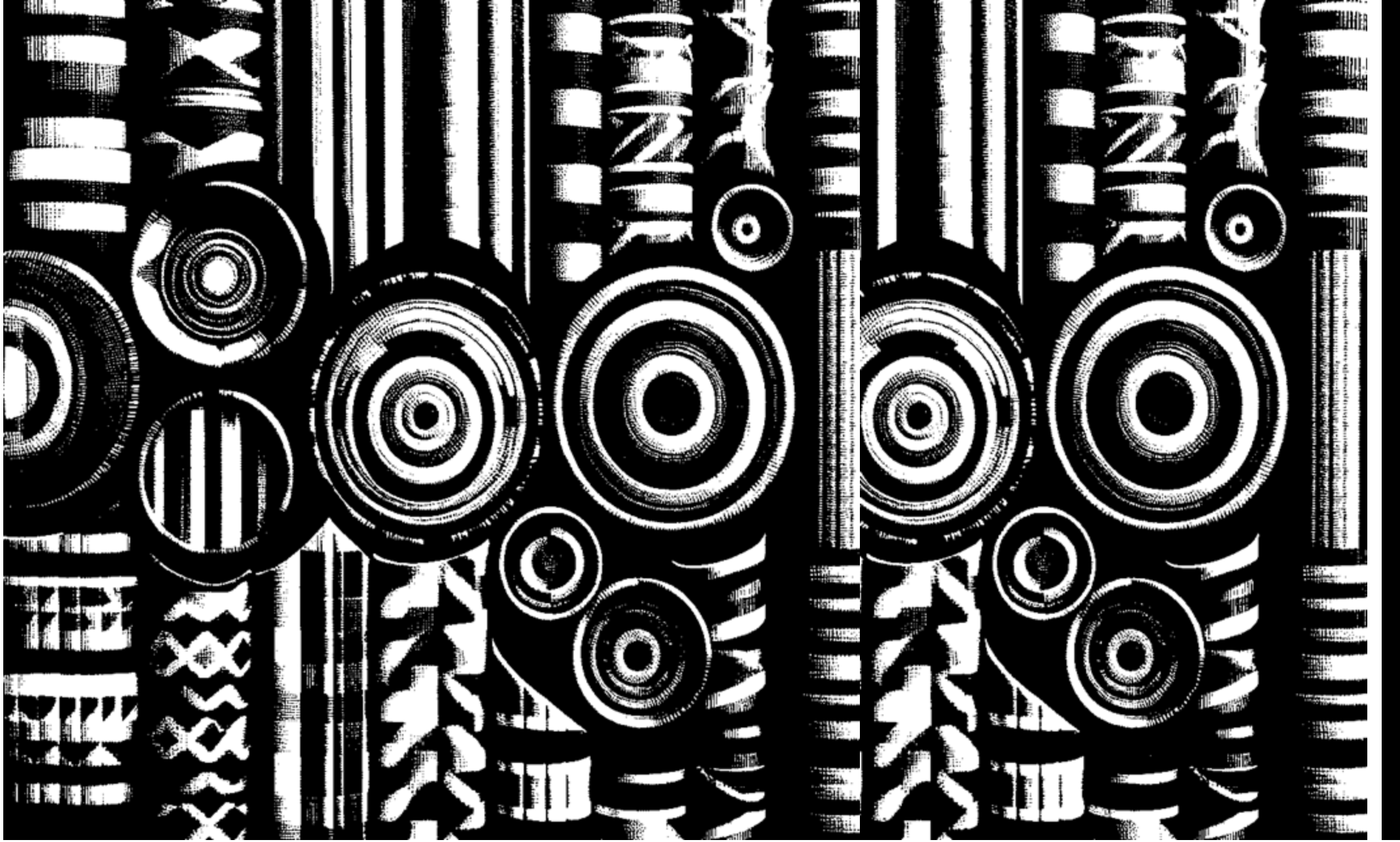


END OF SESSION

thank you



desmond.israel@gmail.com | Linkedin.com/in/desmondisrael | @desmond_israel |



THE CISO SUMMIT

ISRAEL D. ESQ