Education & Membership Guide

iSMG
INFORMATION SECURITY
MEDIA GROUP

Letter from the Editor

From headline-making data breaches to hacktivist attacks, there never have been so many high-profile incidents, which in turn have sparked greater public awareness of information security risks.

Tom Field

Now, more than ever, regulators, board members and even customers are asking smart questions about information security, fraud and compliance. You need to be prepared to give them informed answers.

At Information Security Media Group, we've assembled a broad suite of webinar training programs aimed at giving you the latest information you need about the ever-changing threat, compliance and technology landscape. Among the benefits:

- **Relevant Topics** – From mobile security to fraud prevention and how to conduct an effective risk assessment, we continue to produce new sessions that reflect today's top priorities.
- **Experienced Faculty** – For our virtual faculty, we draw upon industry thought-leaders, top consultants, current industry/security leaders, even federal regulators.
- **Convenience** – You don't need to travel off-site or even to a conference room to experience our programs. They are delivered straight to your desktop.

The ROI on our training programs is three-fold:

1. Cost-effective access to education that will help you in your job today;
2. Access to world-class leaders in our virtual faculty;
3. Ability, through our Membership Program, to gain on-demand access to our training library.

Please check out our latest catalog, and be sure to offer your own suggestions for new course offerings.

Tom Field,
Vice President, Editorial
Information Security Media Group

iSMG INFORMATION SECURITY MEDIA GROUP

Table of Contents

Compliance. Fraud. Risk Management. Whether you're IT or C-Suite, our courses have your team covered.

RISK MANAGEMENT
INFORMATION SECURITY
COMPLIANCE
FRAUD
Webinar Training
Risk Assessment Framework for Online Channel: Learn from an Expert
Incident Response Essentials: Regulatory

Our Mission

We task an expert faculty of industry professionals to develop a constantly expanding curriculum of exclusive education in the areas that matter most to financial institutions: information security, risk management, fraud, and compliance.

As industry trends change, new threats emerge, and regulations expand, so does our curriculum.

What Differentiates Our Education

Our presenter faculty consists of keynote level industry practitioners with years of experience implementing the areas their webinars focus on. Our experts include regulators and authors of regulations from the FDIC, authorities on risk management from NIST, and C-level information security professionals at financial institutions ranging from multinational to community banks.

A 350+ course curriculum provides a depth and breadth of education that can be found nowhere else. These sessions and accompanying handbooks deliver actionable advice and resources that can be implemented immediately to achieve business goals.

Sessions such as our series on Risk Management Framework: Learn from NIST are not a simple overview of how to conduct a risk assessment. Ron Ross, Sr. Computer Scientist and lead author of SP 800-37, details critical elements of NIST's Risk Management Framework, utilization of ongoing monitoring, and the key inhibitors many institutions face when implementing these procedures. Our webinars provide an insider's insight into the best course of action and how to avoid pitfalls others may become victim to.

Industry Insight

We understand that as the industry, threats, and regulations evolve, so do the needs of our members. We develop at least 50 new courses each quarter to stay ahead of the latest trends. These sessions are based not only on our educational advisory team, which includes experts from the ABA, NACHA, Gartner, and several banking institutions, but also input that comes directly from our current members.

Key Topics

We strive to provide the exclusive custom webinars to meet the needs of each and every member. Our internal staff has years of direct experience in the banking industry so we understand how quickly educational needs expand and how hard it is to rely solely on internal education or industry conferences. Since our key focus is information security, risk management, fraud, and compliance, we can provide a deeper curriculum and industry-specific relevance not found by other providers.

Education with Results

For these reasons, we have developed a comprehensive solution for risk management, information security, fraud and compliance professionals who demand details, not overviews; actionable advice, not checklist briefings; and custom-built, industry-specific education, not one-size-fits-all training. The banking community relies on these educational webinars to provide action items to put to work immediately to satisfy a direct business initiative.

iSMG
INFORMATION SECURITY
MEDIA GROUP

Don’t miss out. Join the other 45,000+ satisfied webinar attendees from thousands of organizations worldwide.

The Web Advantage

Essential education designed to ensure you meet and exceed your organization's security and risk goals.

Continually Expanding Curriculum

We task our expert presenters with developing new webinars continually throughout the year. On average, our curriculum increases by approximately 50 new courses each quarter. Coupled with the convenience of our online delivery, the latest education on the most recent threats, trends, and regulations is available as you need it.

A dedicated team of Membership Advisers speak directly with our member community to understand their needs and get custom webinar topics to develop and add to our webinar library.

First Look: New FFIEC Guidelines

Risk Assessments, Authentication Are Areas of Improvement

A preliminary draft of the new online authentication guidance from the Federal Financial Institutions Examination Council puts greater responsibility on the shoulders of financial institutions to enhance their security and prevent fraud. Read more...

ARTICLE

RSA Breach: A CISO's Action Items

How One RSA Customer Is Stepping Up Monitoring

Tracy Kitten, January 28, 2011 3:30 PM

Convenience

Convenience is essential when it comes to professional education. A volatile threat landscape, constantly changing industry trends, emerging technologies, and periodic regulatory updates make it difficult to stay up-to-date. Annual industry conferences and an aging internal education become outdated quickly.

Premium members gain unlimited OnDemand access to all sessions. They can even watch on mobile devices, including tablets and smartphones, making it easier than ever to stay up-to-date.

Comprehensive Education

We specialize only in the areas of information security, risk management, fraud, compliance, and governance for the financial industry. This is not general security awareness training or industry-generic security best practices. We've developed over 500 webinars by experts for experienced mid/senior-level professionals with core responsibilities in these areas.

The need to respond to regulators, upper management, other business units, and even customers on information security and risk management is ubiquitous. Our curriculum provides the one resource every institution needs to prepare.

Credit eligible articles, interviews, handbooks, and webinars are tracked and Proof of Attendance Certificates can be downloaded to submit to certifying associations for Continuing Professional Education (CPE) hours.

Expert Education & Discussion

We do not have an internal staff of webinar developers who research and create webinars. We rely solely on industry experts who have direct experience implementing the initiatives they are educating on. Regulators and regulation authors also speak directly from an insider's perspective to give insight and instruction on exactly what institutions will be audited on and how to be compliant.

With a Premium Membership, our expert faculty of practitioners can be directly corresponded with. Members can ask questions, provide their educational needs for custom webinar development, and even gain a peer-review of what others in the industry have successfully implemented.

Webinar Presenters

A who's who of banking and security leaders.

We work with actual practitioners at financial services organizations who speak directly from experience.

Training and education are only as effective as our experts and their expertise. That is why we utilize only the best and brightest in the financial industry to lead our webinars.

All of our presenters are carefully selected and coached to maximize their training effectiveness. Most have hands-on experience at financial institutions or regulatory agencies, and many have faced the same challenges you do. They have successfully navigated their way to a solution – which they will convey to you.

When it comes to the core objective of our training webinars, we stress the "how-to." After attending our sessions, you will walk away with definitive steps and practical advice that you can utilize at your own institution. Our presenters work hard to go beyond the theory and give solid advice you can immediately put into practice.

Presenter Biographies

Kirk Arthur

Supervisory Special Agent,
U.S. Secret Service Electronic Crimes Task Force and Asset Forfeiture Section, SF

Tim Barnett

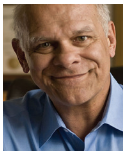
Chief Technology Officer,
Bluefin Payment Systems

Ori Bach

Senior Security Strategist,
Trusteer - IBM Security Systems

Seth Berman

Executive Managing Director,
Stroz Friedberg



Allan Bachman

Education Manager,
Association of Certified Fraud Examiners

Amy Blackshaw

Manager, Product Marketing,
RSA

Joseph Burton
Managing Partner,
Duane Morris LLP

Andrew Case
Core Developer,
Volatility Foundation

Randy Chartash
Chief, Economic Crime Section,
United States Attorney's Office

Claudel Chéry
Postal Inspector,
U.S. Postal Inspection Service

Peter Chronis
CSO,
EarthLink

Anton Chuvakin
Research VP,
Gartner GTP Security and Risk Management Strategies

Wendy Cohen
Global Data Security Executive,
Expedient Solutions, Inc.

Julie Conroy
Research Director,
Aite Group

Jeffrey Dant
Special Agent,
U.S. Secret Service

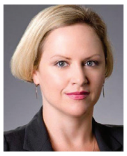
Joe Doetzl
CISO, Head of Cyber Security,
ABB Enterprise Software

Ed Ferrara
VP and Principal Analyst,
Forrester Research

Rick Gamache
CIO,
Red Sky Alliance

Liz Garner
Vice President,
Merchant Advisory Group

Shona Harper
Chief Privacy Officer, Europe & Asia-Pacific,
TD Bank



Katya Hirose
Dir. Global Risk & Investigations Practice,
FTI Consulting

Keith Hoover
Assistant to the Special Agent in Charge,
U.S. Secret Service

Presenters

Doug Johnson

VP & Senior Advisor, Risk Management Policy,
American Bankers Association

Shirley Inscoe

Senior Analyst, Retail Banking Practice,
Aite Group

Lance James

Head of Cyber Intelligence,
Deloitte & Touche

T.J. Horan

VP Product Management,
FICO

Neira Jones

Independent Advisor & International Speaker

Nikki Junker

Media Manager,
Identity Theft Resource Center

Kate Larson

Regulatory Counsel,
Consumer Bankers Association

Erez Liebermann

Deputy Chief, Criminal Division,
U.S. Attorney's Office, District of NJ

Avivah Litan

VP & Distinguished Analyst,
Gartner Research

Jon Long

Compliance Solutions Director,
CompliancePoint

David Lott

Payments Risk Expert, Retail Payments Risk Forum,
Federal Reserve Bank of Atlanta

John Lyons

CEO,
International Cyber Security Protection Alliance

Gregory Marrett

Principle Fraud Investigator,
Capital One

Rohan Massey

Partner,
McDermott Will & Emery UK LLP

David Matthews

General Counsel,
National Restaurant Association

Johnny May

Independent Security Consultant & Trainer,
Security Resources Unlimited, LLC

Dan McKenzie
Head of Enterprise Fraud Strategy,
RBC Bank

Dr. Dale Meyerrose
Major General,
U.S. Air Force, Ret.

Allison Miller
Senior Director, Platform Business Operations,
Electronic Arts

Eduardo Monteagudo
EVP,
First American Bank

Marco Morana
SVP,
UK Financial Institution

Garet Moravec
Former Head of Airborne Platform Systems Cyber Security,
Lockheed Martin Aeronautics

Kevin Morrison
Dir. of Global Security & Compliance,
The Results Companies

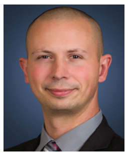
Graham Mott
Head of Development,
LINK Scheme

Anant Nambiar
VP & General Manager, Global Fraud & Security Solutions,
FICO

Jason Paguandas
Dir., Canadian Banking Fraud Strategy & Analytics,
RBC Bank

Malcolm Palmore
Assistant Special Agent in Charge,
FBI San Francisco Cyber Division

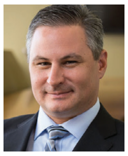
Michael Panico
Dir. Information Security, Content Protection,
Warner Bros.



Al Pascual
Senior Industry Analyst, Fraud & Security,
Javelin Strategy & Research

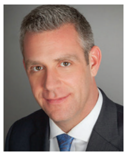
Kim Peretti
Partner,
Alston & Bird, LLP

Eduardo Perez
SVP, North America Risk Services,
Visa Inc.



David Pollino
SVP, Enterprise Fraud Prevention Officer,
Bank of the West

Presenters



David Pommerehn
Senior Counsel & AVP,
Consumer Bankers Association

Mark Pulido
Postal Inspector,
U.S. Postal Inspection Service, Chicago

Ronald Raether
Partner,
Faruki Ireland & Cox PLL

James Ratley
President & CEO,
Association of Certified Fraud Examiners

Nathalie Reinelt
Analyst,
Aite Group

Ellen Richey
EVP, Chief Legal Officer & Chief Enterprise Risk Officer,
Visa Inc.

Richard Rushing
CISO,
Motorola Mobility

Bob Russo
Transitioning General Manager,
PCI Security Standards Council

Sean Sanner
VP Analytics & Reporting Manager, Fraud Prevention Group,
Bank of the West

David Shroyer
Information Security Officer,
Ally Financial

Dennis Simmons
CEO,
SWACHA

Steve Strickland
Academy Founder & Senior Police Lead,
City of London Police

Mark Sullivan
Dir. Fraud Programs,
Interac Association

Michael Theis
Chief Counterintelligence Expert,
Carnegie Mellon University CERT Insider Threat Center

Russell Thomas
Data Scientist,
Zions Bank

Eric Thompson
IT Threat Strategist,
RSA

Randy Trzeciak

Tech Lead, Insider Threat Research Team,
Carnegie Mellon University CERT Insider Threat Center

Mike Urban

Dir. Financial Crime Portfolio Management,
Fiserv

James Van Dyke

President & Founder,
Javelin Strategy & Research

John Walker

Dir. CSIRT and Cyber Forensics,
Cytelligence

Matt Baker

Former Director of Intelligence,
AFCYBER (Air Force Cyber Command) and 24th Air Force

John Walp

Corporate Information Security Officer,
M&T Bank

Tim Webb

SVP, Fraud Management,
Citizens Financial Group

Tracy Wilkison

Deputy Chief, Cyber and Intellectual Property Crimes Section,
U.S. Department of Justice

Kirstin Wells

VP, Risk Officer,
Federal Reserve Bank of Chicago

Michael Wyffels

SVP & CTO,
QCR Holdings Inc.

Paul Yanowitch

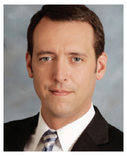
Assistant U.S. Attorney,
Northern District of Texas

Mitch Zahler

SVP, Cybersecurity,
HSBC

Todd Brungard

VP & BSA Officer,
Peapack-Gladstone Bank



Rob Zerby

VP, Financial Crimes Manager, Financial Crimes Operations,
Wells Fargo Financial Crimes Risk Management

Course Category Matrix

#	Course Title	ID
1	2014 Faces of Fraud	534
2	2014 Faces of Fraud Survey - Special European Edition	463
3	2014 Faces of Fraud Survey Presentation - Special Canadian Edition	448
4	2014 Identity Theft and Fraud Prevention Survey Results Webinar	567
5	2014's Top 10 Fraud Stories: What Lessons Can We Learn, and What Can We Expect in the Year Ahead?	537
6	2015 Faces of Fraud	542
7	2015 Insider Threat Report	609
8	5 Must-Haves for an Enterprise Mobility Management (EMM) Solution	527
9	Account Takeover 2014: Evolving Schemes & Solutions	421
10	Account Takeover, Payment Fraud and Spoofed Identities: The Common Thread	531
11	Account Takeover: Re-Assessing Strategies and Solutions	371
12	Actionable Threat Intelligence: From Theory to Practice	613
13	Advances in Application Security: Run-time Application Self Protection	523
14	Adversarial Machine Learning for Fraud Detection - How Can Organizations Benefit from the Pioneering Work of the NSA and Facebook?	473
15	Adversarial Machine Learning for Fraud Detection: How Can Organizations Benefit from the Pioneering Work of the NSA and Facebook?	480
16	Alerts that Matter: Prioritizing and Triaging Alert Data	468
17	Attacking Payment Card Fraud Where It Is Most Vulnerable: Voice Biometrics In the Call Center and The Shifting Legal Landscape	481
18	Automate and Standardize your IAM to Radically Reduce Risk	641
19	Beyond HIPAA Risk Assessments: Added Measures for Avoiding PHI Breaches	611
20	Big Data Analytics & Context-Aware Security	419
21	Big Data Analytics & Fraud Detection	592
22	Black Friday' Cybersecurity Challenges for the Banking & Merchant Community	526
23	Bridging the Gap Between Breach Prevention and Incident Response	417
24	Building a Banking DDoS Mitigation Strategy and the Evolving Security Threat Landscape	639
25	Business and Risk Based Framework Deployment	497
26	Call Center Fraud: The Latest Scams and Strategies - Voice Biometrics and Caller Validation	464
27	Case Study: How Threat Intelligence was Used to Defeat an Advanced Attack in Progress	571
28	Catch Criminals Before the Damage is Done - Mitigating Account Takeovers	361
29	CEO Bob Carr on EMV & Payments Security	560
30	Changing Perceptions and Attitudes - A New Way of Thinking About Defense	603
31	Chasing Down RAT's - Combatting Account Takeover Fraud at the Age of Remote Access Trojan's and Data Breaches	646

Big Data	Cybersecurity	Data Breach	Fraud	Governance	ID Theft	Mobility	Payments	Risk Management	Technology
		○	●			○			
			●	○				○	
			●						
		●	●		●				
		●	●				○		
			●						
	●	●							●
	●		○			●			○
			●						○
		●	●					○	○
			○						○
	●	●							●
									●
○			●						○
○			●						○
		●	○	○					●
			●						○
	●	●						●	●
								●	
●		○	●					○	●
●			●						●
		●							●
								●	●
	●	●						●	●
				●				●	○
			●						●
		●							●
			○		○			○	○
	○	○	●				●		
									●
	●	●							●

● = Primary Category   ○ = Secondary Category

Course Category Matrix

#	Course Title	ID
32	Cloud Infrastructure: Same Security Needs, Dynamic New Environment	566
33	Consumer Fraud Awareness: What's Working, What's Not & What's Next?	605
34	Creating Actionable Intelligence and the Visualization of Big Data Analytics	466
35	Customer Awareness: What Works in Fraud Detection, Prevention	423
36	Cyber Crime & Justice: The Need for Public/Private Collaboration	375
37	Cyber Investigations: How to Work with Law Enforcement	565
38	Cyber Threat Intelligence	491
39	Cybercrime Q&A with Federal Prosecutor Erez Liebermann	384
40	Data Breach Battle Plans for Financial Services	640
41	DDoS 2014: Expert Insights on Building a Better Defense	392
42	Developments in ATM Fraud	467
43	Digital Identity Verification for Fraud Mitigation	614
44	Dispelling the Myths of Malware Attacks	620
45	Dropsmacked and Boxed In: Understanding the New Threats in Online File Sharing	365
46	Fraud Investigation Life-Cycle: From Forensics to Working w/ Law Enforcement	410
47	Fraud Investigations & Navigating the European Legal Landscape	474
48	Fraud Investigations: How to Work Effectively with Law Enforcement, Government and Litigators	593
49	Fraud Outlook: Evolving Threats and Legal Minefields	428
50	Future of Payment Card Security	488
51	Healthcare - The New Cybercrime Target: How to Secure Your Data and Ensure HIPAA Compliance	617
52	Healthcare Information Security Today: 2014 Survey Results and Analysis	394
53	How Cybercriminals Use Phone Scams To Takeover Accounts and Commit Fraud	644
54	How DDoS Taught Competitors to Make Information Sharing Work	374
55	How to Fight Fraud with Artificial Intelligence and Intelligent Analytics	409
56	How to Implement the NIST Cybersecurity Framework Using COBIT 5	533
57	How to Tackle Vendor Risk Hazards: Operationalizing Third-Party Risk Management in Today's Regulated Environment	437
58	Identities - A Journey from Anonymous Bitcoin Fraud to Managing Verified Authentication	470
59	Identity Data Privacy is Dead: Why We Need to Migrate From Static Identity Verification to Dynamic Identity Proofing	541
60	Identity Theft vs. Identity Fraud	427
61	Identity Theft: How the Name Game Has Changed	583
62	Insider Fraud Detection: The Appliance of Science	585
63	Insider Threat: Mitigating the Risk	610

Big Data	Cybersecurity	Data Breach	Fraud	Governance	ID Theft	Mobility	Payments	Risk Management	Technology
									●
			●	●					
●			●						●
		○	●	●				○	
			○						○
				●					
●									●
			●						
	●	●						●	●
	●								○
			●						
	●	●							●
	●	●						●	●
	○							○	●
		○	●	○					●
			●						
			●	○					
			●						○
			●				●		○
	●	●							
								●	
	●	●	●						●
			○	○				○	○
		○	●		○				●
	●								
								●	●
			●		●				○
			●		○				
		○	●		●				
			●		●				
			●						
	●	●							

● = Primary Category ○ = Secondary Category

#	Course Title	ID
64	Investigate, Respond Retaliate?	496
65	Investigative Analytics: Velocity to Respond	554
66	Is Your Data Center Ready for Today's DDoS Threats?	441
67	Keynote: Advanced Persistent Confusion: Demystifying APT's and Cyber Attacks	595
68	Keynote: The State of Fraud Today	570
69	Leverage Mobile to Prevent Malware from Impersonating You	381
70	Looking for Anomalies: Try Machine Data	532
71	Malware Activity & Network Anomaly Detection	494
72	Managing Information Security Risk in Your Partner Ecosystem	366
73	Managing Insider Risks: How to Detect and Respond to Malicious and Unintentional Threats	426
74	Mobile Banking and Fraud	589
75	Mobile Deposit Capture: Balancing Fraud Prevention and Customer Convenience	615
76	Mobile Deposits & Fraud: Managing the Risk	572
77	Mobile Fraud	469
78	Mobile Fraud - Leveraging Threat Intelligence in Mobile Banking and the Risks of Virtual Currencies	487
79	Mobile Fraud: Understanding the Unknown and Reaping the Rewards of Mobile Banking	483
80	Mobile: Fraud's New Frontier	422
81	Mobile: Security Risk or Strength?	411
82	Online Banking Fraud Detection - Lessons from Brazil	472
83	Organized Retail Crime Rings in the Cellular Wireless Industry - ID and First Party Fraud	586
84	Overcoming Network Security & Compliance Challenges Impacting Healthcare Enterprises	391
85	Payment Card Fraud & the Future of Secure Payment	425
86	Payment Card Fraud and the Merchant Challenge	379
87	Payment Card Fraud Response: Taking on the Processor	424
88	Payment Card Fraud, EMV Adoption & the Merchant Challenge	412
89	Payment Card Fraud: The Present and the Future	482
90	Phase 1 - Establishing a Security Baseline - Inside and Out	597
91	Phase 2 - Cyber Threat Intelligence and OSINT: What You Can Learn About Your Adversaries and What They Can Learn About You	598
92	Phase 3 - Zero-Day Threats, Known Vulnerabilities and Anomaly Detection	599
93	Phase 4 - Security Analytics & Big Data	600
94	Phase 5 - Investigate, Respond, Retaliate? Focus First On The People And The Process, Not The Technology	601
95	PHI Security: The Role of Encryption and Tokenization	607

Big Data	Cybersecurity	Data Breach	Fraud	Governance	ID Theft	Mobility	Payments	Risk Management	Technology
○		○							●
	●			●					○
								●	●
	●								
			●						○
						○			○
	○	●							●
			○						●
								○	
			●					●	
			●			●			
	●	●				●			●
		●	●				●	○	○
			●			●			○
			●			●	○		○
			●			●			○
			○			●			○
			○			●			●
			●						○
			●		●	●			
	●								●
			●				●		○
		○	○				○		○
		○	●	○			●		
		○	●	○			●		●
			●				○		○
		●						○	
									●
●									●
		●		○					
	●	●							

● = Primary Category ○ = Secondary Category

Course Category Matrix

#	Course Title	ID
96	Policy Driven Security - Deploy Only Those Security Technologies and Controls That You Need	530
97	POS Security Essentials: How to Prevent Payment Card Breaches	568
98	Post-Fraud Investigation: Effective, Efficient, Defensible	376
99	Preparing For and Responding To Large Scale Data Breaches	539
100	Preparing for OCR Audits: Presented by Mac McMillan of the HIMSS Privacy and Policy Task Force	459
101	Preparing For The Ripple Effects Of EMV and The Future Of Payment Card Security	594
102	Preventing Security Breaches with Passwords That Can't Be Stolen	443
103	Privacy, Big Data and the Internet of Things: Where Do You Draw the Line?	395
104	Proactive DDoS Defense: Steps to Take Before the Attack	362
105	Real World Applications of Big Data Analytics - Social Network Analysis and Post Breach Fraud Detection	454
106	Reduce Call-Center Fraud - and Costs - While Improving Customer Satisfaction	398
107	ROI of Scalable Application Security	648
108	Scaling Security with Virtualized Infrastructure	460
109	Secure E-Banking: Consumer-Friendly Strong Authentication	580
110	Securing Mobile Banking: Authentication & Identity Management	415
111	Securing the Brave New World of Online Patient Information	433
112	Securing the Internet of Things	399
113	Security Alerts: Identifying Noise vs. Signals	576
114	Security Analytics	495
115	Security Baseline - The First Line of Weapon Delivery Defense	492
116	Security Without Compromise: One Approach for the Financial Services Industry	385
117	Solving the Identity and Access Problem Across Domains	386
118	Solving the Mobile Security Challenge	461
119	State of Global Fraud - Dealing with Today's Crimes and Anticipating Tomorrow's	462
120	Stop Mobile Payment Fraud, Not Customers	642
121	Stress Free Audits, Reduced Risk, Higher Confidence - How IAM Contributes to the Bottom Line	368
122	Targeted Attacks - 6 Keys for Fighting Back	616
123	Technology Spotlight: Identity Theft Protection Using Advanced Analytics	569
124	The Analyst's Eye: Top Fraud Threats to Watch in 2014	380
125	The Changing Landscape of Data Breaches & Consumer Protection in 2015	612
126	The Danger Within: Responding to Unintentional and Intentional Insider Threats	406
127	The Enemy Within: Responding to Insider Threats	373
128	The Evolution of Advanced Malware	618

Big Data	Cybersecurity	Data Breach	Fraud	Governance	ID Theft	Mobility	Payments	Risk Management	Technology
○			●	●					○
		●	●				●		
			○	○				○	○
		●	●						
		●				○			○
			●				●		
		●						●	●
●									●
								○	○
●		○	●						●
									●
	●	●							●
	○	○				●			●
	●								●
						●		●	●
		●						●	●
	●			●					○
	●	●							●
	●							●	
	●								
									●
									●
	●	●	○			○			●
			●	○				○	
	●	●							●
				●				○	○
	●	●							●
			●		●				○
			○					○	
	●	●							●
			●					○	○
			○					○	○
	●	●							●

● = Primary Category ○ = Secondary Category

Course Category Matrix

#	Course Title	ID
129	The Fraud Ecosystem and the Deep Web	535
130	The Fraud Ecosystem, Deep Web and Fraud-as-a-Service (FaaS)	588
131	The Fraud Ecosystem, the Deep Web & Creating Actionable Intelligence	451
132	The Future Of Payment Security: Where Do We Go From Here And Who Is Liable When We Get There?	540
133	The IT Security Requirements of Stage 2 Meaningful Use for Hospitals	382
134	The Mobile Banking Threatscape	372
135	The Next Stage of Fraud Prevention: Balancing Risk and Customer Experience	364
136	The Secret Fraud Eco-System and How to Put Threat Intelligence to Work	420
137	The State of APT	489
138	The Three Ds of Incident Response - Protecting Your Company From Insider Threats	403
139	The Trojan War: Responding to the Evolution of Cross-Channel Attacks	378
140	Threat Intelligence & the Underground Eco-System	478
141	Threat Intelligence and OSINT: What You Can Learn About Your Adversaries and What They Can Learn About You	544
142	Top 5 Fraud Stories Influencing 2015	645
143	Top Fraud Threats to Watch in 2014: Technology and Legal Ramifications	414
144	Trends in Account Takeover: Social Engineering & Evolving Malware	405
145	Understanding the Identity Risks You Experience, Not the Risks You Perceive - Identity Theft and Synthetic Identity	450
146	Upgrading to an APT-Capable Defense; Where to Start, How to Get Funding and See an Immediate Reduction in Risk	602
147	Visa on Future of Payment Card Security	413
148	Visualization of Big Data Analytics	484
149	Zero-day Threat Defense and Known Vulnerabilities	493

This matrix includes only our very latest sessions. For a full list of all 350+ courses, visit www.bankinfosecurity.com/webinars

Big Data	Cybersecurity	Data Breach	Fraud	Governance	ID Theft	Mobility	Payments	Risk Management	Technology
		●	●						○
			●						
○		●	●						○
		○	●				●		
			○			○			○
			○			○		○	
		●	○						
								○	●
			●	●				●	●
			○					○	○
●			●						●
			●						○
		○	●				○		
		○	●						○
			●		●				○
			●		●			○	
				●				●	
			●				●		○
●		○	●						●
		●							

● = Primary Category ○ = Secondary Category

Curriculum Tracks

Pick and choose which courses you attend, or run through some of our pre-selected tracks for your topic area.

Risk Management Track

Our vital education for all senior operations and technology professionals covers all aspects of risk mitigation. From Board Responsibilities to employee use of Social Networking, this track helps prepare for the risks and threats every institution faces on a daily basis.

Among our newest sessions: Expert insights on how to manage mobile technologies in the workplace, and an Enterprise Risk Management primer from NIST – the organization that wrote the book on risk management.

FEATURED

MGMT602

Upgrading to an APT-Capable Defense; Where to Start, How to Get Funding and See an Immediate Reduction in Risk

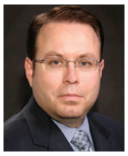
The cost of not having an effective security program has reached the tipping point and has overtaken the cost of having one. Learn how to internally "sell" the adaptation of existing programs to meet this threat.

Presented by: Peter Chronis, CSO, EarthLink; Joe Doetzl, CISO, Head of Cyber Security, ABB Enterprise Software; Kevin Morrison, Dir. of Global Security & Compliance, The Results Companies

Course Title	ID
2014 Faces of Fraud Survey - Special European Edition	463
Account Takeover, Payment Fraud and Spoofed Identities: The Common Thread	531
Automate and Standardize your IAM to Radically Reduce Risk	641
Beyond HIPAA Risk Assessments: Added Measures for Avoiding PHI Breaches	611
Big Data Analytics & Context-Aware Security	419
Bridging the Gap Between Breach Prevention and Incident Response	417
Building a Banking DDoS Mitigation Strategy and the Evolving Security Threat Landscape	639
Business and Risk Based Framework Deployment	497
Customer Awareness: What Works in Fraud Detection, Prevention	423
Data Breach Battle Plans for Financial Services	640
Dispelling the Myths of Malware Attacks	620
Healthcare Information Security Today: 2014 Survey Results and Analysis	394

Course Title	ID
How to Tackle Vendor Risk Hazards: Operationalizing Third-Party Risk Management in Today's Regulated Environment	437
Is Your Data Center Ready for Today's DDoS Threats?	441
Managing Insider Risks: How to Detect and Respond to Malicious and Unintentional Threats	426
Mobile Deposits & Fraud: Managing the Risk	572
Phase 1 - Establishing a Security Baseline - Inside and Out	597
Post-Fraud Investigation: Effective, Efficient, Defensible	376
Preventing Security Breaches with Passwords That Can't Be Stolen	443
Securing Mobile Banking: Authentication & Identity Management	415
Securing the Brave New World of Online Patient Information	433
Security Analytics	495
State of Global Fraud - Dealing with Today's Crimes and Anticipating Tomorrow's	462
The Analyst's Eye: Top Fraud Threats to Watch in 2014	380
The Danger Within: Responding to Unintentional and Intentional Insider Threats	406
The State of APT	489
The Three Ds of Incident Response - Protecting Your Company From Insider Threats	403
The Trojan War: Responding to the Evolution of Cross-Channel Attacks	378
Understanding the Identity Risks You Experience, Not the Risks You Perceive - Identity Theft and Synthetic Identity	450
Upgrading to an APT-Capable Defense; Where to Start, How to Get Funding and See an Immediate Reduction in Risk	602

Featured Presenters



Eduardo Perez

SVP, North America Risk Services,
Visa Inc.

Matt Baker

Former Director of Intelligence,
AFCYBER (Air Force Cyber Command) and 24th Air Force

Peter Chronis

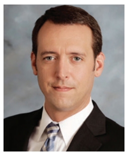
CSO,
EarthLink

Mitch Zahler

SVP, Cybersecurity,
HSBC

John Lyons

CEO,
International Cyber Security Protection Alliance



Rob Zerby

VP, Financial Crimes Manager, Financial Crimes Operations, **Wells Fargo Financial Crimes Risk Management**

Fraud Track

Financial institutions and their customers have been increasingly attacked by incidents of fraud, including: ATM fraud, insider threat, payment card fraud, check fraud, skimming, phishing, and cybercrime. This track focuses on what organizations need to know to prepare, prevent, detect and react to these threats.

These sessions focus not just on external threats, but also on the emerging risk to all organizations – the insider threat.

FEATURED

FR588

The Fraud Ecosystem, Deep Web and Fraud-as-a-Service (FaaS)

As various batches of stolen credit card “dumps” are offered for sale with discount structures and money-back guarantees, it is clear just how sophisticated the Fraud Ecosystem has become. The fraudsters have created well-organized forums offering a broad variety of products that constitute a feature-rich Fraud-as-a-Service network. With card-checker, identity, rent-a-hacker and phishing services, it’s becoming increasingly simple to select the type of stolen data you wish to purchase and the type of fraud you wish to commit.

Presented by Lance James, Head of Cyber Intelligence, Deloitte & Touche

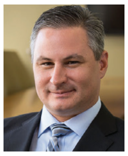
Course Title	ID
2014 Faces of Fraud	534
2014 Identity Theft and Fraud Prevention Survey Results Webinar	567
2014's Top 10 Fraud Stories: What Lessons Can We Learn, and What Can We Expect in the Year Ahead?	537
2015 Faces of Fraud	542
5 Must-Haves for an Enterprise Mobility Management (EMM) Solution	527
Account Takeover, Payment Fraud and Spoofed Identities: The Common Thread	531
Big Data Analytics & Fraud Detection	592
CEO Bob Carr on EMV & Payments Security	560
Consumer Fraud Awareness: What's Working, What's Not & What's Next?	605
Fraud Investigations: How to Work Effectively with Law Enforcement, Government and Litigators	593
Future of Payment Card Security	488
How Cybercriminals Use Phone Scams To Takeover Accounts and Commit Fraud	644
Identity Data Privacy is Dead: Why We Need to Migrate From Static Identity Verification to Dynamic Identity Proofing	541
Identity Theft: How the Name Game Has Changed	583
Insider Fraud Detection: The Appliance of Science	585
Keynote: The State of Fraud Today	570
Malware Activity & Network Anomaly Detection	494
Mobile Banking and Fraud	589
Mobile Deposits & Fraud: Managing the Risk	572
Organized Retail Crime Rings in the Cellular Wireless Industry - ID and First Party Fraud	586

Course Title	ID
Policy Driven Security - Deploy Only Those Security Technologies and Controls That You Need	530
POS Security Essentials: How to Prevent Payment Card Breaches	568
Preparing For and Responding To Large Scale Data Breaches	539
Preparing For The Ripple Effects Of EMV and The Future Of Payment Card Security	594
Technology Spotlight: Identity Theft Protection Using Advanced Analytics	569
The Fraud Ecosystem and the Deep Web	535
The Fraud Ecosystem, Deep Web and Fraud-as-a-Service (FaaS)	588
The Future Of Payment Security: Where Do We Go From Here And Who Is Liable When We Get There?	540
Threat Intelligence and OSINT: What You Can Learn About Your Adversaries and What They Can Learn About You	544
Top 5 Fraud Stories Influencing 2015	645

Featured Presenters

Gregory Marrett
Principle Fraud Investigator,
Capital One

Anant Nambiar
VP & General Manager, Global Fraud & Security Solutions,
FICO



David Pollino
SVP, Enterprise Fraud Prevention Officer,
Bank of the West

James Ratley
President & CEO,
Association of Certified Fraud Examiners

Tim Webb
SVP, Fraud Management,
Citizens Financial Group

What organizations need to know to prepare, prevent, detect and react to these threats.

Data Breach Track

As the world becomes more hyper-connected, and companies and individuals share more and more data, the financial incentives for malicious actors continues to increase. Industries that are common targets are implementing solutions, such as data obfuscation and advanced authentication, which will dramatically reduce their risk profile. This changing security dynamic will force a shift in the behavior of opportunistic cybercriminals, resulting in new targets and fraud schemes leveraging stolen data. This track focuses on how specific technologies will affect the availability of data sought by cybercriminals, how to predict your risk, and developing an effective breach response plan.

FEATURED

DB539

Preparing For and Responding To Large Scale Data Breaches

In this in-depth session we will learn: How current security initiatives and regulations will affect cybercriminals' choice of breach targets; Which industries or specific industry segments should prepare for increased attention from cybercriminals; Which solutions different industries can rely on to insulate themselves from future breach attempts; How businesses can prepare for the inevitable fraud implications of future third-party breaches.

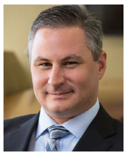
Presented by Al Pascual, Senior Industry Analyst, Fraud & Security, Javelin Strategy & Research

Course Title	ID
2014 Identity Theft and Fraud Prevention Survey Results Webinar	567
2014's Top 10 Fraud Stories: What Lessons Can We Learn, and What Can We Expect in the Year Ahead?	537
2015 Insider Threat Report	609
Actionable Threat Intelligence: From Theory to Practice	613
Automate and Standardize your IAM to Radically Reduce Risk	641
Building a Banking DDoS Mitigation Strategy and the Evolving Security Threat Landscape	639
Case Study: How Threat Intelligence was Used to Defeat an Advanced Attack in Progress	571
CEO Bob Carr on EMV & Payments Security	560
Chasing Down RAT's - Combatting Account Takeover Fraud at the Age of Remote Access Trojan's and Data Breaches	646
Data Breach Battle Plans for Financial Services	640
Digital Identity Verification for Fraud Mitigation	614
Dispelling the Myths of Malware Attacks	620
Healthcare - The New Cybercrime Target: How to Secure Your Data and Ensure HIPAA Compliance	617
How Cybercriminals Use Phone Scams To Takeover Accounts and Commit Fraud	644
Insider Threat: Mitigating the Risk	610
Mobile Deposit Capture: Balancing Fraud Prevention and Customer Convenience	615
Mobile Deposits & Fraud: Managing the Risk	572
Phase 1 - Establishing a Security Baseline - Inside and Out	597

Course Title	ID
Phase 5 - Investigate, Respond, Retaliate? Focus First On The People And The Process, Not The Technology	601
PHI Security: The Role of Encryption and Tokenization	607
POS Security Essentials: How to Prevent Payment Card Breaches	568
Preparing For and Responding To Large Scale Data Breaches	539
ROI of Scalable Application Security	648
Security Alerts: Identifying Noise vs. Signals	576
Stop Mobile Payment Fraud, Not Customers	642
Targeted Attacks - 6 Keys for Fighting Back	616
The Changing Landscape of Data Breaches & Consumer Protection in 2015	612
The Evolution of Advanced Malware	618
The Future Of Payment Security: Where Do We Go From Here And Who Is Liable When We Get There?	540
Top 5 Fraud Stories Influencing 2015	645

Featured Presenters

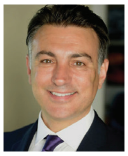
Al Pascual
Senior Industry Analyst, Fraud & Security,
Javelin Strategy & Research



David Pollino
SVP, Enterprise Fraud Prevention Officer,
Bank of the West

Garet Moravec
Former Head of Airborne Platform Systems Cyber Security,
Lockheed Martin Aeronautics

Matthew Rosenquist
Cyber Security Strategist,
Intel Corporation



Michael Panico
Dir. Information Security, Content Protection,
Warner Bros.

John Walker
Dir. CSIRT and Cyber Forensics,
Cytelligence

Technology Track

Changes in the ways that we create, store, and consume information in the digital, connected age have dramatically increased the need to protect our information assets. Traditionally, an "endpoint" referred to a desktop computer; today that definition has expanded to include laptops, tablets, smartphones, and even removable storage devices such as USB flash drives.

In addition to the proliferation of devices to protect, new and more dangerous malware is surfacing at an alarming rate. From targeted spear-phishing to aggressive zero-day exploits, attackers are working hard to circumvent traditional security measures - and in many high profile cases, succeeding. This track focuses on the ever-changing technology landscape and emerging threats targeting those endpoints.

FEATURED

FR454

Real World Applications of Big Data Analytics

Malicious activity triggers measurable events at almost every stage of the attack. There are multiple sensory technologies available, but collecting this data from disparate sources can often just result in the creation of a very large pool of unrelated "facts," an impenetrable noise where no signal can be found. But begin to add context to that data and you now have information. Triangulate multiple pieces of information together and you can create intelligence. The best practices and examples of how this can be achieved will be demonstrated in this session.

Presented by Jason Paguandas, Dir., Canadian Banking Fraud Strategy & Analytics, RBC Bank; Dan McKenzie, Head of Enterprise Fraud Strategy, RBC Bank

Course Title	ID
2015 Insider Threat Report	609
Actionable Threat Intelligence: From Theory to Practice	613
Advances in Application Security: Run-time Application Self Protection	523
Automate and Standardize your IAM to Radically Reduce Risk	641
Big Data Analytics & Fraud Detection	592
'Black Friday' Cybersecurity Challenges for the Banking & Merchant Community	526
Building a Banking DDoS Mitigation Strategy and the Evolving Security Threat Landscape	639
Case Study: How Threat Intelligence was Used to Defeat an Advanced Attack in Progress	571
Changing Perceptions and Attitudes - A New Way of Thinking About Defense	603
Chasing Down RAT's - Combatting Account Takeover Fraud at the Age of Remote Access Trojan's and Data Breaches	646
Cloud Infrastructure: Same Security Needs, Dynamic New Environment	566
Cyber Threat Intelligence	491
Data Breach Battle Plans for Financial Services	640
Digital Identity Verification for Fraud Mitigation	614
Dispelling the Myths of Malware Attacks	620

Course Title	ID
How Cybercriminals Use Phone Scams To Takeover Accounts and Commit Fraud	644
Investigate, Respond Retaliate?	496
Looking for Anomalies: Try Machine Data	532
Malware Activity & Network Anomaly Detection	494
Mobile Deposit Capture: Balancing Fraud Prevention and Customer Convenience	615
Phase 3 - Zero-Day Threats, Known Vulnerabilities and Anomaly Detection	599
Real World Applications of Big Data Analytics	454
ROI of Scalable Application Security	648
Secure E-Banking: Consumer-Friendly Strong Authentication	580
Security Alerts: Identifying Noise vs. Signals	576
Stop Mobile Payment Fraud, Not Customers	642
Targeted Attacks - 6 Keys for Fighting Back	616
The Changing Landscape of Data Breaches & Consumer Protection in 2015	612
The Evolution of Advanced Malware	618
Visa on Future of Payment Card Security	413

Featured Presenters

Andrew Case

Core Developer,

Volatility Foundation

Lance James

Head of Cyber Intelligence,

Deloitte & Touche

Anton Chuvakin

Research VP,

Gartner GTP Security and Risk Management Strategies

Eric Thompson

IT Threat Strategist,

RSA

Ori Bach

Senior Security Strategist,

Trusteer - IBM Security Systems

Julie Conroy

Research Director,

Aite Group

Payments Track

Payments make up the majority of transactions at any institution. Millions of debit and credit card, checking, online, and mobile transactions happen every minute of every day, making payments one of the biggest opportunities for attack. Our Payments Security track provides education on regulations, threats, and the largest cases of breaches to prepare your institution.

Course Title	ID
2014's Top 10 Fraud Stories: What Lessons Can We Learn, and What Can We Expect in the Year Ahead?	537
CEO Bob Carr on EMV & Payments Security	560
Future of Payment Card Security	488
Mobile Deposits & Fraud: Managing the Risk	572
Mobile Fraud - Leveraging Threat Intelligence in Mobile Banking and the Risks of Virtual Currencies	487
Payment Card Fraud & the Future of Secure Payment	425
Payment Card Fraud and the Merchant Challenge	379
Payment Card Fraud Response: Taking on the Processor	424
Payment Card Fraud, EMV Adoption & the Merchant Challenge	412
Payment Card Fraud: The Present and the Future	482
POS Security Essentials: How to Prevent Payment Card Breaches	568
Preparing For The Ripple Effects Of EMV and The Future Of Payment Card Security	594
The Future Of Payment Security: Where Do We Go From Here And Who Is Liable When We Get There?	540
Top 5 Fraud Stories Influencing 2015	645
Visa on Future of Payment Card Security	413

FEATURED

PAY413

Visa on Future of Payment Card Security

High-profile retail data breaches have captured the attention of executives and policymakers alike. Beyond the financial consequences, there is one positive outcome: a renewed focus by financial institutions and retailers to advance payment system security. In this exclusive session, Visa's Ellen Richey discusses: The complexity of the payments ecosystem, how to improve payments security by de-valuing data; and the merits of merging security solutions, including EMV, tokenization and encryption.

Presented by Ellen Richey, EVP, Chief Legal Officer & Chief Enterprise Risk Officer, Visa Inc.

Featured Presenters

Eduardo Perez

SVP, North America Risk Services,
Visa Inc.

Dennis Simmons

CEO,
SWACHA

Mark Sullivan

Dir. Fraud Programs,
Interac Association

John Walp

Corporate Information Security Officer,
M&T Bank

Kirstin Wells

VP, Risk Officer,
Federal Reserve Bank of Chicago

Governance Track

Senior leaders at institutions require specialized education regarding matters of business continuity, risk management, incident response and preparing the teams and employees they manage. This track highlights the needs of management ultimately responsible for the direction of an institution's course of action in these areas.

Learn the basics of establishing a culture of security within your organization, as well as the latest methods for educating employees, customers and your own senior leaders.

Course Title	ID
2014 Faces of Fraud Survey - Special European Edition	463
Alerts that Matter: Prioritizing and Triaging Alert Data	468
Business and Risk Based Framework Deployment	497
Consumer Fraud Awareness: What's Working, What's Not & What's Next?	605
Customer Awareness: What Works in Fraud Detection, Prevention	423
Cyber Investigations: How to Work with Law Enforcement	565
Fraud Investigation Life-Cycle: From Forensics to Working w/ Law Enforcement	410
Fraud Investigations: How to Work Effectively with Law Enforcement, Government and Litigators	593
How DDoS Taught Competitors to Make Information Sharing Work	374
Investigative Analytics: Velocity to Respond	554
Payment Card Fraud Response: Taking on the Processor	424
Payment Card Fraud, EMV Adoption & the Merchant Challenge	412
Phase 5 - Investigate, Respond, Retaliate? Focus First On The People And The Process, Not The Technology	601
Policy Driven Security - Deploy Only Those Security Technologies and Controls That You Need	530
Post-Fraud Investigation: Effective, Efficient, Defensible	376
Securing the Internet of Things	399
State of Global Fraud - Dealing with Today's Crimes and Anticipating Tomorrow's	462
Stress Free Audits, Reduced Risk, Higher Confidence - How IAM Contributes to the Bottom Line	368
The Three Ds of Incident Response - Protecting Your Company From Insider Threats	403
Upgrading to an APT-Capable Defense; Where to Start, How to Get Funding and See an Immediate Reduction in Risk	602
Threat Detection, Compliance & Incident Response	181

Featured Presenters

Shona Harper
Chief Privacy Officer, Europe & Asia-Pacific,
TD Bank

Avivah Litan
VP & Distinguished Analyst,
Gartner Research

Kevin Morrison
Dir. of Global Security & Compliance,
The Results Companies

Richard Rushing
CISO,
Motorola Mobility

Matthew Speare
EVP, Governance & Integration,
Regions Bank

Premium Membership

Become a Premium Member to stay up-to-date on the latest information security and risk management topics.

Monthly	4 Months	Annual
	SAVE 40%	BEST VALUE
$349/mo	$199/mo	$179/mo
3 Webinars Per Month	Unlimited Webinars	Unlimited Webinars
OnDemand Access	OnDemand Access	OnDemand Access
CPE Credit Tracking	CPE Credit Tracking	CPE Credit Tracking

Groups: Save up to an additional 30% with a group membership.

Membership Features

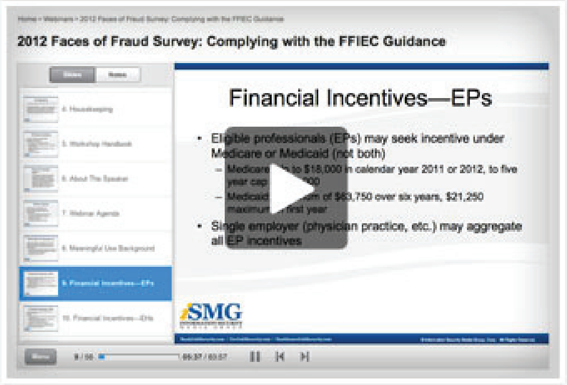
Unlimited Access

Gain unrestricted access to an expanding curriculum of over 350 courses. No education solution is as comprehensive. Our industry expert practitioners have developed over 300 hours of exclusive courses and, on average, create 15 new courses each quarter.

This continually growing resource ensures you have the latest information available as you need it.

OnDemand Viewing

Convenience is essential when it comes to your professional education. OnDemand capabilities allow you to access the education around your availability, not ours. Whether it's 15 minutes before a meeting, 30 minutes on your lunch break, or even during your daily commute, our education is always at your fingertips.

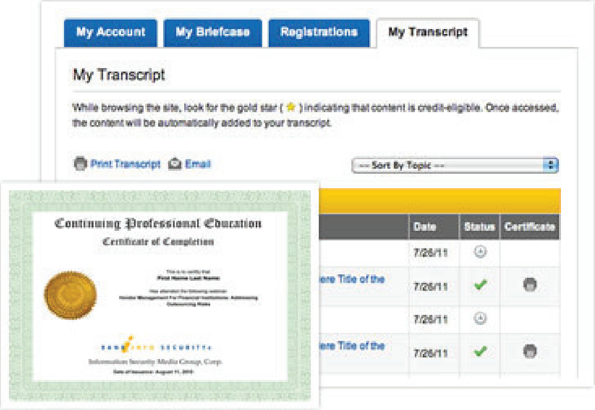


Home › Webinars › 2012 Faces of Fraud Survey: Complying with the FFIEC Guidance

2012 Faces of Fraud Survey: Complying with the FFIEC Guidance

Financial Incentives—EPs

- Eligible professionals (EPs) may seek incentive under Medicare or Medicaid (not both)
  - Medicare up to $18,000 in calendar year 2011 or 2012, to five year cap of $44,000
  - Medicaid maximum of $63,750 over six years, $21,250 maximum in first year
- Single employer (physician practice, etc.) may aggregate all EP incentives



My Account | My Briefcase | Registrations | My Transcript

My Transcript

While browsing the site, look for the gold star (⭐) indicating that content is credit-eligible. Once accessed, the content will be automatically added to your transcript.

	Date	Status	Certificate
	7/26/11	○	
ere Title of the	7/26/11	✓	●
	7/26/11	○	
ere Title of the	7/26/11	✓	●

Continuing Professional Education

Certificate of Completion

This is to certify that

First Name Last Name

Has attended the following webinar:

Vendor Management For Financial Institutions: Addressing Outsourcing Risks

BANK INFO SECURITY

Information Security Media Group, Corp.

Date of Issuance: August 11, 2011

Continuing Professional Education

Responding to regulators, senior management and certifying associations can become a hassle. Our Transcript Tracking feature lists date, title and hours of all credit-eligible webinars, articles, interviews, handbooks and other content accessed.

This transcript can be broken down by topic and attendance certificates can be e-mailed or printed directly from our system, making it easy to keep track and report on your continued education.

Presentation Materials

Each Premium Webinar comes with a course handbook developed by the expert presenter. This not only includes all slide materials, but also additional research and reading that couldn't be conveyed during the 90-minute session.

We strive to keep our webinars engaging and packed with actionable advice that can be put to use immediately. These handbooks help us provide further detailed information while keeping the presentation fresh.

USERNAME
user 1
PASSWORD
*****
FFIEC Authentication Guidance: How to Prepare for Your Next Exam
BANK INFO SECURITY
ISMG

Questions & Answers

Detailed answers to all your questions about courses, presenters, CPE credits and membership options.

What is a membership?

A Premium Membership enables OnDemand access and transcript tracking for all 350+ educational webinars in our expansive curriculum. One-month members gain access to three webinars, while all other levels of membership grant unlimited access. New features also include mobile webinar access and a membership community discussion forum.

Is membership individual-based or for the entire organization?

Many institutions provide this access enterprise-wide to meet their information security, risk management, compliance and fraud teams' needs. However, due to our transcript tracking feature, membership must be associated to each specific user.

What else is included besides the ability to attend unlimited webinars?

In addition to webinar access, members also have an exclusive transcript-tracking feature that monitors all educational webinars, articles, interviews and handbooks accessed. Transcripts and proof-of-attendance certificates can be printed or e-mailed directly from this system. Members also get exclusive features, such as mobile device webinar access and a membership community discussion forum, which can be used to directly communicate with peers and expert presenters.

Do I earn Continuing Professional Education (CPE) credits for the webinars I attend?

Yes. Members utilize their transcript to submit proof-of-attendance certificates to certifying associations and senior management. These certificates indicate session title, date, member name and hours earned. This easy-to-use transcript interface also allows for an organization, by category, to help drill down for each specific certification's requirements.

Can I sign up my entire group as part of the membership?

Absolutely. We have a custom offering for teams of all sizes. An increasing number of organizations are relying on us to supplement their information security, risk management, compliance and fraud educational needs. In fact, the larger the team, the more cost-effective membership becomes. Group rates are available for teams as small as two.

Can I as a manager see a report on who has attended which webinars?

Yes. Each member has the capability to e-mail their transcript to managers at any time during their membership. This easy-to-use transcript interface also allows you to organize by category to help drill down for each specific business group's requirements.

What is the standard length of a webinar?

Webinars range from 1 hour to 3 hours+. The average duration is 90 minutes.

Can I add other members of my team to an existing Membership?

Yes. Memberships are always associated directly with a contact in our system. If at any point in time you feel that additional team members would benefit from our education, we can get them activated. You don't even need to wait until your expiration date.

I don't work for a banking institution. Will I benefit from the Membership?

Risk management and information security professionals in any industry will benefit from the ISMG Premium Membership. The majority of presentations are purposefully designed so that any information security and risk management professionals, regardless of industry, will be able to enhance their understanding of each topic presented.

I already attend industry conferences. Why do I need the Membership?

While industry conferences do afford some level of networking opportunities, the fact is that much of what goes on at these conferences does not include true education and learning. With an ISMG Premium Membership, you can be assured that each and every training webinar is 100% focused on true education and career advancement. In addition, there are no travel expenses, time out of the office or non education-based social interaction.

I am not a technologist. Will I benefit from the Membership?

A subset of our training webinars do focus on more technical topics, however the majority are produced for non-tech professionals. Besides technology-focused training webinars, we offer classes dealing with governance and management, compliance, fraud, vendor management, business continuity/disaster recovery and more.

I am not involved with the day-to-day operations of the organization I am with. Will I benefit from the Membership?

Yes, risk management and information security is something every person within an organization needs to be cognizant of. With dozens of classes on many diversified topics, there are presentations that will be applicable to anyone within an organization.

I am not based in the United States. Will I benefit from these webinars?

Yes. While some of our webinars may be specific to U.S.-based rules and regulations, many of them deal with information security and risk management standards and guidelines that are applicable to all professionals around the world. Even the U.S.-based topics cover a wide range of content, most of which is applicable to guidelines and standards produced outside the U.S.

Who are the typical presenters for the webinars under the Membership program?

Typical presenters for our webinars are real practitioners. They are risk management and information security professionals, regulators and industry experts who speak directly from experience. Each presenter must go through a rigorous screening process to ensure they are able to offer unique, actionable advice for whichever topic they are presenting on.

Is there a calendar of webinars available for review?

Yes. View the most up-to-date webinar calendar at http://www.bankinfosecurity.com/webinars-calendar.

What types of topics are covered in these webinars?

The training curriculum covers a wide range of risk management and information security topics. The courses are grouped into the following topic areas: Governance & Management, Fraud, Compliance, BSA/Anti-Money Laundering, Vendor Management, Business Continuity/Disaster Recovery, Privacy, Technology and IT Audits.

Do I have to travel to attend these webinars?

No. Every webinar is presented online. There is no time away from the office and no travel expenses. Each registrant receives a unique access link to view the webinar on their computer.

How do I pay for Membership?

You can purchase an ISMG Premium Membership directly through one of our websites or via a dedicated account representative. We accept credit card payments, checks and electronic funds transfers.

Are these webinars available OnDemand?

Yes. In addition to being regularly scheduled on our webinar calendar, Premium Members have access to any webinar that has aired at least once at any time in our OnDemand library. Premium Membership is the only way to access our premium courses OnDemand.

Do I get to ask specific questions either during or after the webinars (preferably directly to the instructor)?

Yes. Every webinar includes a Q&A session and attendees are encouraged to ask questions. Any questions that are not addressed during the presentation will be answered afterwards. Premium Members may also submit questions after viewing a webinar via our online dedicated webinar response form.

Are there any additional costs associated with attending these webinars?

No. The only additional cost that may be applicable is phone access. However, every webinar attendee has the option to connect to the audio portion of the webinar from their computer via streaming audio. So long as your computer has speakers, you do not need to dial in using a standard phone connection.

Become a Premium Member.

Exclusive access to 350+ webinars. Turn our industry experts into your OnDemand professional resource.

Get started today:

www.bankinfosecurity.com/memberships

Contact our membership team:

Call: (800) 944-0401
Email: memberships@bankinfosecurity.com

iSMG
INFORMATION SECURITY
MEDIA GROUP

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com