

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 BITS Payments Risk Competency Framework

Payments Risk Competency 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	Skills required for effective payments risk mitigation are not identified. 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 exist to measure the source, magnitude and direction of payments risk, either from new or legacy products or services. 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. Competency level assessment: Self
Level 2: Repeatable but Siloed and Intuitive	Minimum skill requirements for effective payments mitigation are identified for critical areas. Training is provided 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 consistent set of risk mitigation processes begins to emerge, but are largely intuitive. Some aspects of the process are repeatable because of individual expertise and some documentation. Informal understanding of policies and procedures may exist. There is an informal group that meets occasionally to address specific payments loss events and designs specific risk mitigation procedures to address these events.	Management begins to reactively assess payments risk inherent to existing operations, products and services. A knowledge base of payments risk and common approaches to the use of payments risk mitigation tools exist and accues to those who produce the initial assessments but it is not well understood outside of the local project team. Vendor tools may have been acquired, but are probably not applied correctly, and may even have not been used or properly implemented.	Management and the Board are aware that external stakeholders (key customers, regulators, investors) require independent assurance. However, there is little perceived value in independent audit until it becomes mandatory. Competency level assessment: Internal, more formal
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.	There is understanding of the need to act. Management effectively communicates the overall issues, including those arising from changes to payment network rules, new or revised regulatory guidance, technology trends, etc. Effective communication occurs within and across organizational lines regarding payments issues.	Use of good practices has emerged. Payments risk mitigation processes, policies and procedures are appropriately defined and documented for all key activities. Formal understanding of policies and procedures exists. A standing Payments Committee with representatives from major payment channels exists. Specific loss events are evaluated for root cause and risk mitigation procedures are developed. Payments risk and performance metrics are reported and trends are monitored.	Management begins to proactively develop payments risk tolerances, limits, policies, procedures and objectives. A plan has been defined for use and tools have been standardized 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 with one another.	Management becomes acclimated to the requirements (frequency, issues, documentation request) of independent auditors. Management begins to allocate internal resources to hire internal auditors, payments risk management specialists, and to codify key policies. The organization begins to think "what will the auditors" say. Competency level assessment: Independent audit
Level 4: Managed and Measurable	Skills requirements are 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.	There is understanding of the full set of payments risk mitigation requirements and the need to keep staff current about material changes that could impact the payments business. Mature communication techniques are applied within and across organizational lines and standard communication tools are in use. Feedback from customer-facing associates and backroom operational associates is captured and acted upon in a timely manner. Policy exceptions are identified and reported to the Payments Committee.	Payments risk mitigation process is sound and complete; internal best practices are applied across multiple areas of the business. All aspects of the process are documented and repeatable. Policies have been approved and signed off by management, including the board of directors. Standards for developing and maintaining the processes and procedures are adopted and followed. Periodic review is required. A Payments Committee with representatives of all payments channels exists. Payments risk and performance metrics are reported and trends are monitored. The company metrics are compared to peer benchmarks and/or payment brand metrics.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve from ad hoc to either off the shelf or robust in-house solutions, and some have been integrated with other 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 begun to benchmark itself against industry performance metrics. Processes for capturing new types of payments risk are reliable and extended before entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in sensible risk taking and in payments risk avoidance. Management policies and board committee documents clearly indicate that management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. Competency level assessment: External audit
Level 5: Optimized	Continuous improvement of skills, based on clearly defined personal and organizational goals, is encouraged. Training and education support external best practices and use of leading edge payments risk mitigation concepts and techniques. Professional certification is required for key positions. Knowledge sharing is an enterprise culture and knowledge-based risk mitigation systems are being deployed. External experts and industry leaders are used for 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. Competency level assessment: External certified risk based audit

Risk Competency Framework Informs Aggregate Risk Assessment

Revised Payments Risk Competency Framework

Payments Risk Competency 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	Skills required for effective payments risk mitigation are not identified. 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 exist to measure the source, magnitude and direction of payments risk, either from new or legacy products or services. 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. Competency level assessment: Self
Level 2: Repeatable but Siloed and Intuitive	Minimum skill requirements for effective payments mitigation are identified for critical areas. Training is provided 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 consistent set of risk mitigation processes begins to emerge, but are largely intuitive. Some aspects of the process are repeatable because of individual expertise and some documentation. Informal understanding of policies and procedures may exist. There is an informal group that meets occasionally to address specific payments loss events and designs specific risk mitigation procedures to address these events.	Management begins to reactively assess payments risk inherent to existing operations, products and services. A knowledge base of payments risk and common approaches to the use of payments risk mitigation tools exist and accrues to those who produce the initial assessments but it is not well understood outside of the local project team. Vendor tools may have been acquired, but are probably not applied correctly, and may even have not been used or properly implemented.	Management and the Board are aware that external stakeholders (key customers, regulators, investors) require independent assurance. However, there is little perceived value in independent audit until it becomes mandatory. Competency level assessment: Internal, more formal
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.	There is understanding of the need to act. Management effectively communicates the overall issues, including those arising from changes to payment network rules, new or revised regulatory guidance, technology trends, etc. Effective communication occurs within and across organizational lines regarding payments issues.	Use of good practices has emerged. Payments risk mitigation processes, policies and procedures are appropriately defined and documented for all key activities. Formal understanding of policies and procedures exists. A standing Payments Committee with representatives from major payment channels exists. Specific loss events are evaluated for root cause and risk mitigation procedures are developed. Payments risk and performance metrics are reported and trends are monitored.	Management begins to proactively develop payments risk tolerances, limits, policies, procedures and objectives. A plan has been defined for use and tools have been standardized 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 management but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Management becomes acclimated to the requirements (frequency, issues, documentation request) of independent auditors. Management begins to allocate internal resources to hire internal auditors, payments risk management specialists, and to codify key policies. The organization begins to think "what will the auditors" say. Competency level assessment: Independent audit
Level 4: Managed and Measurable	Skills requirements are 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.	There is understanding of the full set of payments risk mitigation requirements and the need to keep staff current about material changes that could impact the payments business. Mature communication techniques are applied within and across organizational lines and standard communication tools are in use. Feedback from customer-facing associates and backroom operational associates is captured and acted upon in a timely manner. Policy exceptions are identified and reported to the Payments Committee.	Payments risk mitigation process is sound and complete. Internal best practices are applied across multiple areas of the business. All aspects of the process are documented and repeatable. Policies have been approved and signed off by management, including the board of directors. Standards for developing and maintaining the processes and procedures are adopted and followed. Periodic review is required. A Payments Committee with representatives of all payments channels exists. Payments risk and performance metrics are reported and trends are monitored. The company metrics are compared to peer benchmarks and/or payment brand metrics.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve from ad hoc to either off the shelf or robust in-house solutions, and some have been integrated with other 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 begun to benchmark itself against industry performance metrics. Processes for capturing new types of payments risk are reliable and extended before entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in sensible risk taking and in payments risk avoidance. Management policies and board committee documents clearly indicate that management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. Competency level assessment: External audit
Level 5: Optimized	Continuous improvement of skills, based on clearly defined personal and organizational goals, is encouraged. Training and education support external best practices and use of leading edge payments risk mitigation concepts and techniques. Professional certification is required for key positions. Knowledge sharing is an enterprise culture and knowledge-based risk mitigation systems are being deployed. External experts and industry leaders are used for 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 exceeds. 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 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. Competency level assessment: External certified risk based audit



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.

Additional Considerations: (1) Would Maturity Levels 1 and 2 monitor these type red flags? (2) Would these expectations encourage adoption of higher maturity levels?

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