



2011 Course Catalog

Educational Webinars for Financial Institutions

Welcome to the University of You



The bad news: Fraud incidents are on the rise. Our “Faces of Fraud” survey indicates that banking institutions are under constant attack by payment card, check, phishing/vishing, ACH/wire and even internal data leakage.

The good news: Institutions also are investing more time and resources in employee training – not just for information security professionals, either, but for everyone in the organization, ranging from customer-facing personnel to senior business management.

Why the renewed emphasis on training? Mostly, to keep up with the latest threats, as well as new trends and technologies. In some cases, to comply with industry or government regulations. In all cases, continuing education is vital for today’s professionals to stay current – and particularly when training counts toward continuing education credits for industry certifications.

At Information Security Media Group, publisher of BankInfoSecurity.com, GovInfoSecurity.com and HealthcareInfoSecurity.com, we’ve assembled a broad suite of webinar training programs that are relevant to your career needs. These sessions cover the gamut of industry/security topics such as:

- **Regulatory Compliance** – including sessions that walk you through risks assessments, anti-money laundering and vendor management, as well as how to prepare for an ID Theft Red Flags Rule exam.
- **Fraud** – with emphasis on hot topics such as skimming, phishing and how to resist social engineering.
- **Today’s Pressing Needs** – how to mitigate risks presented by the insider threat, social media and emerging technologies such as cloud computing.

For our virtual faculty, we draw upon a broad range of presenters. Industry thought-leaders, top consultants, current industry/security leaders, even federal regulators.

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 course offerings that could most benefit you.

Tom Field

Editorial Director, Information Security Media Group
tfield@ismgcorp.com



Topics You Care About

When it comes to information security and risk management for financial services organizations continuing education is a must in this ever changing environment. Security is an evolving practice and failure to protect your customers’ information will have serious consequences. As a result, everyone — from IT staffers and risk officers to business managers and executives — needs to keep pace.

Our extensive library of education and training webinars covers all facets of risk management and information security for professionals at institutions of all sizes. Whether you deal with strictly compliance initiatives or delve into the intricacies of technology implementation, we have training webinars for you.



Here are some of the topics our training covers:

Authentication
Cloud Computing
Compliance
DR/Business Continuity
Data Loss Prevention
Emerging Technologies
Encryption

Fraud Detection & Prevention
Governance, Risk, & Compliance
Hiring & Background Checks
Identity & Access Management
Identity Theft & Phishing
Incident Response
Insider Fraud

Mobile Banking
Physical Security
Security Policies & Standards
Social Engineering
Training and Education
Vendor Management
Web Application Security

Presented by Industry Experts

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

Training and education are only as effective as the presenter and his/her subject matter expertise. That is why we strive to utilize only the best and brightest in the financial industry to present our training webinars.

Many of our presenters have gone through the same challenges you do, and 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, most importantly, how-to. After attending our webinars you will walk away with definitive steps and actionable advice that you can utilize at your institution. Our presenters go through a considerable vetting process and are monitored throughout the entire webinar production cycle to ensure only the highest quality educational content is conveyed.



Matthew Speare

SVP of Information Technology, M&T Bank

Matthew oversees security for M&T Bank Corporation, the nation's 17th largest bank holding company, based in Buffalo, New York. He is responsible for developing and sustaining an information risk program that effectively protects the personal information of millions of M & T Bank customers.



William Henley

Former Director of IT Risk Management, OTS

William has spent his entire professional career as a financial institution regulator. Henley is the Director of IT Risk Management for the Office of Thrift Supervision. In his role as the Director, Henley serves as the principal advisor regarding the development, implementation and maintenance of policies, procedures and guidelines.



Steven Jones

Director of Information Security, Synovus Financial

As a member of senior management, Steven is responsible for the company's organizational policy, risk management, security awareness, identity management, disaster recovery, and other areas of risk management. He is active in BITS, Information Risk Executive Council, and serves on several advisory boards including SecureWorks and Blue Coat.



Tom Wills

Senior Analyst Risk, Security and Fraud, Javelin Strategy and Research

Tom leads Javelin Strategy & Research's strategic risk management, security, fraud, and compliance advisory services. He spent the last two and a half decades helping large, global enterprises and financial institutions strategically navigate the challenges of security. His breadth of expertise enables Javelin to deepen its support of clients.



Paul Smocer

VP Security, BITS

Paul leads the security program management at BITS, a division of the Financial Services Roundtable. Smocer brings over 30 years' experience in security and control functions in his background, most recently focusing on technology risk management at The Bank of New York Mellon and leading information security at the former Mellon Financial.



Linda Coven

Head of Online Banking Channel Solutions, Silicon Valley Bank

Linda is a 20 year veteran of the banking industry who developed and manages the online banking platform for Silicon Valley Bank. With over 7 years experience at SVB, she serves as strategic advisor to the company's executives and steering committee related to products and services that will help further the commercial bank's strategic objectives.



David Matthews

Deputy Chief Information Security Officer for the City of Seattle

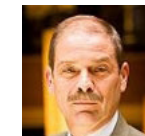
David Matthews is currently the Deputy Chief Information Security Officer for the City of Seattle. He has worked in the Information Technology field since 1992. He began working for the City of Seattle as the Technology Manager for the Legislative Department (City Council) in 1998.



Neil Katkov

Celent

Neil is the manager of Celent's Asia Research group. His areas of expertise include the Asian financial services industry, financial services distribution channels, and compliance issues including anti-money laundering and business continuity planning. Dr. Katkov produces Celent's popular reports on IT spending trends in the Asian banking, securities, and insurance industries.



David Dixon

Managing Director of Financial Crime Norkom

David provides leadership for Norkom's development and delivery of industry leading financial crime solutions. He brings more than 20 years' experience providing financial crime and risk management expertise to global financial services firms.



Randy Sabett

Information Security Attorney, SN&R LLP

Randy, CISSP, is a partner in the Washington, D.C. office of Sonnenschein Nath & Rosenthal LLP, where he is a member of the Internet, Communications & Data Protection Practice. He counsels clients on information security, privacy, IT licensing and patents.



E.J. Hilbert

Former FBI Special Agent

E.J. is a former Federal Bureau of Investigation Special Agent specializing in international hacking, carding and fraud teams. He has trained law enforcement representatives throughout the U.S., Canada, the United Kingdom, Belarus, Russia and the Ukraine. E.J. served as the agent in charge of the investigations into the intrusions of over 300 financial institutions.



Kevin Sullivan

Investigator, New York State Police

Kevin Sullivan is an investigator with the NY State Police and was the state investigations coordinator assigned to the NY HIFCA El Dorado Task Force in Manhattan. He has 20 years of police experience, specializing in anti-money laundering and conducting numerous investigations. Sullivan has a Masters in Economic Crime Management and is a certified anti-money laundering specialist.



Charles Robertson

Sr. Product Manager, Verafin

Dr. Robertson contributes directly to the development of Verafin's advanced anti-fraud solutions and behavior-based analytics, and speaks frequently about money laundering and fraud across North America. Dr. Robertson has an extensive background in R&D related to image processing, pattern recognition and artificial intelligence.



Mike Urban

Sr. Dir. & Fraud Chief, FICO

Mike Urban has 15 years experience in financial fraud management. At FICO, he analyzes fraud issues and trends to provide continuous improvements in fraud detection technology and fraud management. Urban regularly works with law enforcement to help prosecute criminals and has been responsible for uncovering several crime rings in the US.



James Christiansen

CEO, Evantix

Prior to joining Evantix, James was Chief Information Security Officer for Experian Solutions. James joined Experian after serving as Chief Information Security Officer for General Motors. Prior to joining GM, James leveraged his years of security experience to provide global leadership to Visa International. James has been featured in the New York Times.



Keir Breitenfeld

Sr. Dir. Fraud and Identity Solutions, Experian Decision Analytics

Keir Breitenfeld's responsibilities at Experian include stewardship of their comprehensive suite of consumer and commercial authentication and fraud management products and services. Keir brings with him a diverse set of experiences including fraud operations management, risk management consulting, and project management.



Ori Eisen

Founder, Chairman and Chief Innovation Officer, 41st Parameter

Ori Eisen has spent the last ten years in the information technology industry, his background includes an in-depth application of innovative solutions for preventing business to consumer e-commerce fraud. Prior to launching 41st Parameter, Mr. Eisen served as the Worldwide Fraud Director for American Express.



Reed Taussig

President & CEO, ThreatMetrix

Reed has over 30 years experience in the computer hardware and software fields. Prior to ThreatMetrix, Mr. Taussig was president and CEO of Vormetric, Inc., a leader in data privacy and protection. Under his leadership, Vormetric established itself as a leading provider of encryption solutions for the Payment Card Industry Data Security Standards industry.



Krista Tedder

VP Debit Solutions - Fraud and Risk Management, MasterCard

Krista is currently responsible for fraud and collections solutions for financial institutions. Krista provides consultation services to financial institutions with a focus on reducing operational expenses and strengthening brand reputation through consistent customer experience and stronger fraud management capabilities.



Dr. Markus Jakobsson

Associate Prof., Indiana University

Markus is Associate Professor at Indiana University's School of Informatics. He is also Associate Director of the Center of Applied Cybersecurity Research, and founder of RavenWhite, Inc. He is an author, as well as the inventor or co-inventor of more than fifty patents.



Bill Sewall

Information Security, Compliance and Risk Management Specialist

Bill is an Information security, compliance and risk management specialist with 30 years experience as a corporate attorney and general counsel, CIO, information security officer, and operational risk manager. Most recently, Sewall spent 10 years as a senior executive information security officer in Citigroup.



Steve Neville

Director of Identity Products, Entrust

Steve joined Entrust in 1999, and has played a consistent leadership role in Entrust's product evolution and innovation. Working closely with customers and key departments such as R&D, sales and marketing, Steve is passionate about ensuring that Entrust fields market-driven, innovative products.



George Tubin

Senior Research Director, TowerGroup, Inc.

George Tubin's areas of expertise include consumer online banking, online fraud and identity theft prevention, information security strategy, and customer authentication, mobile banking and contact center strategies and technologies. Before joining TowerGroup, George was a senior consultant with ADS Financial Services Solutions.



Andy Schmidt

Research Director - Global Payments, TowerGroup, Inc.

Andy Schmidt focuses on trends and developments in the payments, including payments hubs, mobile payments, service-oriented architecture, standards, and anti-money laundering. Andy has 20 years of experience in the financial services industry as both a banker and a consultant.



Harold Moss

CTO - Cloud Security Strategy, IBM

Harold Moss, as a member of the corporates strategy team, participates in defining technical directions for security technologies and is an active contributor to the IBM Security Technology Institute. Harold is currently working on cloud security for various cloud patterns, as well as correlating workload to specific cloud patterns.



Jeff Lake

VP - Federal Operations, Proofpoint

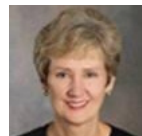
Jeff Lake directs Proofpoint's strategic growth in the U.S. federal government market. With over 20 years of technology and security experience, Lake has held several leadership positions in technical sales, consulting and operations. Previously, Lake was a commissioned U.S. Army Military Intelligence officer, holds a Top Secret security clearance.



Terry Austin

President & CEO Guardian Analytics, Inc.

Terry Austin is the CEO at Guardian Analytics and a regular speaker at conferences and seminars on the topic of new strategies for fraud prevention at banks and credit unions.



Shirley Inscoc

Director - Financial Services Solutions, Memento

A 29-year banking veteran, Shirley Inscoc is a recognized expert in helping financial institutions apply innovative technology and strategies to address dynamic and costly fraud challenges. Shirley is a former SVP of Enterprise Payments Strategy at Wachovia, Chair of BITS Fraud Reduction Steering Committee, and Co-Chair of Early Warning Services' Advisory Committee.



Patrick Howard

Chief Information Security Officer, Nuclear Regulatory Commission

Patrick D. Howard serves as the Chief Information Security Officer of the Nuclear Regulatory Commission. He provides vision, leadership and oversight in developing, promulgating and implementing an agency IT security strategy.



Michael Smith

Security Evangelist, Akamai

Michael Smith is the customer-facing ambassador from the Information Security Team at Akamai, helping customers to understand both the internal security program and the unique security features and capabilities of the Akamai product portfolio and cloud-based solutions. He is also an adjunct professor for Carnegie Mellon University.



Evelyn Royer

Vice President, Purdue Employee Federal Credit Union

Evelyn joined Purdue Employees Federal Credit Union in 1994 as the internal auditor and later was promoted to accounting manager. She was chosen to develop the risk management department in 2002, and in 2005 she was named vice president, overseeing collections, compliance, internal audit and servicing for loans, deposits and plastic products.



Tom Walsh

CISSP and Certified Business Continuity Professional

A nationally recognized speaker on a range of information security related topics, including business continuity and disaster recovery. Prior to launching a consulting firm offering information technology risk management services for its clients, Tom was responsible for leading information security efforts for Saint Luke's Health System in Missouri.



Rebecca Herold

Analyst

Rebecca is an information, security, privacy and compliance analyst, author and instructor. Herold is also an adjunct professor for the Norwich University Master of Science in Information Assurance program. She has provided information security, privacy and regulatory services to organizations from a wide range of industries throughout the world.

Course Category Matrix

Webinar Title	BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
5 Critical Data Security Predictions for 2011					○		○	●	
Anti-Money Laundering/Fraud Convergence: Why Should I Care?	●		○	○		○			
Anti-Money Laundering: The Practitioner’s Guide to the Laws	●		○			○			
Anti-Money Laundering: The Investigator’s Guide to the Laws	●		○			○			
Application Security Testing and OCC Bulletin 2009-16 Compliance			○				○	●	○
Are You Effectively Protecting Your Customer’s Private Data?	○					○	●		
Assessing Encryption Standards for Financial Institutions						○		●	○
ATM Fraud: Strategies to Beat the Skimming Scams				●				○	
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks					●		○		
Beyond Compliance: Meeting the New Threat Landscape Head-On			●					○	
Beyond Heartland: How to Prevent Breaches of Security and Trust				●			○	○	
Beyond Phishing - The Growing Crimeware Threat				●			○		
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System					●				
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	●		○			○			
Business Banking Under Attack: How to Fight Back Against Cybercriminals				●				○	
Business Continuity Planning Best Practices		●							
Business Continuity Risk Assessment & Resource Allocation		●			○	○			
Business Impact Analysis — How to Get it Right		●			○				
Check Fraud Management 2.0: A New Approach to a Persistent Challenge				●				○	
Cloud Computing: Regulatory Security & Privacy Challenges			●				○	●	●
Creating a Culture of Security - Top 10 Elements of an Information Security Program			○		●				
Data Protection and Incident Response					●		○		○
Debit Fraud: Trends and Typologies				●		○		●	
Defending Against The Insider Threat				●	○		○		
Developing an Effective Information Security Awareness Training Program - Getting the Word Out	○				●				
Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today’s Banking Climate				●			○		
Email Security Requirements for Healthcare Providers: HIPAA & Beyond			○				○	●	

● Primary Category ○ Secondary Category

Webinar Title	BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
Evaluating Security Risks Associated with Banking Vendors							○	○	●
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	●		○						○
Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge			○	●				●	
Fighting Fraud Schemes: Education, Response and Defense				●	○			○	
Fighting Online Banking Cybercrime with a Holistic Security Strategy				●	○			○	
Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights			○	●				○	
Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities				●			○	○	
Gaining Control of Compliance Mandates, Security Threats, & Data Leaks			●			○			
GLBA Privacy Requirements: How to Build an Effective Program That Meets GLBA Compliance and Ensures Customer Privacy			●				○		
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials			●				○		
How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution				●			○	○	
How to Develop & Maintain Information Security Policies & Procedures			○		●	○			
How to Launch a Secure & Successful Mobile Banking Platform								●	
How to Prepare for Your First Identity Theft Red Flags Rule Exam			●			○	○		
How to Prevent Data Leakage from Compromising Your Company's Security					●				
How to Use Your Mobile Phone for Free Two-Factor Authentication								●	
How Well Do You Know Your Vendors?					○		○		●
Identity Theft: How to Respond to the New National Crisis				●			○		
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication			●				○		○
Incident Response: How to React to Payment Card Fraud				●			○		○
Information Security for Management – What Your Senior Leaders Need to Know			○		●				
Information Security Risk Assessments: Understanding the Process			○		●	○			
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands			●					○	
Insider Fraud - Profiling & Prevention				●			○		
Insider Threat: Defend Your Enterprise					●				
Insider Threats - Safeguarding Financial Enterprise Information Assets				●					
Integrating Risk Management with Business Strategy					●				
Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution			●			○	○		
Is Your Device Identification Ready for New FFIEC Guidance?			●				○	●	

Webinar Title	BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
Key Considerations for Business Resiliency					●				
Legal Considerations About Cloud Computing			○		○			●	○
Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b			●			○			
Maintaining Secure Government Information Systems					●			○	
Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses				○				●	
Managing Shared Passwords for Super-User Accounts					○			●	
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud				●			○	○	
Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard			●				○		○
Meeting Federal Compliance to Secure Windows Desktops			●			○		●	
Money Laundering Update: The Latest Threats to Your Institution	●			○		○			
Next-Generation Threats: Understanding, Investigating and Defending Global Attacks Against the Financial Services Industry				○				●	
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?		○			●	○	○		
Pandemic Planning & Response Techniques		●	○						
PCI Compliance: Tips, Tricks & Emerging Technologies			●					○	
PCI: What Healthcare Organizations Need to Know			●					○	
Power Systems: How to Prevent Unauthorized Transactions			○			○		●	
Preparing for an Information Technology Regulatory Exam			●					○	
Preparing for Your Next Audit: The Five Habits of Successful Security Programs			○			●			
Preparing Your Institution for an IT General Controls Audit						●			
Preventing Phone Fraud with Voice Biometric Authentication				●				○	
Preventing TJX Type Data Breaches								●	○
Preventing Unauthorized Access To Your Institution's Data						○		●	
Proactive IT Risk Assessment Strategies			○		●				
Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention			●			○		●	
Protecting the Exchange of Sensitive Customer Data with Your Vendors							○	○	●
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors			●						○
Responding to a Privacy Breach: Protect Yourself and Your Vendors	○						●		○
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know			●		○				
Securing Your Email Infrastructure			○				○	●	

Webinar Title	BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
Security Risks of Unified Communications: Social Media & Web 2.0								●	
Social Engineering: How to Train Your Employees to Spot and Stop the Scams			○		●		○		
Social Networking Compliance for FINRA Regulated Organizations			●			○	○	●	
Social Networking: Is Your Institution Ready for the Risks?						○	●		
Steps to Managing Security Risk from Your Software Vendors			○						●
Taking Fraud Out of Online Banking				●			○	○	
Testing Security Controls at a Banking Institution: Learn from the Experts			○			○		●	
The Dirty Little Secret About Network Security			○		○			●	
The Faces of Fraud: How to Counter 2011's Biggest Threats				●	○				
The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink				●				●	
The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights								●	
The Identity Enabled Network: The Future of Secure Cyberspace					○			●	
The Identity Management Challenge for Financial Institutions				○			○	●	
The Mobile Environment: Challenges and Opportunities for Secure Banking						○		●	
The Reality of Cyberattacks: Emerging Solutions for Today's Threats								●	
Time: The Hidden Risks - How to Create Compliant Time Practices			○					●	
Top 5 Reports IT Auditors Request			○		○	●			
Top 20 Critical Controls to Ensure Painless FISMA Compliance			○		●				
Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?			●				○	○	○
User Authentication: Best Practices for Managing Risk & Compliance			○		○			●	
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks			○			○			●
Vendor Management Part II: Assessing Vendors - the Do's and Don'ts of Choosing a Third-Party Service Provider			○			○	○		●
Vendor Management Part III: Inside the BITS Shared Assessments Program						○			●
Voice Over IP -Helping Financial Institutions Learn and Mitigate Security Risks								●	
You & Your Vendors: How to Best Secure Data Exchange			○					○	●
ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band				●				○	

Start Training Today

Take advantage of our easy attendance options



A la Carte

The easiest way to attend a webinar. If you're looking for an introduction to what our training offers, attending a webinar a la carte is the best entry-point.

- One webinar at a time
- Single attendee or Corporate Pass (Up to 5 attendees)

[Get Started](#)

Vouchers

Purchase seats to a determined number of webinars up-front, and use them for whichever sessions you please, for yourself or for anyone at your institution.

- Multiple webinars, available in packs of 4, 10, and 20
- Flexible schedule

[Get Started](#)

Annual Membership

Register once, attend as many webinars as you'd like for an entire year. If you plan to attend multiple webinars, this is the option for you.

- [Unlimited webinars for 1 year](#)
- [Corporate and Enterprise memberships available](#)
- [Transcript tracking interface](#)
- [Certificates which may be used towards CPE credits](#)
- [OnDemand access to our entire catalog, 24/7](#)

[Get Started](#)

Membership: A Sound Business Case

For one flat annual fee – either as an individual or as a corporate member – you and your team can attend any or all of our unique webinars over the course of your subscription. These are sessions that normally cost hundreds of dollars each, but all are open to you as part of your membership.



Individual Membership

One person gains access to our entire library of webinars for one year. Included is a transcript-tracking page which organizes all of the classes the member attends along with the ability to print proof of attendance certificates on-demand, which may be used towards securing CPE credits.

[Learn More](#)



Corporate Membership

Ideal for your institution's information risk management and security team - up to 5 people from the institution can attend as many webinars as they'd like for an entire year. Each member can pick-and-choose their own webinars to attend, and have their own transcript-tracking page where they can print proof of attendance certificates, which may be used towards securing CPE credits.

[Learn More](#)

Enterprise Membership

Your entire organization gains unlimited access to our training portfolio for the entire year. Each division may access the webinars that are appropriate based on their information security and risk management responsibilities. Transcript tracking pages are available to prove attendance, which may be used towards securing CPE credits.

[Learn More](#)

Registration Form

Customer Information

_____		_____	
First Name		Last Name	

Title			

Email Address			

_____		_____	
Company Name		Industry	

Address			

_____		_____	_____
City		State	Zip

_____		_____	
Telephone		Fax	

Webinar Title (optional)

1. _____

2. _____

3. _____

Payment Method

Check enclosed (Payable to "Information Security Media Group, Corp.")

Visa Mastercard AMEX Discover Company P.O.

_____		_____	
Card Number		Exp. Date	

Billing Address			

_____		_____	_____
City		State	Zip

_____		_____	
Signature		Date	

Webinar Benefits

- **Earn CPE credits**
- **Save time & money — no travel required**
- **Further your education on information security, fraud, compliance, and risk management topics**

Select Attendance Method

Multiple Sessions

Vouchers (4 pack) \$1,095

Vouchers (10 pack) \$2,795

Vouchers (20 pack) \$5,295

Unlimited Sessions (1 year)

Individual Membership \$1,895

Corporate Membership (Up to 5 individuals) \$6,995

Enterprise Membership (Unlimited individuals) CALL

Print and mail this form to:
 Information Security Media Group
 4 Independence Way, Suite 130
 Princeton, NJ 08540
or fax: (732) 875-1065

Register Online
 The easiest way to register! Visit
BankInfoSecurity.com/training



About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

Employee training is a necessity for individuals in the banking industry. Our training webinars are taught by industry experts, devoted to current topics and offer the ability to earn CPE credits. Learn to solve the information security and risk management challenges of today with ISMG training.

Contact

Contact a representative for information on membership options:

ISMG Membership Team
 (800) 944-0401
memberships@ismgcorp.com





4 Independence Way | Princeton, NJ 08540
ISMGCorp.com