Payments Risk Management Knowledge FINAL

ID	*Topic Area/Knowledge Statement*	**Comments/ Notes**
1000	**FUNDAMENTALS OF PAYMENTS RISK MANAGEMENT**	**27%**
1001	Fraud strategies, trends, and threats, including prevention and mitigation	
1002	Enterprise Risk Management (ERM) techniques and methodologies (e.g., inherent vs. residual risk, detected vs. preventive controls, controls vs. mitigants)	
1003	Risk management frameworks (e.g., identifying, reporting, issue-tracking, escalation, resolution, and validation)	Include COSO, NIST in Handbook
1004	Factors that impact risk profiles (e.g., size and complexity of payment system products and services, IT infrastructure, dependence on third parties)	
1005	Factors that impact the scope and frequency of effective risk assessment (e.g., scope and complexity of the financial institution's activities, regulatory requirements, business complexities, transaction type)	
1006	Role of risk management in strategic planning (e.g., vetting and validation of products, procedures, and changes)	
1007	The impact of service disruptions on the integrity of payment systems	
1008	Types of risk (i.e., operational, credit, liquidity, strategic, reputational, legal, compliance, cross-channel, fraud, systemic, third-party, counterparty)	
1009	Testing, documenting, process flows, and sampling	
1010	The role of client/customer agreements with respect to payment products and services	
1011	Trend analysis methodologies and applications (e.g., relevance of issues and big picture, cross-channel, information sharing)	
1012	Types of non-public, financial and non-financial personal information that requires protection	
1013	Credit analysis techniques	
1014	Internal and external fraud databases and analysis tools	
1015	Risk and trend analysis and evaluation methodologies (e.g., correlation, predictive modeling, interdependencies, prioritization, cost-benefit)	
1016	Technology-based risk scoring applications (e.g., neural networks, behavioral fraud analysis)	
2000	**PAYMENT SYSTEMS**	**16%**
2001	Financial markets, including federal funds, foreign exchange, and cross-border	
2002	Alternative and/or emerging payment systems (e.g., distributed ledger, Hawala, mobile, blockchain, real-time)	
2003	Internal payment processing systems and applications	
2004	Intrabank and interbank payment and messaging systems (e.g., SWIFT, financial market utilities [FMU], payments clearing and settlement systems [PCSS])	
2005	Characteristics of transactions (e.g., parties, speed of settlement, finality)	
2006	Payment channels, processes, and types	
2007	Roles and responsibilities of participants based on payment channel	
2008	Type and timing of information to be provided by payment system participants	
3000	**PAYMENTS RISK POLICY AND GOVERNANCE**	**10%**
3001	Risk appetite and tolerance (e.g., risk acceptance, transferal, assignment)	

3002	Roles, responsibilities, and structure of organizational units and stakeholders	
3003	Regulatory environment impact on clients/customers and/or internal programs	
3004	Internal policies that address risk types	
3005	Effective procedures to support policies (e.g., risk, credit/underwriting, monitoring)	
4000	**PAYMENTS RISK MANAGEMENT SYSTEMS AND CONTROLS**	**22%**
4001	Business continuity and/or contingency plans as they relate to payments offered or processed (e.g., recovery and restoration of data, procedures for maintaining communication, alternative power sources, backup sites, recovery strategy, testing)	
4002	Types and applications of internal controls (e.g., financial, technical, procedural, administrative)	
4003	Processing and settlement of retail and wholesale payments (e.g., segregation of duties, reconcilement of input to output, management review)	
4004	Audit standards and practices	
4005	Authentication methods to verify identity	
4006	Capital adequacy relative to the value of payments across multiple systems	
4007	Processes and procedures to detect and prevent fraud and abusive, unfair, and/or deceptive financial transactions	
4008	Operational controls for funds transfer, clearance, and settlement activities (e.g., separation of duties and dual control procedures)	
4009	Anomalous transaction detection systems capabilities (e.g., payment history, behavior, purchase type, delivery information)	
4010	Customer identification program (CIP) and know your customer (KYC) due diligence program components and oversight	
4011	Onboarding procedures and processes	
4012	Vendor management programs and processes, including due diligence processes for selecting third-party service providers, and oversight processes for monitoring them	
5000	**PHYSICAL AND INFORMATION SECURITY**	**13%**
5001	Authentication requirements for transfer initiation	
5002	Policies, procedures, and systems to detect data breaches, alteration, and/or destruction	
5003	Policies, procedures, and systems to receive, store, transmit, and destroy payments and associated data in a secure manner and protect against data breaches, (e.g., PCI, OC5)	
5004	Record retention, destruction, and discoverability	
5005	Computer hardware, software, and telecommunications protocols used to support payments processing	
5006	Payments network infrastructure and connectivity	
5007	Data security procedures, techniques, and access controls (e.g., password complexity and strength, corporate and consumer authentication, access rights and privileges, segregation of staff access to account information, sensitive data retention policies/rules, encryption, access control of secure areas and documents, visitor monitoring and control)	
5008	Physical storage and security of data (e.g., locked storage space, key inventory, clean desk policy)	

6000	REGULATORY ENVIRONMENT	12%
6001	Rules and guidance applicable to specific payment systems (e.g., ECCHO Rules, *NACHA Operating Rules*, Clearing house and bankcard network operating rules, Federal Financial Institution Examination Council [FFIEC] Handbook)	
6002	Laws and regulations applicable to specific payment systems (e.g., Currency and Foreign Transactions Reporting Act of 1970; Regulations CC, DD, E, J; Bank Secrecy Act/Anti-Money Laundering (BSA/AML); Office of Foreign Assets Control (OFAC) requirements; Federal Reserve Bank Operating Circular 3)	
6003	Regulatory requirements for incident reporting (e.g., data breach, suspicious activity)	