

Revised BITS Payments Risk Competency Framework: Background and Context

**BITS Third Party Payment System Access
Working Group**

March 2010

Revised BITS Payments Risk Competency Framework: Background and Context

- **The Revised BITS Payments Risk Competency Framework (see page six) is a tool with broad utility across payment applications and payment providers.**
 - **The framework is designed to be utilized by:**
 - **Financial institutions**
 - **Third party payments providers**
 - **ACH providers**
 - **Regulators**
 - **Card networks**

Revised BITS Payments Risk Competency Framework: Background and Context

- The framework can feed existing or new regulatory risk assessment approaches, with positive industry consequences. It can provide:
 - Clearly defined high level best practices for payments fraud mitigation with clear guidance on how to achieve sustainable risk management excellence.
 - A more robust, standardized approach for evaluating the quality of payments risk management across a wide range of risk environments and relevant institutions.

Revised BITS Payments Risk Competency Framework: Background and Context

- **The Payments Risk Competency approach provides a standardized framework to relate risk management practices to the scope and complexity of a firm's payments business risk:**
 - **Enables the development of specific risk management practices that are appropriately scaled to the scope and complexity of payments risk (see illustrations on pages seven and eight)**
- **The Framework's risk management practices suggest an approach to embedding risk mitigation into existing process, instead of executing them as stand-alone compliance procedures.**

Revised BITS Payments Risk Competency Framework: Background and Context

- **Benefits of a Sustainable Payments Risk Assessments Approach:**
 - **Mature Risk Tools, Measurement and Analysis and Communication practices enable timely recognition of a changing risk profile**
 - **Mature Governance structures, Policies, Standards and Procedures establish management's expectations**
 - **Independent review of payments risk management process confirms the effectiveness of the program**
 - **The ultimate business benefit is reduced operational losses**

Revised Payments Risk Competency Framework

Level	Skills and Expertise	Awareness and Communication	Governance, Policies, Standards and Procedures	Risk Tools, Measurement, and Analysis	Audit and Competency Level Assessment
Level 1: Initial	Unidentified skills required for effective payments mitigation. A training plan does not exist and no formal training occurs.	Recognition of the need for the payments risk mitigation process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to payments risk mitigation processes and practices. The processes and policies are not consistently defined. There is no oversight of payment product risk or performance.	No systemic processes measure the source, magnitude and direction of payments risk. Some desktop based risk mitigation tools may exist, on a one-off basis. Management is unaware of the cost of compliance vs. the risk of inaction.	Independent assurance over key business and technical processes is not performed. <i>Competency level assessment: Self</i>
Level 2: Repeatable but Siloed and Intuitive	Minimum skills required for effective payments mitigation are identified for critical areas. Training is in response to needs or events, rather than on the basis of an agreed plan, and informal training on the job occurs.	There is awareness of the need to act. Management has begun to communicate regularly on payment system risk mitigation issues. Communication addressing payments risk issues occurs within individual organizational structures, but not between silos.	A set of mostly intuitive risk mitigation processes begins. Aspects of the process are repeatable from documentation and individual expertise. Informal understanding of policies and procedures may exist. An informal group meets occasionally to address and design risk mitigation procedures in response to specific payments events.	Management reactively assesses payments risk in existing operations, products and services. Knowledge-based and common approach payments risk mitigation tools exist and accrue to those who produce the initial assessments, but is not well understood outside of the local project team. Vendor tools may be acquired, but not be applied correctly, used or properly implemented.	Management and the Board understand external stakeholders require independent assurance. However, they perceive little value in an independent audit unless mandatory. <i>Competency level assessment: Internal, more formal</i>
Level 3: Defined Process	Skills requirements, including the development of a payments risk mitigation common body of knowledge, are defined and documented for all areas. A formal training plan has been developed, but formal training is based on individual initiative.	Understanding of the need to act. Management effectively communicates overall issues, including those from changes to network rules, new or revised regulatory guidance, technology trends, etc. Effective communication occurs within and across organizational lines.	Use of good practices emerge. Formal understanding of defined and documented risk mitigation processes, policies and procedures for key activities. Payments Committee has representatives from major payment channels. Specific loss events evaluated for cause and risk mitigation procedures. Payments risk and performance metrics reported and monitored for trends.	Management proactively develops payments risk tolerances, limits, policies, procedures and objectives. Defined plan for use and standardized tools to automate the payments risk mitigation process for basic purposes. Formal responsibility for measuring and reporting risk is assigned. Ad hoc tools are used to acquire data used for risk management but may not all be in accordance with the agreed plan, and may not be integrated.	Management acclimates to requirements of independent auditors. Management hires internal auditors and payments risk management specialists and codifies key policies. Auditor's opinion is important to the organization. <i>Competency level assessment: independent audit</i>
Level 4: Managed and Measurable	Skills requirements routinely updated for all areas, proficiency is ensured for all critical areas and certification is encouraged. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal payments risk mitigation experts are involved and the effectiveness of the training plan is assessed.	Payments risk mitigation requirements and importance of updating staff on changes that impact the payments business is understood. Mature communication techniques applied within and across organization and standard communication tools used. Feedback from customer-facing associates and backroom operational associates is captured and responded to efficiently. Policy exceptions identified and reported to the Payments Committee.	Payments risk mitigation process is sound and complete. Internal best practices applied across multiple business areas. All process aspects documented and repeatable. Policies approved and signed by management, including the Board of Directors. Standards for developing and maintaining processes and procedures, requiring a periodic review, adopted and followed. Payments Committee has representatives of all payments channels. Payments risk and performance metrics reported and monitored. Metrics compared to peers and/or payment brand.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve to either vendor or in-house solutions and some integrate with related tools. A wide range of payments risk mitigation techniques are used, with appropriate actions taken by management on a timely basis. The FI has benchmarks itself against industry performance metrics. Processes for capturing new types of payments risk are reliable and extended prior to entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in risk taking and payments risk avoidance. Management policies and board committee documents clearly indicate management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. <i>Competency level assessment: External audit</i>
Level 5: Optimized	Continuous personal and organizational skills improvement encouraged. Training and education support external best practices and leading risk mitigation techniques. Key positions require professional certification. Knowledge sharing is an enterprise culture. Knowledge-based risk mitigation systems deployed. External experts and industry leaders provide guidance.	There is forward-looking understanding of payments risk mitigation requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied within and across organizational lines and integrated communication tools are in use. Policy exceptions are identified by automated systems that allow action to be taken to effectively mitigate risk. Exceptions are reported to the Senior Management Committee.	External best practices and standards are applied. Process documentation is evolved to automated workflow. Processes, policies and procedures are standardized and integrated to enable end-to-end management and improvement. There is payment product oversight by a Senior Management Committee that meets regularly to proactively address risk in new payment products, review key payments risk and performance metrics and set payment risk appetite.	Payments risk management metrics increase in number and sophistication, and may include online or real time tools. These tools are fully integrated across the enterprise to enable end-to-end support of the processes. Enterprise wide monitoring and issue remediation is in place and as a result the FI has the ability to monitor transactions seamlessly across channels. The FI routinely benchmarks against industry performance metrics and typically excels. A portfolio approach is used to identify and aggregate enterprise-level cross channel payments risks. The entity is completely up to date with both regulatory requirements and any relevant regulatory guidance.	Internal audit and payments risk management practices are enterprise wide, repeatable and not dependent on key personnel or favorable business conditions. Audit tools and procedures reliably evolve and forecast over the horizon risks. Continuous monitoring is routine. <i>Competency level assessment: External certified risk based audit</i>

Risk Competency Framework Informs Aggregate Risk Assessment

Revised Payments Risk Competency Framework

Level	Skills and Expertise	Awareness and Communication	Governance, Policies, Standards and Procedures	Risk Tools, Measurement, and Analysis	Audit and Competency Level Assessment
Level 1: Initial	Undefined skills required for effective payments mitigation. A training plan does not exist and no formal training occurs.	Recognition of the need for the payments risk mitigation process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to payments risk mitigation processes and practices. The processes and policies are not consistently defined. There is no oversight of payment product risk or performance.	No systemic processes measure the source, magnitude and direction of payments risk. Some desktop based risk mitigation tools may exist, on a one-off basis. Management is unaware of the cost of compliance vs. the risk of inaction.	Independent assurance over key business and technical processes is not performed. <i>Competency level assessment: Self</i>
Level 2: Repeatable but Siloed and Intuitive	Minimum skills required for effective payments mitigation are identified for critical areas. Training is in response to needs or events, rather than on the basis of an agreed plan, and informal training on the job occurs.	There is awareness of the need to act. Management has begun to communicate regularly on payment system risk mitigation issues. Communication addressing payments risk issues occurs within individual organizational structures, but not between silos.	A set of mostly intuitive risk mitigation processes begins. Aspects of the process are repeatable from documentation and individual expertise. Informal understanding of policies and procedures may exist. An informal group meets occasionally to address and design risk mitigation procedures in response to specific payments events.	Management reactively assesses payments risk in existing operations, products and services. Knowledge-based and common approach payments risk mitigation tools exist and accrue to those who produce the initial assessments, but is not well understood outside of the local project team. Vendor tools may be acquired, but not be applied correctly, used or properly implemented.	Management and the Board understand external stakeholders require independent assurance. However, they perceive little value in an independent audit unless mandatory. <i>Competency level assessment: Internal, more formal</i>
Level 3: Defined Process	Skills requirements, including the development of a payments risk mitigation common body of knowledge, are defined and documented for all areas. A formal training plan has been developed, but formal training is based on individual initiative.	Understanding of the need to act. Management effectively communicates overall issues, including those from changes to network rules, new or revised regulatory guidance, technology trends, etc. Effective communication occurs within and across organizational lines.	Use of good practices emerge. Formal understanding of defined and documented risk mitigation processes, policies and procedures for key activities. Payments Committee has representatives from majoring payment channels. Specific loss events evaluated for cause and risk mitigation procedures. Payments risk and performance metrics reported and monitored for trends.	Management proactively develops payments risk tolerances, limits, policies, procedures and objectives. Defined plan for use and standardized tools to automate the payments risk mitigation process for basic purposes. Formal responsibilities for measuring and reporting risk is assigned. Ad hoc tools are used to acquire data used for risk management but may not all be in accordance with the agreed plan, and may not be integrated.	Management acclimates requirements of independent auditors. Management hires internal auditors and payments risk risk management specialists and codifies key policies. Auditor's opinion is important to the organization. <i>Competency level assessment: Independent audit</i>
Level 4: Managed and Measurable	Skills requirements routinely updated for all areas, proficiency is ensured for all critical areas and certification is encouraged. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal payments risk mitigation experts are involved and the effectiveness of the training plan is assessed.	Payments risk mitigation requirements and importance of updating staff on changes that impact the payments business is understood. Mature communication techniques applied within and across organization and standard communication tools used. Feedback from customer-facing associates and backroom operations associates is captured and responded to efficiently. Policy exceptions identified and reported to the Payments Committee.	Payments risk mitigation process is sound and complete. Internal best practices applied across multiple business areas. All process aspects documented and repeatable. Policies approved and signed by management, including the Board of Directors. Standards for developing and maintaining processes and procedures, requiring a periodic review, adopted and followed. Payments Committee has representatives of all payments channels. Payments risk and performance metrics reported and monitored. Metrics compared to peers and/or payment brand.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve to either vendor or in-house solutions and some integrate with related tools. A wide range of payments risk mitigation techniques are used, with appropriate actions taken by management on a timely basis. The FI has benchmarks itself against industry performance metrics. Processes for capturing new types of payments risk are reliable and extended prior to entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in risk taking and payments risk avoidance. Management policies and board committee documents clearly indicate management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. <i>Competency level assessment: External audit</i>
Level 5: Optimized	Continuous personal and organizational skills improvement encouraged. Training and education support external best practices and leading risk mitigation techniques. Key positions require professional certification. Knowledge sharing is an enterprise culture. Knowledge-based risk mitigation systems deployed. External experts and industry leaders provide guidance.	There is forward-looking understanding of payments risk mitigation requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied within and across organizational lines and integrated communication tools are in use. Policy exceptions are identified by automated systems that allow action to be taken to effectively mitigate risk. Exceptions are reported to the Senior Management Committee.	External best practices and standards are applied. Process documentation is evolved to automated workflow. Processes, policies and procedures are standardized and integrated to enable end-to-end management and improvement. There is payment product oversight by a Senior Management Committee that meets regularly to proactively address risk in new payment products, review key payments risk and performance metrics and set payment risk appetite.	Payments risk management metrics increase in number and sophistication, and may include online or real time tools. These tools are fully integrated across the enterprise to enable end-to-end support of the processes. Enterprise wide monitoring and issue remediation is in place and as a result the FI has the ability to monitor transactions seamlessly across channels. The FI routinely benchmarks against industry performance metrics and typically excels. A portfolio approach is used to identify and aggregate enterprise-level cross channel payments risks. The entity is completely up to date with both regulatory requirements and any relevant regulatory guidance.	Internal audit and payments risk management practices are enterprise wide, repeatable and not dependent on key personnel or favorable business conditions. Audit tools and procedures reliably evolve and forecast over the horizon risks. Continuous monitoring is routine. <i>Competency level assessment: External certified risk based audit</i>



Aggregate Risk Matrix*

Quality of Risk Management	Quantity of Risk		
	Low	Moderate	High
Weak	Low to Moderate	Moderate to High	High
Satisfactory	Low	Moderate	Moderate to High
Strong	Low	Low to Moderate	Moderate

*Source: Comptroller's Handbook - Large Bank Supervision

ACH Monitoring Red Flags Matrix

Control Objective	Risk	Monitoring Red Flag	ODFI Trigger Response by Maturity Level		
			Low (1-2)	Mid (3)	High (4-5)
Ensure Originator/Third Party is engaged in the business described during initial underwriting.	Business engages in high-risk or prohibited activities that introduces potential loss in payments system.	Percentage of returns in each category (NSF, Invalid, and Unauthorized) for Originator/Third Party above the industry average.	Interim Site Visit	Enhanced Monitoring or Interim Site Visit	Define and follow risk-based response plan
Ensure changes in Originator's/Third Party's business model are detected.	Originator's/Third Party's business model has changed since original underwriting presenting an increased risk to the payments system.	Change from underlying Originator/Third Party regarding agreed upon frequency of sends, file sizes and settlement times.	Immediate customer contact AND Interim Site Visit. Update Underwriting.	Immediate customer contact AND Enhanced Monitoring or Interim Site Visit. Update Underwriting.	Immediate customer contact AND Define and follow risk-based response plan. Update Underwriting.
Ensure changes in Originator's/Third Party's business model are detected.	Originator's/Third Party's business model has changed since original underwriting presenting an increased risk to the payments system.	Change from underlying Originator/Third Party regarding agreed upon transaction types.	Immediate customer contact AND Interim Site Visit. Update Underwriting.	Enhanced Monitoring or Interim Site Visit. Update Underwriting.	Define and follow risk-based response plan. Update Underwriting.
Ensure changes in Originator's/Third Party's business model are detected.	Originator's/Third Party's business model has changed since original underwriting presenting an increased risk to the payments system.	Exceeding three-day aggregate limits.	Immediate customer contact AND Interim Site Visit. Update Underwriting.	Immediate customer contact AND Enhanced Monitoring or Interim Site Visit. Update Underwriting.	Immediate customer contact AND define and follow risk-based response plan. Update Underwriting.
Ensure deterioration in Originator's/Third Party's business conditions are identified on a timely basis.	Originator/Third Party is experiencing cash flow problems or other issues that are impacting ability to settle transactions.	Originator/Third Party has other classified (high risk) credits with the ODFI or interim financials provided by Originator/Third Party indicate material change in financial condition.	Coordinate response with other Business Lines	Coordinate response with other Business Lines	Coordinate response with other Business Lines. Follow risk-based response plan.

For more information, contact:

Nicole Muryn

Nicole@FSRound.org

202-589-2535

Gary Roboff

Gary@FSRound.org

914-478-9360

Heather Wyson

Heather@FSRound.org

202-589-2446