AP’s Ultimate Fraud Defense Checklist: Stop Threats Before They Cost You

Presented by:

Rich Arminio, Edenred Pay

Mark Brousseau, Brousseau & Associates

Edenred | Pay

IOFM Fall CONFERENCE & EXPO

Do you need NASBA CPE credits?

- Navigate to website: **iofm.cnf.io**
  or scan the QR code →
- Check-in and check-out of your sessions to track your attendance for NASBA CPEs
- Certified with IOFM? No need to check-in and out of sessions. Self-report CEUs on IOFM.com instead after the event!

Edenred | Pay

IOFM Fall
CONFERENCE & EXPO

Edenred Pay

Trusted by some of the nation's most prominent brands.

Experienced

- 30+ years in business
- 15+ years expertise in payments & invoice automation
- PCI, SOC 2 & HIPAA compliant
- Major U.S. bank partners
- In-house issuing & processing capabilities
- Certified Mastercard & Visa processor

Reliable

- More than 9,000 corporate customers
- $100b+ spend in invoices processed
- $9B+ virtual card processed annually
- 1M supplier relationships
- 20K platform users
- Largest customers with programs over $1BN

Innovative

- 22-40%+ vendor virtual card participation in accounts payable program
- Proprietary supplier database
- Dedicated Relationship Manager and Customer Service Manager
- Complete Invoice-to-Pay AP Automation Services
- Innovative card delivery methods: Straight-to- Processing, RPA on vendor portals

Automate

- A single solution for processing all paper and electronic invoices
- Automate payments in a single platform integrated with your ERP
- Guaranteed data capture accuracy
- Digital workflows configured to any business or industry requirement
- Complete audit tracking

Optimize

- Invoice and payment transparency
- Touch-free posting of invoices to ERPs and accounting software
- Online collaboration with expert-assisted exceptions resolution
- Intelligent payment decisioning
- Proprietary supplier database with expanding acceptance network

Monetize

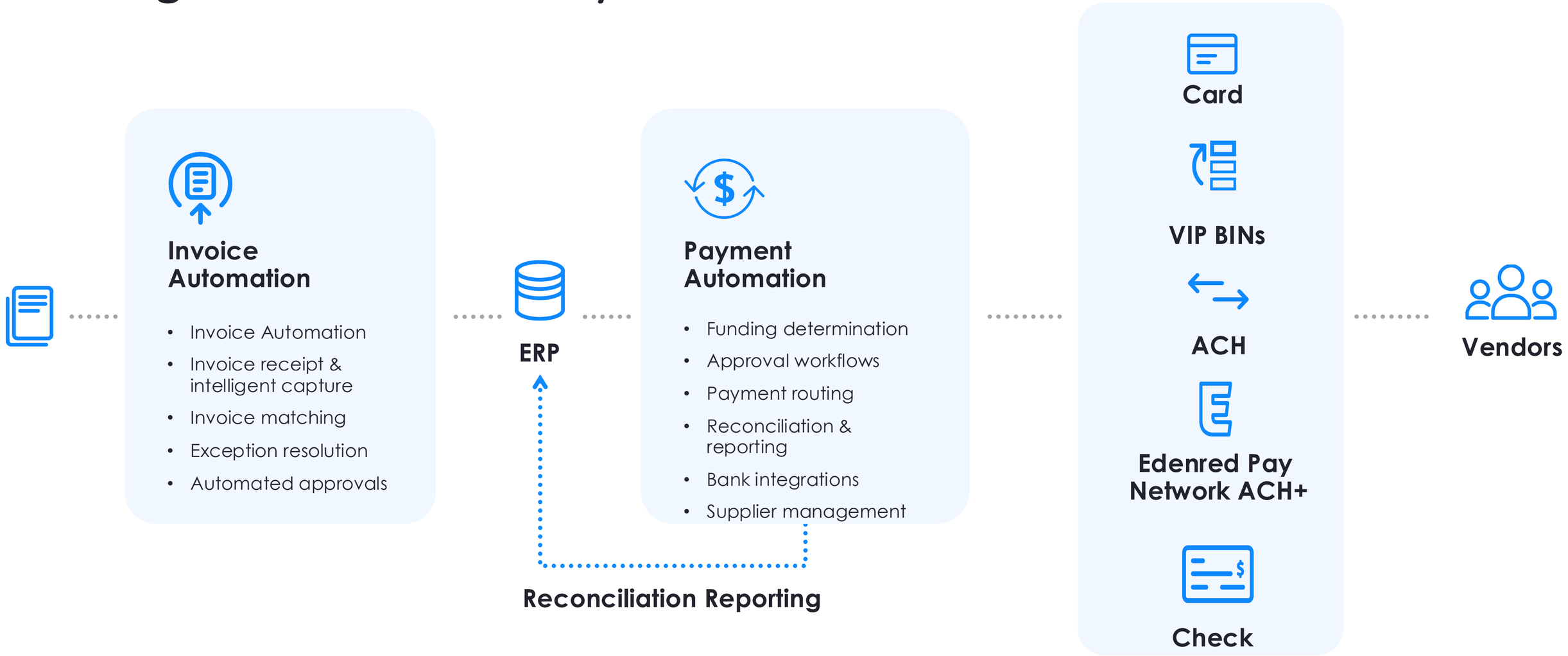
- Rebates on qualifying virtual card and network payments
- Vendor match for optimum virtual card adoption
- Optimized Vendor contact details via invoice images
- Real-time cash flow insights at the business unit and executive level
- Tools for extending payment terms

Elevate your processes

Elevate your department

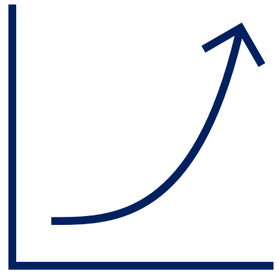
Elevate your business

Integrated Invoice-to-Pay Platform



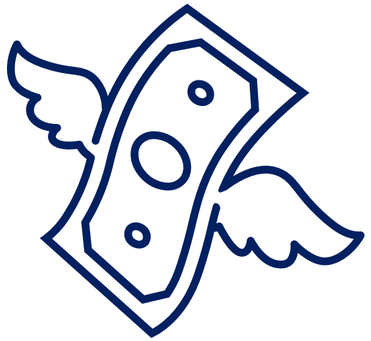
The Evolving Fraud Landscape

The Threat is Growing – And Getting Smarter



Payment fraud attempts up 80% since 2020

Attackers use AI, spoofing, and social engineering



One wrong click can trigger a six or seven-figure loss

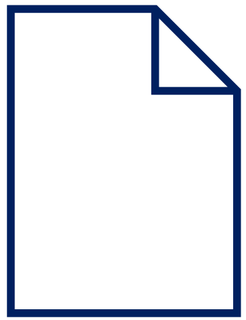
No industry or company size is immune

Common Schemes Targeting AP

Know Your Enemy

Phony bank account changes

Fake emails trying to “update” bank details



Fake invoices

Fraudsters intercept and alter legitimate invoices

Business email compromise (BEC)

Fake exec or vendor instructions

Deepfake-enabled voice fraud

AI voices mimicking real suppliers or execs

Why AP is a Prime Target

Where Fraudsters Find the Weak Spots

Email-heavy workflows → **easy entry point**

Manual processes → **poor verification trails**

Staff under pressure → **errors and rushed decisions**

Lack of vendor authentication → **open door**

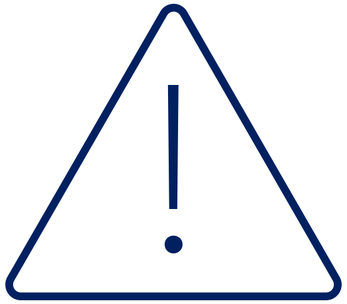
Real-World Impact

What Happens When Controls Fail

Misrouted payments can’t always be recovered

Financial loss leads to reputational damage

Regulatory exposure and internal fallout



A single incident can derail an entire quarter

Common Payment Fraud Schemes

Scheme Type	How It Works	Detection Difficulty	Typical Loss (Avg.)
Bank Change Scam	Email impersonation	High	$150K
BEC	Fake executive request	High	$125K
Vendor Impersonation	Lookalike domains	Medium	$80K
Deepfake Voice	Audio spoof	Very High	$250K

How Outdated Processes Leave AP Vulnerable

AP’s Ultimate Fraud Defense Checklist

Edenred | Pay

IOFM Fall CONFERENCE & EXPO

Legacy Processes, Modern Risks

Manual ≠ Secure

- Email approvals are easily spoofed
- Excel tracking hides anomalies
- Paper-based documentation limits visibility
- Check payments expose sensitive data

The Cost of Inefficiency

Time Lost = Risk Gained

- Every manual touchpoint adds exposure
- Delayed verifications = delayed detection
- Reactive controls miss evolving schemes
- Staff burnout increases human error

Red Flags of a Vulnerable Process

Warning Signs in Your AP Workflow

- Bank change requests handled by email
- Supplier info stored in spreadsheets
- No dual-approval for payment changes
- Vendor vetting done inconsistently

The Automation Advantage

Technology is Your Shield

- AI-driven verification detects anomalies
- Secure portals prevent unauthorized updates
- Automated audit trails strengthen compliance
- Continuous monitoring flags risk in real time

The Automation Advantage

Process Step	Manual Workflow	Automated Workflow	Risk Reduction
Vendor Setup	Email form	Secure portal	High
Bank Change	Manual update	Verified change request	Very High
Invoice Approval	Email routing	Rule-based workflow	High
Payment Execution	Manual ACH entry	Dual-auth electronic	Very High

Spot and Close the People, Process & Technology Gaps

AP’s Ultimate Fraud Defense Checklist

Edenred | Pay

IOFM Fall CONFERENCE & EXPO

People Gaps

Training is Your First Line of Defense

- Staff unaware of latest fraud tactics
- No standardized response playbook
- Over-reliance on “gut checks”
- Weak accountability across teams

Process Gaps

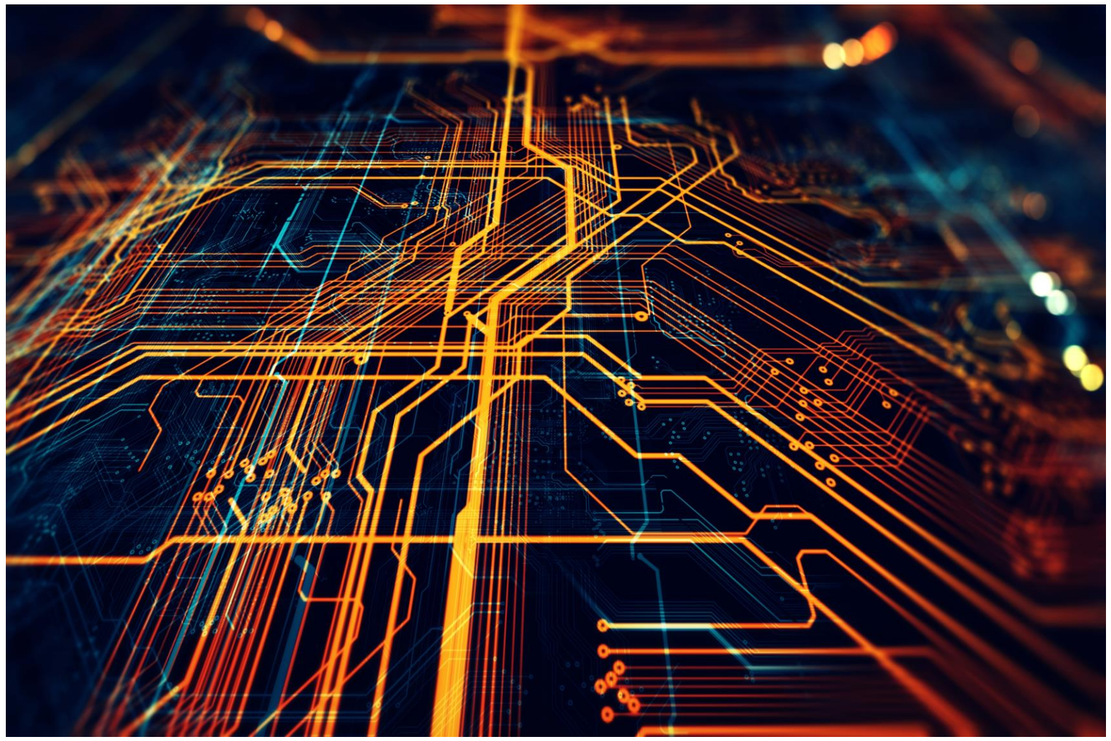
Controls Must Match the Risk

- Missing multi-level approvals
- Vendor setup not separated from payment approval
- Inconsistent bank verification procedures
- No formal incident escalation process

Technology Gaps

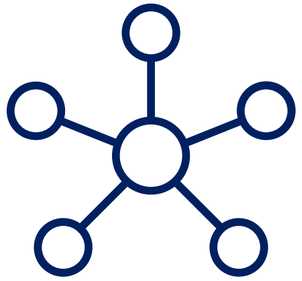
The Wrong Tools Invite Trouble

- Email is not secure
- ERPs not built for fraud prevention
- No anomaly detection or alerts
- Lack of supplier self-service verification
- Fragmented systems = blind spots



Closing the Gaps

Build a Unified Fraud Defense Framework



Centralize supplier data and verification

Enforce dual control on changes and payments

Integrate AI-based fraud detection

Audit, test, and update controls quarterly

Best Practices to Reduce the Risk of AP Payment Fraud

AP's Ultimate Fraud Defense Checklist

Edenred | Pay

IOFM Fall CONFERENCE & EXPO

Strengthen Verification Controls

Trust, But Always Verify

Independently verify every bank account change request

Use phone-back verification via known contacts

Use self-service supplier portals for onboarding & updates

Automate TIN, OFAC, & ownership checks

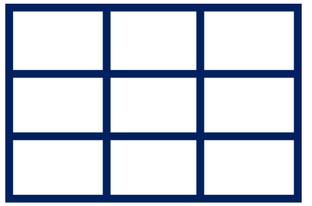
Secure Payment Methods

Replace Risky Paper with Protected Digital Channels

Virtual cards add built-in fraud protection

Network payments include account validation layers

Positive pay protects check disbursements

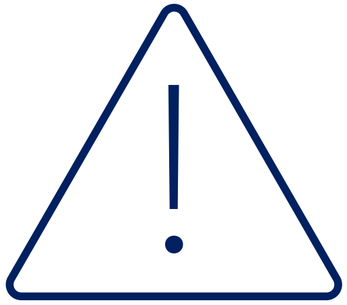


Automated reconciliation identifies issues fast

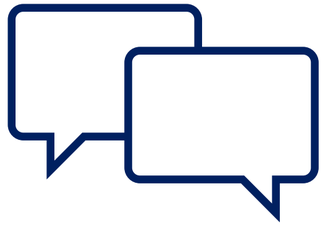
Build a Culture of Vigilance

Everyone Owns Fraud Mitigation

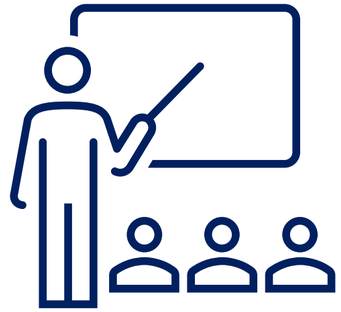
Conduct quarterly fire drills



Reward staff who report anomalies



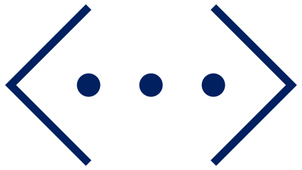
Share fraud incident lessons internally



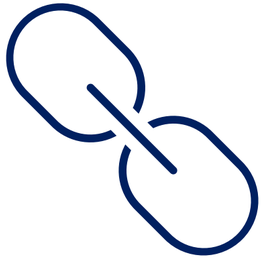
Make fraud prevention part of employee onboarding

Partner with the Right Technology Provider

Strength in Smart Automation



Use platforms that combine payment + verification



Ensure integrations with ERPs & banks

Choose providers with supplier onboarding expertise

Demand continuous monitoring and reporting

Build a Fraud Response Plan that Drives Fast, Confident Action

AP’s Ultimate Fraud Defense Checklist

Edenred | Pay

IOFM Fall CONFERENCE & EXPO

Why Every AP Team Needs a Response Plan

When (Not If) an Incident Happens

- Speed determines financial recovery
- Stakeholders need clear communication
- Regulators expect documented protocols
- Panic leads to mistakes – plans prevent them

Components of a Strong Plan

Define, Detect, Decide, and Document

- Incident definition and severity levels
- Escalation paths and response time targets
- Contact lists and communication templates
- Post-incident reviews & improvement tracking

Incident Simulation & Training

Practice Makes Prepared

- Run annual tabletop exercises
- Test detection-to-response speed
- Identify gaps between teams and systems
- Update playbooks after every drill

Turning Lessons Into Resilience

Evolve Faster than the Fraudsters

- Analyze incident data for patterns
- Strengthen controls where breakdowns occurred
- Build cross-functional ownership of fraud defense
- Celebrate “near-miss” detections as wins

Apply a Step-by-Step Fraud Mitigation Checklist

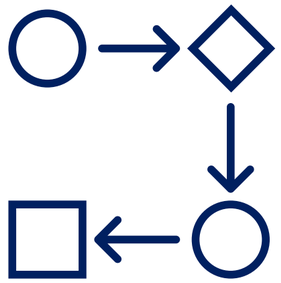
AP’s Ultimate Fraud Defense Checklist

Edenred | Pay

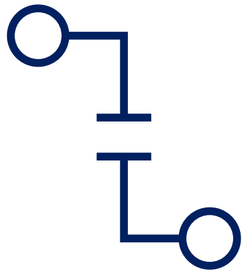
IOFM Fall CONFERENCE & EXPO

The Checklist Framework

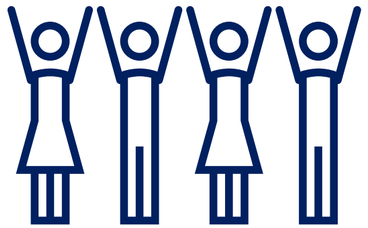
Assess. Improve. Monitor.



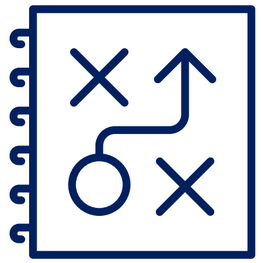
Evaluate current controls



Identify top vulnerabilities



Implement quick wins



Plan long-term improvements

Your Fraud Mitigation Roadmap

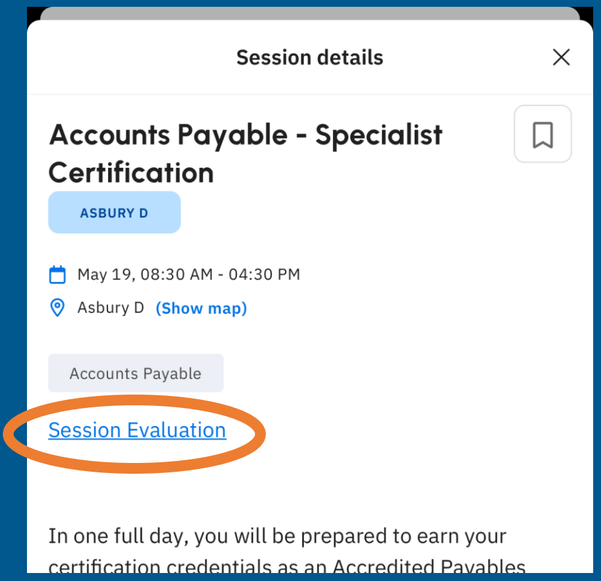
Build Layers of Protection

1. **People:** Train & test your team
2. **Process:** Standardize workflows
3. **Technology:** Automate verification
4. **Response:** Prepare for the unexpected

Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app

Session Presented by | Edenred Pay



Edenred | Pay

IOFM Fall CONFERENCE & EXPO

QUESTIONS?

Rich Arminio
Edenred Pay
203-641-2863
richard.arminio@edenred.com

Mark Brousseau
Brousseau & Associates
410-262-5078
m_brousseau@msn.com
@markbrousseau

REMINDER!

If you checked in for NASBA CPE credit, check out at iofm.cnf.io