infoRisk® TODAY

Course Matrix

Information Security | Risk Management | Compliance | Fraud

ISMG INFORMATION SECURITY MEDIA GROUP

From the RSA SecurID breach to Sony and Epsilon, there never have been so many high-profile incidents, which in turn have sparked greater public awareness of information security risks.

Tom Field

One of the results: a greater emphasis on training and awareness – for everyone in the organization, ranging from customer-facing personnel to senior business management.

At Information Security Media Group, we've assembled a broad suite of webinar training programs relevant to your career needs, including:

- Regulatory Compliance – with a new suite of exclusive sessions on how to conform with the FFIEC Authentication Guidance.
- Fraud – with an 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 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 catalogue, and be sure to offer your own suggestions for new course offerings.

Tom Field,
Editorial Director
Information Security Media Group

Table of Contents

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

Course Category Matrix

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
1	5 Critical Data Security Predictions for 2011	205						○		○	●	
2	Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249		○							●	
3	Anti-Money Laundering/Fraud Convergence: Why Should I Care?	59		○	●		○		○			
4	Anti-Money Laundering: The Practitioner's Guide to the Laws	153		○	●				○			
5	Anti-Money Laundering: The Investigator's Guide to the Laws	154		○	●				○			
6	Application Security Testing and OCC Bulletin 2008-16 Compliance	110		○						○	●	○
7	Assessing Encryption Standards for Financial Institutions	130							○		●	○
8	ATM Fraud: Strategies to Beat the Skimming Scams	125					●				○	
9	Automating Security Controls Within Government Information Systems	160						●	○		●	
10	Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87						●		○		
11	Malware, Phishing & Mobile Security: Trending Threats	215		●							○	
12	Beyond Heartland: How to Prevent Breaches of Security and Trust	129					●			○	○	
13	Beyond Phishing - The Growing Crimeware Threat	29					●			○		
14	Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238		○			○				●	
15	Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11						●				
16	BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80		○	●				○			
17	Business Banking Under Attack: How to Fight Back Against Cybercriminals	149					●				○	
18	Business Continuity Planning Best Practices	27				●						
19	Business Continuity Risk Assessment & Resource Allocation	96				●		○	○			
20	Business Impact Analysis — How to Get it Right	95				●		○				
21	Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152					●				○	
22	Cloud Computing: Regulatory Security & Privacy Challenges	188		●						○	●	●
23	Complying with the FFIEC Guidance on a Budget	253		●			○				○	
24	Creating a Culture of Responsible Application Security	248						○	○		●	
25	Creating a Culture of Security - Top 10 Elements of an Information Security Program	150		○				●				
26	Cross-Border Fraud: How to Spot it, How to Stop it	183					●	○				
27	Data Protection and Incident Response	162						●		○		○
28	Data Protection: The Dirty Little Secret	208							○		●	
29	Debit Fraud: Trends and Typologies	194					●		○		●	
30	Defending Against The Insider Threat	67					●	○		○		
31	Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate	168					●			○		
32	Electronic Evidence & e-Discovery: What You Need to Know & Protect	158		●				○	○			
33	Email Security Requirements for Healthcare Providers: HIPAA & Beyond	180		○						○	●	

● = Primary Category ○ = Secondary Category

Course Category Matrix

infoRisk TODAY

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
34	Embezzlement (Part 1): When Everyone Lies, Cheats & Steals	133					●					
35	Embezzlement (Part 2): Conducting Financial Crime Investigations	134					●					
36	Encrypting Servers Across the Financial Services Enterprise	257							○		●	
37	Encryption: What, Why and Especially How			○					○		●	○
38	Evaluating Security Risks Associated with Banking Vendors	127								○	○	●
39	Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86		○	●							○
40	FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251		●	○		○		○			
41	FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244		○				●	○			
42	FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242		●			○					●
43	FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232		●			○		○		○	
44	FFIEC Authentication Guidance: How to Create a Layered Security Strategy	246		○					○		●	
45	FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230		●			○	○			○	
46	FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243		○								●
47	FFIEC Authentication: How to Invest in Anti-Fraud and Operational Controls	245		○							●	
48	FFIEC Authentication: The Myths and Truths of Anomaly Detection	241		○			○				●	
49	FFIEC Guidance: How to Use Layered Security to Fight Fraud	247		○					○		●	
50	Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge	187		○			●				●	
51	Fighting Fraud Schemes: Education, Response and Defense	40					●	○			○	
52	Fighting Online Banking Cybercrime with a Holistic Security Strategy	172					●	○			○	
53	Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights	120		○			●				○	
54	Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities	177					●	○			●	
55	Fraud Prevention Strategies for 2010: How to Protect Your Customers...and Your Business	171					●			○	○	
56	Gaining Control of Compliance Mandates, Security Threats, & Data Leaks	147		●					○			
57	GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy	94		●						○		
58	HIPAA and HITECH Enforcement: How to Secure Health Information	174		●						○		
59	How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution	83					●			○	○	
60	How to Achieve Network Security Without Compromising Performance	225						○			●	
61	How to Build a Successful Enterprise Risk Management Program	250						●	○			
62	How to Develop & Maintain Information Security Policies & Procedures	135		○				●	○			
63	How to Improve Network Security on a Limited Federal Budget	236						○			●	
64	How To Launch a Secure & Successful Mobile Banking Platform	105									●	
65	How to Prepare for Your First Identity Theft Red Flags Rule Exam	113		●					○	○		
66	How to Prevent Data Leakage from Compromising Your Company's Security	50						●				

● = Primary Category ○ = Secondary Category

Course Category Matrix

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
67	How to Prevent Security Breaches Through Effective Management and Control of USB Devices	148						○	○		●	
68	How to Use Your Mobile Phone for Free Two-Factor Authentication	58									●	
69	How Well Do You Know Your Vendors?	13						○		○		●
70	ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance	142		●			○			○		
71	Identity Theft: How to Respond to the New National Crisis	155					●			○		
72	Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81		●						○		○
73	Incident Response: How to React to Payment Card Fraud	144					●			○		○
74	Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20		○				●				
75	Information Security for Management – What Your Senior Leaders Need to Know	137		○				●				
76	Information Security Policies & Standards Development	53		○				●				
77	Innovative Authentication Process Provides the Ultimate Security for Online Banking	165		○			○				●	
78	IT Risk Assessments: Understanding the Process	10		○				●	○			
79	Information Tech. Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands	28		●							○	
80	Insider Fraud - Profiling & Prevention	35					●			○		
81	Insider Threat: Defend Your Enterprise	66						●				
82	Insider Threats - Safeguarding Financial Enterprise Information Assets	85					●					
83	Integrating Risk Management with Business Strategy	176						●				
84	Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution	65		●					○	○		
85	Is Your Device Identification Ready for New FFIEC Guidance?	217		●						○	●	
86	Key Considerations for Business Resiliency	151						●				
87	Legal Considerations About Cloud Computing	159		○				○			●	○
88	Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b	19		●					○			
89	Maintaining Secure Government Information Systems	173						●			○	
90	Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses	30					○				●	
91	Malware: Fight Back Using Layered Security	222							○		●	
92	Managing Shared Passwords for Super-User Accounts	170						○			●	
93	Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178					●			○	○	
94	Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132		●						○		○
95	Meeting Federal Compliance to Secure Windows Desktops	189		●					○		●	
96	Mobile Technology: How to Mitigate the Risks	256						○			●	
97	Money Laundering Update: The Latest Threats to Your Institution	116			●		○		○			
98	Fraud Prevention: Understand & Mitigate Threats to Global Institutions	213					○				●	
99	Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72				○		●	○	○		

● = Primary Category ○ = Secondary Category

Course Category Matrix

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
100	Pandemic Planning & Response Techniques	77		○		●						
101	PCI Compliance: Tips, Tricks & Emerging Technologies	212		●							○	
102	Power Systems: How to Prevent Unauthorized Transactions	190		○					○		●	
103	Practical User Authentication Strategies for Government Agencies	166					○		○		●	
104	Preparing for an Information Technology Regulatory Exam	18		●							○	
105	Preparing for Your Next Audit: The Five Habits of Successful Security Programs	219		○					●			
106	Preparing Your Institution for an IT Audit	26							●			
107	Preventing Malware: Tips to Staying FFIEC Compliant	223		○							●	
108	Preventing Phone Fraud with Voice Biometric Authentication	36					●				○	
109	Preventing TJX Type Data Breaches	33									●	○
110	Preventing Unauthorized Access To Your Institution's Data	119							○		●	
111	Proactive IT Risk Assessment Strategies	140		○				●				
112	Protect Data in the Cloud: What You Don't Know About the Patriot Act	227		●					○	○	●	
113	Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention	185		●					○		●	
114	Protecting Government Agency Assets Through Improved Software Security	220						○	○		●	
115	Protecting the Exchange of Sensitive Customer Data with Your Vendors	100								○	○	●
116	Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97		●								○
117	Red Hat Enterprise Linux 6 Common Criteria	229							○		●	
118	Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102		●				○				
119	Risk Management Framework: Learn from NIST	255		○				●				
120	Securing Your Email Infrastructure	141		○						○	●	
121	Security Risks of Unified Communications: Social Media & Web 2.0	146									●	
122	Fighting Fraud: Stop Social Engineers in Their Tracks	89		○				●		○		
123	Social Networking: Is Your Institution Ready for the Risks?	145								○	●	
124	Social Networking Compliance for FINRA Regulated Organizations	193		●					○	○	●	
125	5 Steps to Managing Security Risk from Your Software Vendors	143		○								●
126	Taking Fraud Out of Online Banking	44					●			○	○	
127	Testing Security Controls at a Banking Institution: Learn from the Experts	56		○					○		●	
128	The Dirty Little Secret About Network Security	204		○				○			●	
129	The Faces of Fraud: Fighting Back	207					●	○				
130	The Faces of Fraud: How to Counter 2011's Biggest Threats	196					●	○				
131	The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink	192					●				●	
132	The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights	118									●	

● = Primary Category ○ = Secondary Category

Course Category Matrix

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
133	The Identity Enabled Network: The Future of Secure Cyberspace	163						○			●	
134	The Identity Management Challenge for Financial Institutions	48					○			○	●	
135	The Mobile Environment: Challenges and Opportunities for Secure Banking	216							○		●	
136	The Reality of Cyberattacks: Emerging Solutions for Today's Threats	179									●	
137	The Role of Out-of-Wallet Questions in Meeting the Updated FFIEC Guidelines	237		○					○	○	●	
138	The State of Government Information Security Today	226						●				
139	Threat Detection, Compliance & Incident Response	181		●				○				
140	Time: The Hidden Risks - How to Create Compliant Time Practices	161		○							●	
141	Top 20 Critical Controls to Ensure Painless FISMA Compliance	167		○				●				
142	Top 5 Reports IT Auditors Request	214		○				○	●			
143	Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?	73		●						○	○	○
144	Turn FFIEC Compliance into Customer Loyalty and Retention	252		○				●				
145	U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169					●				●	
146	User Authentication: Best Practices for Managing Risk & Compliance	41		○				○			●	
147	Understand How Financial Institutions Can Benefit from Utilizing Tokenization	239		○						○	●	
148	Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98		○					○			●
149	Vendor Management Part II: Assessing Vendors - The Do's and Don'ts of Choosing a Third-Party Service Provider	104		○					○	○		●
150	Vendor Management Part III: Inside the BITS Shared Assessments Program	117							○			●
151	Vendors' Guide to the FFIEC Authentication Guidance	231		●			○					
152	Voice Over IP - Helping Financial Institutions Learn and Mitigate Security Risks	39									●	
153	You & Your Vendors: How to Best Secure Data Exchange	88		○							○	●
154	ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band	211					●				○	

● = Primary Category ○ = Secondary Category

Education OnDemand

Customize your curriculum by attending sessions specific to the needs of your institution.

1 Register

Our 130+ Premium Webinars cover a wide range of topics including information security, compliance, business continuity, fraud, technology, vendor management, and more. We understand that, at many institutions, this broad spectrum of topics can fall under the responsibility of one team and sometimes even one individual. This extensive curriculum allows users to register for any in-depth webinar and gain actionable advice on any topic they're interested in, not only one focused concentration.

Curriculum Tracks

We've organized several webinars into tracks to help users see the depth of our webinar education for some of today's most popular topics.

Customize your education – focus on a webinar track or build your own. You decide what training you need and attend as you need to.

2 Attend

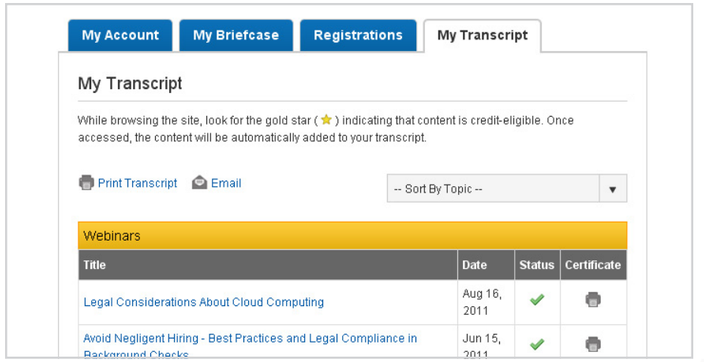
Presented by industry experts with years of experience, these 90 minute sessions provide in-depth actionable advice to implement at your institution. These vital topics warrant so much comprehensive education that our Premium Webinars also come with Presentation Handbooks that include slides and additional research and resources.

In addition, we give our users the added benefit of convenience by providing several ways to attend. Register for a scheduled session on our Webinar Calendar, view Sponsored OnDemand sessions or view any webinar anytime OnDemand as many times as needed with our Premium Annual Membership.

3 Track Your Progress

If required to report to your manager or to an association that provides your certification for your Continuing Professional Education Credits, our system allows tracking for the education you've attended. We can provide Proof of Attendance Certificates for any Premium Webinar attendee.

Premium Annual Members also gain access to a Transcript Tracking interface that shows all Credit Eligible content viewed including articles, podcasts, handbooks and webinars. Annual Members use this interface to print Proof of Attendance Certificates or their entire educational transcript at any time.



Curriculum Tracks

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

FFIEC Authentication Guidance Track

From how to create a layered security program to preparing for your next regulatory exam, our faculty has created a suite of exclusive new training programs designed to help your institution conform with the FFIEC Authentication Guidance. Learn the next steps your institution should take from the industry's top regulators, security leaders and analysts.

Course Title	ID
Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249
Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238
Complying with the FFIEC Guidance on a Budget	253
FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232
FFIEC Authentication Guidance: How to Create a Layered Security Strategy	246
FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230
FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243
FFIEC Authentication: How to Invest in Anti-Fraud and Operational Controls	245
FFIEC Authentication: The Myths and Truths of Anomaly Detection	241
FFIEC Guidance: How to Use Layered Security to Fight Fraud	247
Is Your Device Identification Ready for New FFIEC Guidance?	217
Preventing Malware: Tips to Staying FFIEC Compliant	223
The Role of Out-of-Wallet Questions in Meeting the Updated FFIEC Guidelines	237
Turn FFIEC Compliance into Customer Loyalty and Retention	252
Vendors' Guide to the FFIEC Authentication Guidance	231

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

MGMT255

Risk Management Framework: Learn from NIST

Learn the fundamentals of developing a risk management program from the man who wrote the book on the topic including: understanding the current cyber threats, developing a multi-tiered risk management approach, and implementing NIST's risk management framework.

Presented by Ron Ross, Sr. Computer Scientist & Info Security Researcher, NIST

Course Title	ID
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
Business Continuity Risk Assessment & Resource Allocation	96
Business Impact Analysis — How to Get it Right	95
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Evaluating Security Risks Associated with Banking Vendors	127
How to Build a Successful Enterprise Risk Management Program	250
IT Risk Assessments: Understanding the Process	10
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands	28
Integrating Risk Management with Business Strategy	176
Key Considerations for Business Resiliency	151
Mobile Technology: How to Mitigate the Risks	256
Proactive IT Risk Assessment Strategies	140
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102
Risk Management Framework: Learn from NIST	255
Social Networking: Is Your Institution Ready for the Risks?	145
5 Steps to Managing Security Risk from Your Software Vendors	143
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98

Prepare for the risks and threats every institution faces on a daily basis.

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

FR196

The Faces of Fraud: How to Counter 2011's Biggest Threats

Payment card breaches, check fraud and phishing/vishing - these are the most common forms of fraud striking banking institutions today. Join a panel of fraud experts as they look at eye-opening survey results and how institutions can act upon them.

Presented by Mike Urban, Sr. Director & Fraud Chief, FICO; Matthew Speare, SVP, M&T Bank; Tom Field, Editorial Director, ISMG

Course Title	ID
Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249
ATM Fraud: Strategies to Beat the Skimming Scams	125
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Beyond Phishing - The Growing Crimeware Threat	29
Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238
Business Banking Under Attack: How to Fight Back Against Cybercriminals	149
Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152
Cross-Border Fraud: How to Spot it, How to Stop it	183
Debit Fraud: Trends and Typologies	194
Defending Against The Insider Threat	67
Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate	168
Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge	187
Fighting Fraud Schemes: Education, Response and Defense	40
Fighting Online Banking Cybercrime with a Holistic Security Strategy	172
Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights	120
Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities	177
Fraud Prevention Strategies for 2010: How to Protect Your Customers...and Your Business	171
How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution	83
Identity Theft: How to Respond to the New National Crisis	155

Course Title	ID
Incident Response: How to React to Payment Card Fraud	144
Insider Fraud - Profiling & Prevention	35
Insider Threats - Safeguarding Financial Enterprise Information Assets	85
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178
Fraud Prevention: Understand & Mitigate Threats to Global Institutions	213
Preventing Phone Fraud with Voice Biometric Authentication	36
Taking Fraud Out of Online Banking	44
The Faces of Fraud: Fighting Back	207
The Faces of Fraud: How to Counter 2011's Biggest Threats	196
The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink	192
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169
ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band	211

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

Compliance Track

Government regulation is a key motivator in institutions bolstering their information security and risk management policies and procedures. In many cases the regulatory guidance issued is unclear or vague, making preparation for exams an arduous task. These webinars provide practical advice directly from regulators, examiners and practitioners.

New this year: An entire suite of sessions dedicated to helping financial institutions and their vendors conform with the FFIEC Authentication Guidance.

These webinars provide practical advice directly from regulators, examiners and practitioners.

FEATURED

COMP86

Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties

At the core of any good Anti-Money Laundering (AML) program is the Suspicious Activity Report (SAR), which all financial institutions must file when confronting questionable transactions. Learn all SAR writing guidelines and etiquette as well as how and when to properly complete and file a SAR.

Presented by Kevin Sullivan, Investigator, NY State Police

Course Title	ID
Anti-Money Laundering: The Practitioner's Guide to the Laws	153
Anti-Money Laundering: The Investigator's Guide to the Laws	154
Application Security Testing and OCC Bulletin 2008-16 Compliance	110
ATM Fraud: Strategies to Beat the Skimming Scams	125
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80
Cloud Computing: Regulatory Security & Privacy Challenges	188
Complying with the FFIEC Guidance on a Budget	253
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86
FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232

Course Title	ID
FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230
FFIEC Guidance: How to Use Layered Security to Fight Fraud	247
Gaining Control of Compliance Mandates, Security Threats, & Data Leaks	147
GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy	94
HIPAA and HITECH Enforcement: How to Secure Health Information	174
How to Develop & Maintain Information Security Policies & Procedures	135
How to Prepare for Your First Identity Theft Red Flags Rule Exam	113
ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance	142
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Information Security for Management – What Your Senior Leaders Need to Know	137
Information Security Policies & Standards Development	53
IT Risk Assessments: Understanding the Process	10
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands	28
Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution	65
Is Your Device Identification Ready for New FFIEC Guidance?	217
Legal Considerations About Cloud Computing	159
Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b	19
Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132
Meeting Federal Compliance to Secure Windows Desktops	189
Pandemic Planning & Response Techniques	77
PCI Compliance: Tips, Tricks & Emerging Technologies	212
Preparing for an Information Technology Regulatory Exam	18
Protect Data in the Cloud: What You Don't Know About the Patriot Act	227
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102
Risk Management Framework: Learn from NIST	255
Social Networking Compliance for FINRA Regulated Organizations	193
Threat Detection, Compliance & Incident Response	181
Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?	73
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98
Vendors' Guide to the FFIEC Authentication Guidance	231

Payments Security 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 everyday, 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
ATM Fraud: Strategies to Beat the Skimming Scams	125
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Beyond Phishing - The Growing Crimeware Threat	29
Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152
Cross-Border Fraud: How to Spot it, How to Stop it	183
Debit Fraud: Trends and Typologies	194
Encrypting Servers Across the Financial Services Enterprise	257
Fighting Online Banking Cybercrime with a Holistic Security Strategy	172
How To Launch a Secure & Successful Mobile Banking Platform	105
Innovative Authentication Process Provides the Ultimate Security for Online Banking	165
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178
PCI Compliance: Tips, Tricks & Emerging Technologies	212
Preventing TJX Type Data Breaches	33
Taking Fraud Out of Online Banking	44
The Faces of Fraud: Fighting Back	207
The Mobile Environment: Challenges and Opportunities for Secure Banking	216
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169

Checks, payment cards, online and mobile transactions – payments are the lifeblood of banking and the greatest source of fraud risks.

FEATURED

FR169

U.S. Dept. of Justice on Payment Card Fraud Trends & Threats

Credit and debit cards are under increased attack by fraudsters, and organizations need to step up their efforts to protect against threat. Learn trends in debit and other payment card thefts, lessons learned from the biggest breaches, and what you can do to avoid being the next victim.

Presented by Kim Peretti, former senior counsel with the U.S. Dept. of Justice

Vendor Management Track

When an institution utilizes a vendor, that vendor's vulnerabilities become the institution's vulnerabilities. To ensure your customer's accounts are fully protected from threats, an in-depth vendor management program must be established. Webinars in this track are dedicated to providing you a framework to assess vendors, including what questions to ask and how to best secure sensitive information.

FEATURED

VM98

Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks

The FDIC's Donald Saxinger details exactly what federal regulators are looking for when it comes to managing third-party service provider relationships. Gain a clear understanding of Vendor Management guidance and the four main elements of an effective third-party risk management process.

Presented by Donald Saxinger, Senior Examination Specialist, FDIC and James Christiansen, CEO, Evantix

Course Title	ID
Evaluating Security Risks Associated with Banking Vendors	127
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243
How Well Do You Know Your Vendors?	13
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72
Protecting the Exchange of Sensitive Customer Data with Your Vendors	100
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
5 Steps to Managing Security Risk from Your Software Vendors	143
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98
Vendor Management Part II: Assessing Vendors - The Do's and Don'ts of Choosing a Third-Party Service Provider	104
Vendor Management Part III: Inside the BITS Shared Assessments Program	117
Vendors' Guide to the FFIEC Authentication Guidance	231
You & Your Vendors: How to Best Secure Data Exchange	88

Anti-Money Laundering Track

Anti-money laundering is one of the classic threats to financial institutions, and fighting this complex threat is a key component of Bank Secrecy Act compliance. This webinar track not only provides guidance on becoming BSA compliant and Suspicious Activity Reports but also sheds light onto how AML is evolving into the cross-border risk it is today.

Course Title	ID
Anti-Money Laundering/Fraud Convergence: Why Should I Care?	59
AML: The Practitioner's Guide to the Laws	153
AML: The Investigator's Guide to the Laws	154
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80
Cross-Border Fraud: How to Spot it, How to Stop it	183
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86
Money Laundering Update: The Latest Threats to Your Institution	116

FEATURED

AML153

Anti-Money Laundering: The Practitoner's Guide to the Laws

Money laundering is a growing crime that affects numerous organizations. Learn exactly what you need to know to uphold specific statutes and regulations that govern this crime. Gain details on key AML laws, penalties for money-laundering crimes, and how to respond to money-laundering mandates.

Presented by Kevin Sullivan, Investigator, NY State Police

Anti-Money Laundering has evolved into a cross-border concern for all financial organizations.

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.

FEATURED

GOV137

Information Security for Management – What Your Senior Leaders Need to Know

By law, senior leaders must know what's at risk, how information is protected and what they are doing to maintain compliance. Learn how to engage senior leaders about their role in enforcing security, creating an information security governance structure, and effective metrics to prepare for an incident.

Presented by Bill Sewall, Information Security Specialist

Course Title	ID
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
Creating a Culture of Security - Top 10 Elements of an Information Security Program	150
Data Protection and Incident Response	162
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
How to Build a Successful Enterprise Risk Management Program	250
How to Develop & Maintain Information Security Policies & Procedures	135
Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20
Information Security for Management – What Your Senior Leaders Need to Know	137
Information Security Policies & Standards Development	53
IT Risk Assessments: Understanding the Process	10
Insider Threat: Defend Your Enterprise	66
Integrating Risk Management with Business Strategy	176
Key Considerations for Business Resiliency	151
Maintaining Secure Government Information Systems	173
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72
Proactive IT Risk Assessment Strategies	140
Fighting Fraud: Stop Social Engineers in Their Tracks	89
Social Networking: Is Your Institution Ready for the Risks?	145
Threat Detection, Compliance & Incident Response	181

Premium Membership

Professionals that understand the need for continuing education know the advantages of a custom experience.

Why membership?

With new threats and tech trends emerging in the industry everyday, we understand the importance of up-to-date education. Our 130+ webinar courses presented by expert practitioners provide an extensive curriculum needed for every top professional in this area of expertise.

Unlimited Access

View our library of 130+ webinars as many times as you need. It's a perfect reference tool for specific projects or a refresher on infrequent topics.

OnDemand Viewing

All of our Annual Membership plans include 24/7 on-demand access to our entire library of premium webinars. Access education at your convenience, according to your schedule.

CPE Credit Tracking

Have a certification? Our members receive credit certificates for all content: webinars, articles, podcasts, handbooks and more, that may be used for continuing education credit.

Contact Us

Our team is available to answer all your membership questions and help you find the option that fits your needs.

Call us at (800) 944-0401

Choose from several membership options to fit your training needs.

Individual

One of the most cost-effective educational offerings available. Perfect for: small teams, community or mid-sized institutions, independent consultants, and even solution providers.

Corporate

Grant your team of 5 unlimited year-round webinar education. Limit your need for the difficult and often expensive undertaking of in-person (a.k.a. out-of-office) training sessions for the team.

Enterprise

Custom built to suit your institution's needs. You determine not only the number of team members that need access to our education, but also custom topics or subject matter for us to develop webinars specifically for your group.

Memberships Comparison Chart

	Subscriber Free	PREMIUM MEMBERSHIP Inividual $1,995	Corporate $7,495	Enterprise Tiered
Number of Licenses	1	1	5	Unlimited
Length of Membership	-	1 year	1 year	Custom
Access to 130+ Premium Webinars	$295 each	Unlimited	Unlimited	Unlimited
Latest News & Email Updates	✓	✓	✓	✓
Blogs from ISMG Journalists and Renowned Industry Experts	✓	✓	✓	✓
Interviews with Practitioners, Regulators, and Industry Analysts	✓	✓	✓	✓
Register for FREE Webinars	✓	✓	✓	✓
eHandbooks - Topical Driven Educational Resource	✓	✓	✓	✓
Premium Webinars				
Interact with Webinar Speakers		✓	✓	✓
Participate in Webinar Q&A		✓	✓	✓
Earn Continuing Education Credits (CPEs)		✓	✓	✓
Proof of Attendance Certificates		✓	✓	✓
Continuing Professional Education (CPE) Transcript Tracking		✓	✓	✓
OnDemand Access to All Webinars		✓	✓	✓
Webinar Handbooks and other Course Materials		✓	✓	✓
Accessibility				
Priority Registration for All Webinars		✓	✓	✓
Mobile Access (Available 2012)		✓	✓	✓
Automatic New Webinar Notification		✓	✓	✓
Access to All Resources for Multiple Team Members			✓	✓
Track Multiple Team Member Activity			✓	✓
Access to Webinar Q&A Transcripts			✓	✓
Ability to Transfer Membership			✓	✓
Manager/Supervisor Access				✓
Advanced Features				
Integrated Learning Management System (LMS)				✓
Integrate Courses into Your Corporate LMS				✓
Custom Webinar Development				✓
Incorporate Webinar Material into Your Internal Training Program				✓
Incorporate Webinar Material into External, Customer-Facing Training				✓
Use Webinars for Commercial Client Training				✓
Opportunity to Participate on the Education Advisory Council				✓

Registration Form

Members can attend unlimited webinars for 1 year.

Attendance Method

Single Session

- ☐ Single Attendee $295
- ☐ Multiple Attendees (Up to 5) $695

Multiple Sessions

- ☐ Vouchers (4 pack) $1,095
- ☐ Vouchers (8 pack) $2,795
- ☐ Vouchers (20 pack) $5,295

Unlimited Sessions (1 year)

- ☐ Individual Membership $1,995
- ☐ Corporate Membership $7,495
- ☐ Enterprise Membership ..... Call

Print and mail this form to:

Information Security Media Group
4 Independence Way, Suite 130
Princeton, NJ 08540

or fax to: (732) 875-1065.

Register Online

The fastest way to register for webinars!

ORDER TOTAL $ _____

Customer Information

NAME _____

TITLE _____

COMPANY _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

E-MAIL _____

PHONE _____ FAX _____

Webinars to Attend (Optional)

1. _____
2. _____
3. _____
4. _____
5. _____

Payment Method

○ **Check Enclosed** (Payable to "Information Security Media Group, Corp.")

○ **Visa** ○ **AMEX** ○ **MasterCard** ○ **Discover** ○ **Company P.O.**

CARD NUMBER _____ EXP. (MM/YY) _____

SIGNATURE _____

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

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

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

ISMG
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com