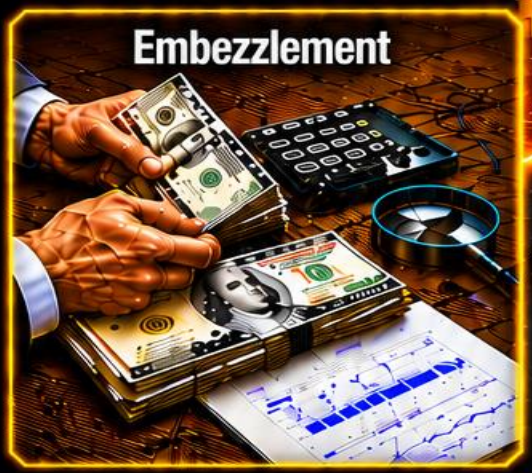
INSIDER RISK MANAGEMENT PROGRAM STAKEHOLDERS TRAINING COURSE & WORKSHOP



Offered By

Insider Threat Defense Group

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

INSIDER RISK MANAGEMENT PROGRAM (IRMP) STAKEHOLDERS TRAINING COURSE & WORSKSHOP ™

IRMP Stakeholder Certificate / Credential ™

TRAINING COURSE OVERVIEW

The Insider Threat Defense Group (ITDG) frequently gets calls from potential clients that have started trying to develop an IRMP, or mature the program, only for the program to stall because it lacks support from all key stakeholders or there is no clear roadmap for developing an IRMP.

IRMP Key Stakeholders:

IRMP Manager, Insider Threat Analyst, FSO, CSO, CISO, Human Resources, CIO – IT, Network Security, Governance, Risk & Compliance, Counterintelligence Investigators, Mental Health / Behavioral Science Professionals, Legal Etc.

Sometimes stakeholders within key departments are territorial, because they feel that the IRMP is trying to tell the stakeholders how to do their jobs. Or stakeholders think what they are doing is sufficient for Insider Risk Management. Sufficient is also what a determined malicious employee is looking for, security gaps, weaknesses and vulnerabilities in an organizations security controls to be successful in whatever their devious objectives might be. Other stakeholders may be reluctant to collaborate with the IRMP because of preconceived notions, privacy concerns or other misconceptions they have about the program.

Regardless of the reasons stakeholders have, the success of an IRMP is largely dependent on stakeholders sharing employee risk and threat information. **One of the most critical components for a program is for stakeholders to fully understand their roles and responsibilities and be universally aligned from an enterprise / holistic perspective to detect, respond to, investigate, prevent and mitigate Insider risks and threats**. There are many underlying and interconnected components that are critical for an IRMP to be comprehensive and effective.

It is critical that an IRMP be built on a solid IRMP Framework of non-technical and technical security controls for the program to be comprehensive and effective.

KEY BENEFITS OF THIS TRAINING COURSE

This **2 day** training course will provide the organization with a comprehensive IRMP Framework & Assessment Methodology 360 ™, that was developed by the ITDG, and is practical, real world, cost effective, proven, unique and holistic. Our framework has empowered organizations with the ability to implement, manage, evaluate and optimize a comprehensive IRMP, and transform existing programs from a siloed **REACTIVE** task into a shared **PROACTIVE** organizational responsibility.

The training will provide comprehensive guidance on conducting an Enterprise Insider Threat Vulnerability Assessment (EITVA). The EITVA is critical for an organization to be able to identify security weaknesses and gaps (Non-Technical, Technical) in key business units and in the organizations security foundations. The results or the EITVA will provide an organization with the ability to implement corrective actions. These corrective actions will enhance the organizations security posture, and can reduce the likelihood of malicious employees taking very financially damaging and other impactful actions against the organization.

The workshop portion of the training will include table top exercises using a variety of employee risk and threat scenarios, that will show the importance of collecting, integrating and analyzing various employee data sources (Internal, External) to identify potential or actual employee risks and threats.

Because of the collaborative and interactive nature of this training course and workshop, stakeholders will be able to engage and ask questions. This will ensure stakeholders have a comprehensive understanding of the importance of enhancing the security foundations of the organization, that can prevent data theft, financial theft, IT sabotage, prevent operational IT disruptions, downtime, loss of productivity, workplace violence, legal exposure and financial losses.

For over 10 years, the ITDG has encountered some organizations that have started developing an IRMP, from mostly a technical / employee monitoring and **RECACTIVE** perspective. This perspective will not provide an organization with a holistic and comprehensive program.

Starting the development of IRMP from a **PROACTIVE** prospective will ensure the organization has a clearly defined IRMP Roadmap / Framework that will make developing the program a much more smoother process. The roadmap serves as a strategic tool that outlines the core capabilities and scope of the program, stakeholder collaboration and responsibilities, resources required (Funding, Personnel), specific tasks to be completed within the program and across the enterprise, milestones and provides key metrics to show the return on investment the program is providing for the organization. Having a clearly defined IRMP Roadmap / Framework will also provide the CEO with a much more comprehensive short and long term plan for the program.

Regardless of the level of maturity that your IRMP is in, the ITDG is very confident that the training is structured to provide value whether participants are involved in building a new program, or looking to mature an established program. If your organization has an existing program, this training is a great way to benchmark and evaluate the program to see if there any security gaps in business units, or in the enterprise security controls.

This training is also an excellent opportunity to get all individuals managing and supporting an IRMP together, to educate and discuss the 2026 Insider Threat Landscape, and how Cyber Threats and Insider Threats are converging, making Insider Threat detection even more challenging. This will allow the program to re-calibrate to defend against the many new emerging types of Insider Threats**.**

PLEASE NOTE:

1) This training course can be tailored to the specific requirements of the organization**. 2)** The training can be conducted on-site or virtually. Based on past experience with previous clients, it is recommend that training be conducted onsite to ensure maximum engagement from stakeholders. **3**) Please call the ITDG at 561-809-6800 with any questions about the training and to receive a quote.

KEY TOPICS COVERED

MODULE 1: INTRODUCTION TO INSIDER THREATS

- ✓ What Are Types Of Insider Threats Your Organization Needs To Be Concerned With?
- ✓ Who Can Be An Insider Threat?
- ✓ Going Beyond Typical Definitions (Real World Examples & The Severe Impacts To Organizations)
- ✓ Insider Threats Overview, Damages & Impacts / Review Of Monthly Reports Produced By The National Insider Threat Interest Group (Eye Opening View Of The Severity Of Insider Threats)
- ✓ The 2026 Insider Threat Landscape And The Convergence Of Cyber Threats, Hackers And Employees
- ✓ Ghost Employees You Cannot See (Artificial Intelligence Agents)

MODULE 2: BUILDING AN IRMP ON A SOLID FOUNDATION OF SECURITY

- ✓ Identifying Key Information Assets (Data Inventory) And The Protection Strategies Required To Safeguard The Information (**Template Provided**)
- ✓ Security Policies And Procedures That Are Critical For Protecting An Organizations Assets (Templates Provided)
- ✓ Insider Risk Management Considerations For Artificial Intelligence Systems / Visibility Into Digital Employees You Cannot See
- ✓ Conducting An Enterprise Insider Threat Vulnerability Assessment To Identify Security Weaknesses & Vulnerabilities In Organizational Security Foundations (Non-Technical, Technical) (**Checklist Provided**)
- ✓ Employment Separation And Termination Procedures Checklist
- ✓ Eye Opening Demonstrations Of The Malicious Insider Threat Playbook Of Tactics For Stealing Information And Data As Easy As 1, 2, 3 (What Your Employees Monitoring Tools Might Be Missing)
- ✓ Evaluating Weaknesses / Vulnerabilities In Organizational Security Foundations (Non-Technical, Technical) (**Checklists Provided**)

MODULE 3: INSIDER THREAT MOTIVATIONS / BEHAVIORAL INDICATORS

- ✓ What Motivates Employees To Transform To Insider Threats?
- ✓ Employee Behavioral Indicator(s) Warning Signs / Risk & Threat Profile Generation (Non-Technical, Technical) (**Checklists Provided**)
- ✓ Contributing Organizational Risk Factors / Recognizing The Employer - Employee Trust Relationship Breakdown Indicators
- ✓ Understanding The Importance Of Going Beyond Pre-Hire Background Investigations To Identify Employee Problems / Concerns Using Employee Continuous Monitoring And Reporting (Post Hire, Case Studies, Solutions)

MODULE 4: IRM PROGAM (IRMP) GOVERANCE

- ✓ How To Define The Business Use Case, Return On Investment And Scope For An IRMP
- ✓ How To Gain Support And Buy In For The IRMP / Discussions With CEO, Board Of Directors, Executive Management (**Template Provided**)
- ✓ Understating The Rational For Alternate Names For An Insider Threat Program / IRMP
- ✓ What Are The Costs Related To Creating & Managing An IRMP? (Personnel, Budgeting, Resources Needed)
- ✓ IRM / IRMP Compliance Regulations / Understanding The Limitations And Risks Of Just Checking The Box
- ✓ Understanding The Employee Lifecycle & The Critical IRM Components And Key Stakeholder Responsibilities
- ✓ Creating An IRMP Governance Structure: Critical Roles, Responsibilities & Collaboration Required By Key Stakeholders For Employee Risk & Threat Information Sharing

- ✓ IRMP Development, Implementation, Management, Evaluation & Optimization A To Z
- ✓ IRMP Legal Considerations
- ✓ Essential Documentation Required For An IRMP (**Templates Provided**)
- ✓ Essential Data Sources For Insider Threat Detection / Investigations (Internal, External)
- ✓ IRMP Optimization (Risk Assessments, Gap Analysis & Strategic Planning)
- ✓ Providing IRMP Metrics To CEO / Board / Senior Management For Resources (Budget, Personnel) To Optimize The IRMP (**Template Provided**)

MODULE 5: INSIDER THREAT AWARENSS, REPORTING, INCIDENT RESPONSE & INVESTIAGTIONS

- ✓ Creating A Workforce Culture Of See Something, Say Something (**Insider Threat Awareness Training Materials Provided**)
- ✓ The Legal And Privacy Considerations On The Collection, Use And Sharing Of Employee Information
- ✓ The Legal And Privacy Aspects Of Workplace Employee Monitoring (Computers, Mobile Devices, Etc.)
- ✓ Creating The Procedures And Framework For Insider Threat Reporting, Conducting Investigations & Case Management (**Templates Provided**)
- ✓ Identifying, Collecting, Correlating And Analyzing The Technical / Non-Technical Data Sources (Internal, External) That Can Support An Insider Threat Investigation

MODULE 6: INSIDER THREAT MONITORING FOR COMPUTER SYSTEMS & NETWORKS

- ✓ Detecting Activity Indicative Of Insider Threat Behavior Using Network Security Tools (NST's) / User Activity Monitoring (UAM) Tools (UAMT's) (**Checklists Provided**)
- ✓ Performing A Gap Analysis To Evaluate The Strengths And Weaknesses Of Existing NST's & UAMT's s (**Checklists Provided**)
- ✓ Detailed Guidance Into The Various Capabilities & Features To Consider And Questions To Ask When Comparing Different Vendor UAM Solutions (**Checklists Provided**)

IRMP TOOLKIT ™

This training provides students a hardcopy handbook and an abundance of training materials, educational resources and templates needed for an IRMP. This will save many hours of documentation creation and makes developing or optimizing the a program almost as easy as 1, 2, 3. The toolkit will be provided to the students on a USB thumb drive or download link.

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDITS

Students attending this training will earn **16 CPE Credits** towards CPE requirements for security certifications they have obtained.

The IRMP Stakeholder Certificate / Credential will certify to organizations like the Defense Counterintelligence & Security Agency, that the student / stakeholder **1)** Has a comprehensive understanding of the operations of an IRMP, **2)** Understands the legal considerations on the collection, use and sharing of employee risk - threat information, **3)** Can identify essential data sources for Insider Threat detection (Internal, External), **4)** Understands the importance and collaboration required with the IRMP to detect, respond to, investigate, prevent and mitigate Insider risks and threats.

TRAINING RECOGNITION / STUDENT SATISFACTION & COMMENTS

Over **1000+** students have attended our training courses and endorsed them as the most affordable, next generation and value packed training for IRM, that are taught from a real world, practical, strategic, operational and tactical perspective.

Our very high levels of client satisfaction are the result of the ITDG being experts at building IRMP's, as we do more than just provide training. We also provide consulting services and incorporate lessons learned from our consulting engagements. **Our student satisfaction levels are in the EXCEPTIONAL range**. You are encouraged you to read the feedback from our students on this link.

COMPANY RECOGNITION

The ITDG Has Provided IRMP Training / Consulting Services To An Impressive List Of 700+ Clients:

White House, U.S. Capital Police, U.S. Secret Service, U.S. Government Agencies, Department Of War (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (FBI, DHS, TSA, DEA, USCBP, Police), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, ExxonMobil, Royal Canadian Mounted Police and many more. (Full Client Listing)

TRAINING COURSE INSTRUCTOR BACKGROUND

IRM is comprised of many different security disciplines that encompass, but are not limited to physical security, information security, computer / network security and other areas.

Mr. Henderson is an industry recognized IRMP Subject Matter Expert, that has 20+ years of experience, has protected classified information up to the TS-SCI level, has a broad background in many security disciplines, has received specialized training, holds numerous security certifications and received numerous awards for his contributions to the security field. (LinkedIn Profile)

- ✓ SCIF Accreditation / Compliance Inspections (Defense Intelligence Agency (DIA), Department Of Energy (DOE))
- ✓ ITP Program / IRM Analyst (DoD Insider Threat Counterintelligence Group / DIA)
- ✓ Senior Information Systems Security Manager (ISSM) For National Media Exploitation Center (DIA Sub Agency) (From Scratch Designed, Implemented And Managed A TS-SCI Information Security / Information Systems Security Program)
- ✓ Information System Security Training Course Instructor (Defense Counterintelligence Security Agency)
- ✓ Information Systems Security Program Management Training Course Instructor (Taught Class To 100 NSA ISSM's)
- ✓ Network Administrator (Department of Justice)
- ✓ Network Engineer (Critical Infrastructure Provider Of Water)
- ✓ Designated Approving Authority Representative / Certifier For TS-SCI Information System & Networks (DOE, DIA)
- ✓ Computer Forensics Investigator - Analyst (Central Intelligence Agency)
- ✓ Network Traffic & Intrusion Analyst (U.S. Special Operations Command)
- ✓ Technical Surveillance Countermeasure Inspections (Detection Of Electronic Covert Spy Devices) (DIA)
- ✓ Founder & Chairman Of The National Insider Threat Special Interest Group (NITSIG) / Largest Network (1000+) Of IRM Professionals In The U.S. & Globally

Additional Information

Please contact the ITDG with any questions you may have about this training.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
IRMP Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk - Threat Vulnerability Assessor
561-809-6800
www.insiderthreatdefensegroup.com
james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org