

white *A Practical Approach to Acquiring Risk Assessment* **paper**

PRESENTED BY THE
RISK & FRAUD
MANAGEMENT COMMITTEE
OF THE ELECTRONIC
TRANSACTIONS
ASSOCIATION

March 2007





**ELECTRONIC TRANSACTIONS ASSOCIATION
2006-2007 RISK & FRAUD
MANAGEMENT COMMITTEE**

Laurie LeBoeuf (Chair)

CEO
Take Charge Business Consulting
14119 Bazell Drive
Willis, TX 77318
lleboeuf@tcbconsultingonline.com

Mimi Hart

President & CEO
MagTek, Inc.
20725 South Annalee Avenue
Carson, CA 90746
mimi.hart@magtek.com

Victoria Strayer

Vice President, Business Risk,
Operations, & Compliance
TSYS Acquiring Solutions
8320 S. Hardy Drive
Tempe, AZ 85284-2007
victoria.strayer@tsysacquiring.com

Jeffrey De Petro (Vice Chair)

Vice President
EVO Merchant Services
515 Broadhollow Road
Melville, NY 11747-3709
jdepetro@goevo.com

Richard (Rick) Heroux

President
Cost Savings Reduction Specialists
2671 SW Port St. Lucie Blvd.
Port St. Lucie, FL 34953
rheroux@carsi.com

Rob Tourt

Discover Network
2500 Lake Cook Rd.
Riverwoods, IL 60015
robtourt@discoverfinancial.com

Cathy Billings

AVP Risk Operations
Transfirst
371 Centennial Parkway
Louisville, CO 80027
cbillings@transfirst.com

Kevin Lavigne

Vice President
Federated Payments
2 Huntington Quadrangle
3rd Floor North
Melville, NY 11747
k1@fpsemail.com

Anthony Urquidez

Director of Operations
Signature Card Services
8360 Melrose Avenue
3rd Floor
Los Angeles, CA 90069
aurquidez@signaturecard.com

Stephanie Cook

Vice President, Risk and Fraud
Metavante Corporation
4900 West Brown Deer Rd
Milwaukee, WI 53223
Stephanie.cook@metavante.com

Chad Nielson

Senior Compliance and Risk Manager
Authorize.net
915 South 500 East
American Fork, UT 84003
cnielson@Authorize.Net

Ex-Officio

Frank D'Angelo

Metavante Corporation
Frank.dangelo@metavante.com

Martin Elliott

VISA USA
900 Metro Center Blvd.
Foster City, CA 94404
melliott@visa.com

Deana Rich

President
Merchant Acquirers Committee (MAC)
deanar@bizla.rr.com

ETA Staff Liaison

Rob Drozdowski
Senior Director
(202) 828-2635
rob.drozdowski@electran.org



ACKNOWLEDGEMENTS

Special thanks to the following individuals for their contributions to this white paper:

- Jeff De Petro
- Richard Heroux
- Laurie LeBoeuf
- Chad Nielson
- Victoria Strayer

TABLE OF CONTENTS

Executive Summary **4**

Risk Assessment Methodology **5**

- 2.1 Evaluation Criteria
- 2.2 Assessment Categories

Internal Audit and Controls **7**

- 3.1 Creation of a Strategic Audit System
- 3.2 Audit Policy Implementation
- 3.3 Audit Planning
- 3.4 Budgets and Reporting
- 3.5 Corrective Action and Dispute Resolution

Business Partner Review **9**

- 4.1 Performing Credit and Business Diligence
- 4.2 Registration
- 4.3 Ongoing Reviews

Merchant Review **11**

- 5.1 Creation of a Credit Policy
- 5.2 Credit Policy Implementation and Compliance
- 5.3 Ongoing Monitoring Assessment Categories

Acquisitions **13**

- 6.1 Purchase Agreement Due Diligence
- 6.2 Portfolio Review
- 6.3 Ongoing Reviews

Conclusion **15**

Appendix A
Risk Assessment Worksheet **16**



EXECUTIVE SUMMARY

Pick up any payments industry publication or attend any industry forum, and at some point the subject of risk mitigation, compliance, and confidence in the payments system is discussed. It is one of the most compelling challenges demanding our immediate attention and call to action—action that must result in a more uniformed approach to risk assessment.

Though risk management programs vary by company and are dependent upon risk profiles and a range of other factors, the core methodologies of an effective risk management program for the payment services industry are the same. They start with a solid credit program that evaluates all new business engagements and span through daily monitoring and ongoing reporting; all designed to mitigate risk while satisfying compliance and audit requirements.

We have compiled an assessment of the applicable risk categories and provided guidance on how to structure risk thinking around these components. These categories apply at the time of the credit review for new merchants, business partners, and acquisitions. They also provide the best way to prepare for the audit review.

The purpose of this white paper is to propose entity level risk assessment methodologies and to provide you with suggested processes and tools for documenting and analyzing risks within your company. This resource is intended to be reviewed and then adapted and customized by individual users within the payment services industry.

The appendix of this document contains a model worksheet intended to provide a framework for developing a customized risk assessment program. The template and criteria outlined in the document are intended to be illustrative in nature. Each company should consider factors unique to its own portfolio and risk management capabilities.

An electronic version of this document may be found on ETA's website at: www.electran.org/info/white_papers.asp.

RISK ASSESSMENT METHODOLOGY

First, in order to effectively manage risk, a company must identify and assess the specific risks to which it is subject. Today, regulators, external and internal auditors, third-party partners, and other types of governing organizations are more frequently requesting, or even requiring, companies to perform entity level risk assessments. These risk assessments can be key tools that help companies understand, document, and work to mitigate the risks to which they are exposed.

The ETA Risk & Fraud Management Committee has reviewed various methodologies and identified 11 types of risk that typically apply to members of the payment services industry. Each of the following risk categories should be evaluated and assessed for applicability to each individual company, department or entity under review.

- Strategic Risk
- Credit Risk
- Market Risk
- Systems Operational Risk
- Business Operational Risk
- Internal Fraud Risk
- External Fraud Risk
- Reporting Risk
- Compliance and Legal Risk
- Systemic Risk
- Reputational Risk

The category specifics will be reviewed in detail later in this document, but first let's review the general risk assessment methodology.

EVALUATION CRITERIA

For each risk category there are three areas of evaluation: Inherent Risk, Control Effectiveness, and Residual Risk.

Inherent Risk

The risk to the company without consideration of internal controls. In other words, if there were no organizational controls in place to reduce risk, what would be the level of risk exposure to the company for this risk category?

- Assessed as High, Moderate or Low depending on the potential impact of the risk exposure
- Impact may be determined by evaluating the potential for significant financial losses and the threat each particular risk has to continuing operations

Control Effectiveness

The evaluation of how effective the company controls are at reducing Inherent Risk. The control assessment should be based on some form of control testing, such as third-party audits, SAS 70 reports, reviews of internal testing documentation, performance, inquiries, examinations or observations.

- Assessed as Strong, Adequate or Weak
- Impact is dependent on (1) whether the control is designed to properly reduce risk, and (2) whether the control is in place and evidence exists to show that it is, in fact, operating effectively

Residual Risk

The remaining risk to the company after considering the effectiveness of their controls.

- Assessed as High, Moderate or Low
- Based on the assessment level of Inherent Risk and Control Effectiveness

The table below summarizes possible scenarios in the risk assessment process. It is important to note that a High Inherent Risk, based upon the specifics of the risk, may not be reduced to Low even with strong controls in place. It is also possible that adequate controls may not be enough to necessarily reduce the Inherent Risk level.

INHERENT RISK	CONTROL ASSESSMENT	RESIDUAL RISK
High	Strong	Moderate
High	Adequate	High
High	Adequate	Moderate
High	Weak	High
Moderate	Strong	Low
Moderate	Adequate	Low
Moderate	Adequate	Moderate
Moderate	Weak	Moderate
Low	Strong	Low
Low	Adequate	Low
Low	Weak	Low

ASSESSMENT CATEGORIES

Following are descriptions of each of the individual risk categories identified for companies in the payments services industry. To help you develop a strong and effective risk management program that is unique to your company's needs, it is recommended that you carefully consider and evaluate the applicability of each of these risk categories in terms of Inherent Risk, Control Assessment, and Residual Risk.

Strategic Risk

The risk involved with pursuing one business strategy over another. Strategic risk may exist in the products or services offered, the types of merchants or partners with which business is conducted, the adoption of certain policies or practices, the use of certain types of technology, or even the markets in which a company expands.

Credit Risk

The risk considered if a party to a payment transaction may be unable to provide the necessary funds for settlement of the payment or transaction.

Market Risk

The risk that industry market forces, such as competitors, partners, new entrants, technological developments, etc., could adversely affect the company business. This includes price erosion, commoditization, and technological disintermediation.

Systems Operational Risk

The risk of system failure or compromise. This includes transactions being altered or delayed due to an unanticipated incident, event, or problem affecting the systems operations. This could involve changes to payment interfaces as dictated by the third-party processors. This also includes natural disasters, software bugs, and unauthorized access to the system.

Business Operational Risk

The risk that a significant policy or procedure doesn't exist, is unclear, inaccurate, outdated, or just as importantly, not enforced. This includes failure to properly follow policies and procedures and the risk that inaccurate information is communicated as a result.

Internal Fraud Risk

The risk that an employee, merchant, reseller, or other partner commits fraud against the company. This includes misappropriation of assets (including theft of funds), consumer information or intellectual capital.

- **Note:** Merchant fraud may be considered Internal for risk assessment purposes as merchants are using the service provider's systems to process payments.

External Fraud Risk

The risk that an unauthorized entity/individual(s) commits fraud against the company or uses the company system to commit fraud. This includes compromised merchant or reseller accounts, theft of card account numbers, bank account numbers, or other sensitive information; extortion, theft of intellectual capital, etc.

Reporting Risk

The risk that inaccurate financial and non-financial information is used to make business decisions or is reported to external sources. This includes the financial report risk associated with Sarbanes Oxley.

Compliance and Legal Risk

The risk that the company, or an affiliated third party (for example, a processor, bank, merchant or reseller), involved with a payment system does not comply with statutory or regulatory requirements resulting in discontinuance of operations, losses or fines to the company, affiliated third parties, or to merchants.

Systemic Risk

The risk that another entity in the processing chain fails, shuts down, or terminates business relationships resulting in the inability of the company to process transactions or perform other critical, committed functions. Examples include regulatory failure, system failure, data security compromise or other market-related factors.

Reputational Risk

The risk of adverse publicity and the possible resulting loss of business from an incident event or problem within the payments industry or within the company directly.

- *The loss of business confidence from an incident may, in many cases, far exceed the direct financial loss or other damage incurred*

Note: All other risks, individually or combined, could lead to Reputational Risk.

INTERNAL AUDIT AND CONTROLS

In bygone times audits were confined to financial and accounting matters exclusively. Electronic systems have evolved so rapidly that the audit function must now be regarded as protecting not only financial information, but also data infrastructure. As a result of this evolution, the audit function now spans the *entire* business enterprise. Representatives from Accounting, Operations, Data Processing/IT and Human Resources, at a minimum, must now be part of enterprise controls and auditing. Internal audits and collaborative oversight are the keys to preserving financial and data integrity.

The single most important construct when determining a sound audit and control system is to create a structure of accountability. This means that certain factors are considered up front. Accounting is really about accountability, and policies and procedures must clearly lay out what is expected of the implementers. A code of ethics and guidance for acceptable use underpin these efforts.

Duties must be separated, to the extent that a single employee does not have the authority to create an obligation and then conclude that obligation (payment) without proper oversight. Simply put the Purchasing Manager, for example, should not have the ability to pay the bills. The less opportunity employees have to conduct inappropriate activities, the better. Always keep in mind that while risk can be minimized, risk exposure can never be completely eliminated; only controlled to an acceptable level.

CREATION OF A STRATEGIC AUDIT SYSTEM

Companies must establish some form of a cross-functional Audit Committee. The Audit Committee (Committee) is the arbiter and final authority for strategy, budget, supervision, and dispute resolution for the audit function. Members should represent a cross section of the stakeholders and should include executive management. Perhaps the most important obligation of the Committee is to communicate expectations to the company's organization. In the case of a public company, the Committee implements Sarbanes-Oxley compliance. In all cases, the audit committee is responsible for federal and state regulatory compliance and other applicable regulations, such as Visa, MasterCard, and other network rules.

Policies and procedures must be formally documented and must delineate the obligations of the entities within the company; extending clear authority to auditors. The auditors themselves should be required, to the extent possible; to operate openly and in concert with the functions they oversee. Audit plans and checklists should

also be documented and subject to the review of the Committees representative. Results and findings should be reported and made part of the corporate record.

Qualified auditing personnel must understand the functions they are auditing and be sensitive to balancing risk with the business needs of the function they are monitoring. Companies cannot tolerate auditors who "descend after the battle and bayonet the wounded." Careful selection of audit personnel assures that auditors will be seen as helpers and facilitators, rather than kibitzers and checkers.

The broad areas verified by the audit strategy are:

- Internal Controls
- Operational Compliance
- Regulatory Compliance
- Financial Compliance

The Committee must oversee this process and ensure that internal audits and corrective actions add value and do not distract the company from its mission.

AUDIT POLICY IMPLEMENTATION

When formulating an audit strategy a risk assessment is critical to focusing the audit process on areas that will produce the most results. Companies tend to think that risk mostly comes from new technological means, but these new areas are merely additions to the old low-tech devices, including theft of secret correspondence and fake contracts. Areas presenting opportunities for fraud primarily include:

- System Risk**
Which business systems provide the greatest targets for business disruption or fraud? For example, computer systems, firewalls, routers, and all access controls which includes access to sensitive merchant, consumer, and employee data. Both internal and external risks need consideration.
- Financial Risk**
Exists within accounting, cash and revenue control systems, payroll, purchasing, inventory and personnel, etc. This area runs the gamut from simple theft to "ghost employees."
- Physical Risk**
Auditors commonly review building access and visitor policies; however, this area is expanding. Companies must not to overlook the security of their paper files. Are they under lock and key? Is access granted on a need-to-know basis?

A good audit system balances correction and prevention by looking for problems before they occur. This means internal auditors should have visibility into the change management process. Auditors should also be involved in the implementation stage of new projects. This will save you from having to re-implement your good ideas. The right auditors know how to plug holes, so leverage them where you can.

AUDIT PLANNING

- **Schedules** - should be resource loaded and prioritized by risk; whether that risk is System, Financial or Physical.
 - Build as you go. A good rule is to commit about 80% of auditor hours to scheduled activities. This will leave enough flexibility for the audit manager to send staff where needed without jeopardizing required, time dependent reports.
- **Checklists** – should always be used and provide documented evidence that the subject matter was logically derived from the policies and procedures of the area being audited. Checklists should also encompass regulations and accounting standards that are applicable to the subject matter at hand.
 - Build on the past. Audit checklists should be living documents with today's auditor building on the work of past audits.
- **Access** - auditing is no longer strictly a forensic process. Auditors need to have the flexibility and authority to delve into a business process in real time and not necessarily wait until something is "on the schedule". Timeliness can be critical to the quality of review into a suspect area or a complaint follow up.

BUDGETS AND REPORTING

Sufficient financial resources must be devoted to the audit system; however, those resources must be flexible enough not to constrain the effectiveness of the process. A common pitfall is to build an adaptive audit team, only to impose a line item budget that makes the plan difficult to carry out. The Committee should review the budget regularly to ensure appropriate balance between fiduciary management and audit control.

CORRECTIVE ACTION AND DISPUTE RESOLUTION

Overall success depends on implementing and codifying the results of the auditors work within the company's processes. Before finalizing an audit report and findings, the auditor should collaborate with the audited manager:

- Discuss the results with the affected manager
- Draft the report and review it with the manager
- Allow the manager to include comments or interim corrective action with the final report

Only after this is complete should the report be presented to the Committee. If there are still areas where the auditor and the audited manager cannot agree, it is up to the Committee to resolve the dispute.

- ☞ A "no surprises" process like this will promote collaboration and resolve disagreements before they turn into dissention.

BUSINESS PARTNER REVIEW

With the increasing threat of data compromise and government regulation, coupled with the intense growth of new players entering this industry, card brands, networks, and regulators are striving to gain visibility into the Business Partner niche. It is clear that all entities contributing a service along the transaction path need to be identified and “known”. The responsibility to protect the payments space and preserve the integrity of the payments stream belongs to the entire payments community.

- All business partners that engage together in the payments chain must understand the role they play, the value they bring to that process, and the risk introduced by their business.

PERFORMING CREDIT AND BUSINESS DILIGENCE

Be thorough in your diligence. Ensure reviews cover all 11 of the risk categories. While the Business Partner might present a compelling business opportunity, compromising the initial credit/risk diligence cycle in the interest of time could result in a risk event for your company that may have been avoided. The negative impacts could include:

- Loss of revenues, current and/or projected
- Compliance violations
- Fines
- Operational expense around loss containment efforts
- Additional audit and regulatory scrutiny
- Compromised reputation with existing merchants, prospects, and within the industry at large

Consider incorporating a risk mitigation clause within all contracts and service agreements. This clause should cover compliance and security requirements, current and future, and detail your service level agreements and escalation paths. Depending on the structure of the relationship, also consider the business partner’s financial commitment to ongoing compliance and controls.

- ➡ Remember, this partner is now part of your business model and impacts your products, services, and reputation.

REGISTRATION

If you determine this is the right Business Partner for you, review all Card Brand and Network registration requirements. The rules vary based upon the services the Business Partner performs and by individual Card Brand/network.

- Depending on the service provided, registration may be required before transactions should actually flow.

When possible, assign an entity identifier for the Business Partner to use. This may aid you in tracking, reporting, and potentially controlling that Partners interaction with you and your systems.

ONGOING REVIEWS

Set up ongoing processes that not only monitor performance and business health, but allow for cultivation and growth of the relationship.

- Appoint a resource accountable for managing the Business Partner relationship. Don’t just let the Business Partner slip into the daily routine and get lost. You may miss additional opportunities or signs of trouble.

Create a checklist that complements your initial risk assessment points. Include applicable items from the Risk Assessment Worksheet, as well as various relationship checkpoints. These should include activities such as:

- Obtaining regular, verifiable, Service Level reporting
- Receiving copies of audits, as applicable (i.e. PCI, SAS-70, etc)
- Listing Business Partner, as applicable, on any required card brand or regulatory reporting
- Holding periodic strategic discussions to ensure goals remain aligned
- Quantifying the value of the partnership and continually aligning against the risk factors. The proper balance may provide a win-win opportunity for you, your partner, and your merchants.

Overall, the Business Partner Review processes should follow a documented approval path that is stringently adhered to. Any exceptions to processes or policies should be well justified, well documented, and require that the Business Partner be more closely monitored, at least initially.

- ❑ Review your procedures periodically and update them to include internal policy changes, network rule modifications, regulatory considerations and your own experience.
- ❑ Maintain a solid communication channel with the Business Partner.

With a thorough understanding of the Partner’s business you can engage in this new opportunity feeling more confident in your revenue forecasts, your return on investment, your regulatory commitments, and your reputation.

Risk Category	Example
Strategic	Business Partner fits with your strategic product direction, both short and long term. In addition, there are no conflicts in areas such as corporate culture, merchant acquisition, target market, etc.
Credit	All credit requirements are met and appropriate approvals secured.
Market	Ensure that Business Partner’s marketing plan complements your own and that there is clear delineation between “shared/referred” business and any direct business they may also offer.
Systems Operations	Validate appropriate disciplines are in place to monitor system performance, track service results and manage maintenance/updates. Require that you are in the communication loop for any scheduled or unscheduled service interruptions.
Business Operations	Develop appropriate operational controls within the Business Partner’s platform and servicing model. This includes: (1) ensuring that processes for reporting issues, outages, and other service issues are documented; (2) requiring a Service Improvement Plan when service events occur that includes root cause analysis and the implementation of preventative measures, and (3) documenting communication guidelines and procedures for formally advising a merchant of an issue.
Internal Fraud	Review the potential Business Partner’s policies that cover responsibilities for protecting sensitive data and the programs in place to keep staff educated on internal and external threats. Review hiring practices, orientation programs, disciplinary guidelines and the partner’s overall commitment to security.
External Fraud	Evaluate the prospects overall expertise in this area. For example, are they savvy enough to be aware of social engineering fraud schemes? What is their physical security model? If you elect to move forward and engage in business with this partner, it may prove beneficial to include them in your own communication/educational programs.
Reporting	Evidence of appropriate financial reporting and ability to provide ongoing evidence, as required. Understand what requirements apply and maintain a calendar of events to ensure that if the documents are not provided proactively, you know when, and from whom, to request them.
Compliance & Legal	Partner has the appropriate business and technical compliance programs in place to maintain PCI, network, and state/federal regulatory compliance, as applicable. Become knowledgeable regarding the company’s history in this area. Ask for previous compliance violations and litigation history, including steps taken to resolve. In addition, evaluate how the company keeps staff informed of regulatory requirements.
Systemic	Validate sufficient monitoring is in place to validate how service level results are calculated and schedule regular reporting to your company.
Reputation	Be familiar with their business practices internally and in the marketplace. Is there anything within their business model, service level history, data security practices, hiring/personnel policies, media, or current reputation that could put your company at Reputational Risk?

MERCHANT REVIEW

Customers are the life blood of any company looking to succeed. As a Payments Service Provider the ability to obtain and *retain* a merchant is key.

The three main areas to address while constructing the merchant review are:

- Creation of a sound credit policy
- Implementation, adherence and application of the credit policy to merchant reviews
- Ongoing monitoring and review of existing merchants

When establishing the guidelines to be applied to the merchant review, you must begin by creating a credit policy. The credit policy establishes the underwriting standards that will be applied to the review of a prospective merchant. The purpose of the underwriting standard is to ensure that pertinent underwriting information is obtained upon which to base the underwriting decisions. The credit policy should be created in relation to what constitutes an acceptable risk to your company.

CREATION OF A CREDIT POLICY

The creation of a sound credit policy is the first step in utilizing the risk assessment to minimize the liability to your company.

Develop a credit policy that not only provides for adherence to the guidelines it establishes, but also leaves room for flexibility and alternatives. In the development cycle, you must determine the level of acceptable underwriting to be performed on each merchant. This should balance against the duties to be performed with ongoing risk monitoring, which compensates and strengthens your position. Ensure that the development and execution of the credit policy covers all 11 of the risk categories.

- The Risk Assessment Methodology should be applied to both the creation of the underwriting standards as well as the application of those standards when conducting a merchant review. The risk assessment should be applied to your credit policy development. This ensures the identification and mitigation of risk aligns with the acceptability of the risk posed.

CREDIT POLICY IMPLEMENTATION AND COMPLIANCE

Implementing the credit policy for new merchants consists of applying the same risk assessment principals. Following the credit policy, and obtaining and analyzing the application and supporting documentation, determines the risk assessment liability to your company as it relates to that merchant. The underwriting standards and documentation should be used to verify the financial standing of the merchant, their principals, product/service sold, and business practices, in order to make sound business decisions and recommendations for approval. Potential merchants should also possess certain financial, operational and managerial skills.

Underwrite an account based on both the financial strength, which gives a comfort level on the company's stability, and its business and operations procedures and judgments, which give a comfort level on the ability of the company to continue to improve its financial position.

ONGOING MONITORING ASSESSMENT CATEGORIES

Ongoing monitoring and merchant reviews should be conducted on an annual basis to maintain the "know your merchant" aspect, as well as to ensure that the merchant is still processing in accordance with the review that was performed at the start. Additionally, any merchant that has a change to their structure, whether be it ownership, location, business type, product/service, etc should be required to be re-reviewed. This allows for the risk level and liability to be re-evaluated and adjusted, accommodating the merchant and your acceptance of the new liability.

- A merchant is approved with a certain structure (i.e. company name, ownership, type of business, product/service sold, processing limit, average ticket, discount rate, reserve rate, etc). Any changes to the structure need to be known and the account re-written to reflect these changes.

Merchant review processes should follow the credit and risk guidelines established to ensure that the risk assessment is adequately applied to understand the liability and to allow for the appropriate level of handling. This will ensure the liability is managed effectively.

RISK CATEGORY	EXAMPLES CREDIT POLICY CREATION	EXAMPLES CREDIT POLICY IMPLEMENTATION
Strategic	Develop a credit policy that ensures that the practices protect and limit the risk for your business	Application of the developed credit policy ensures the policies and practices protect and limit the risk for your business
Credit	Follow the credit policy and apply it to the merchant review—this limits the risk the merchant poses to your business	Review the merchant’s financials on an appropriate ongoing basis to ensure they continue to have the financial strength to support their business
Market	The credit policy must have established guidelines while allowing for appropriate flexibility, to ensure competitiveness within the industry	Review the competing business types and products/services within the merchant’s industry, which will give an idea of the probability of long term success
Systems Operations	Maintain operational policies to ensure there is no reduction in performance or workflow and that a solid business continuity program exists	Ensure that the merchant has adequate operational policies in place so there is no reduction in performance or workflow to ensure continuation of their business
Business Operations	Unsound credit policies create risk and increase liability and probability of loss	Perform reviews to ensure the merchant has sound policies to minimize risk, liability and the probability of loss
Internal Fraud	A sound credit policy should allow you to identify bad actors that may increase the risk of merchant fraud	Ensure that employees are strictly following guidelines and that all sensitive data is secure
External Fraud	The general spirit of the credit policy should be an appropriate part of the company education program to ensure personnel who participate in this cycle are aware of merchant/application fraud trends, hacking, social engineering, etc	Validate that all systems have security levels to prevent fraud and merchant hacking
Reporting	Accuracy of credit policy reporting feeds directly to all financial reporting	Ensure the merchant has adequate internal reporting requirements
Compliance & Legal	Business and technical compliance programs are in place to maintain PCI, network, and regulatory compliance, as applicable. This ensures you fulfill your responsibility to your new merchant	Ensure the merchant has adequate business and technical compliance programs in place to maintain PCI, network, and regulatory compliance, as applicable
Systemic	System SLAs and reporting align with any commitments made to the merchant	Obtain reporting that substantiates performance
Reputation	Be familiar with merchant business practices internally and in the marketplace. Is there anything within the business model, service level history, data security practices, current reputation that could put your company at Reputational Risk?	Be cognizant of any adverse events that would reflect poorly on the merchant’s businesses reputation

ACQUISITIONS

With the current penetration of the merchant market, some companies are expanding their business by acquiring portfolios. This is accomplished by either purchasing the merchant accounts only, or by purchasing the entire company. With either scenario there are risks involved which should be carefully considered. Obviously, selling an existing business is going to bring a different value than selling a “static pool” of merchant contracts, and with that comes risk.

- The consequences can be severe if portfolio transactions are not valued accurately and transitioned carefully after the purchase.

PURCHASE AGREEMENT DUE DILIGENCE

Be thorough in your diligence. Ensure items in the agreement include:

- Terms for releases from the current processors
- Contractual rights to assign the contracts and /or to move the merchant to the buyer’s platform
- Sponsorship transfer within the Card Brands
- Non-competes from the seller
- Employee contracts
- Lifetime residuals

RISK CATEGORY	EXAMPLE
Strategic	Portfolio fits with your strategic product direction; both short and long term. Can be maintained or easily transitioned to your current processor. There are no conflicts in areas such as corporate culture, service levels, target market, etc.
Credit	Explanation of Grade of paper accepted
Market	Review of solicitation promises (free equipment) supply agreements, etc.
Systems Operations	Your company can support the contractual obligations agreed to in the merchant terms and conditions
Business Operations	Business Operations processes are modified to incorporate the new portfolio
Internal Fraud	Evidence of external audits to ensure card brand and regulatory compliance
External Fraud	Policies have been in place to mitigate external fraud. Controls are migrated as appropriate.
Reporting	Ability to provide you up to date reporting on attrition, losses, and activity
Compliance & Legal	An outside attorney familiar with the business has reviewed the contract in addition to review by an outside auditing firm
Systemic	Service levels are modified to include any new requirements for the portfolio
Reputation	Be familiar with the prospect’s business practices in the marketplace. Is there anything within their business model, service level history, data security practices, current reputation that could put your company at Reputational Risk?

PORTFOLIO REVIEW

Once you determine the contract is in compliance, you need to review the account portfolio. There are certain trending patterns you should look for to determine value and risk. Evaluate as much historical data as possible. This will allow you to identify any anomalies in approval percentages or attrition numbers. In addition to the obvious, you will want to review the “make up” of the portfolio broken out by merchant category as well as volumes and entry methods.

Other risk factors include top-heavy portfolios with a high percentage of large merchants.

- Will losing a few of the largest most-profitable merchants seriously impact the revenue stream?

Review Chargeback history as well as pending / outstanding balances in suspense. This will include any fees, penalties, and or ACH rejects.

Review Card Brand violations including those that impact specific sales representatives, merchants, and the company’s PCI compliance status. Check on the status of any required remediation. Insist that the company provide documented evidence supporting the action taken.

ONGOING REVIEWS

Set-up processes for appropriate ongoing monitoring and review of the portfolio. This should include items such as:

- Attrition during the conversion process
- Actual versus forecasted income numbers when evaluation of purchase was conducted
- Strategic discussions to ensure goals remain aligned

Invest the up front cost. Seek the advice of an investment banker or consultant who has participated in these types of transactions before.

- Minimal risk can be achieved by seeking professional help when purchasing a portfolio.

CONCLUSION

Ensuring the appropriate Risk Assessment methodology is in place, and stays in place, is not always easy. You are facing the demands of growing revenues in an increasingly competitive market while absorbing the escalating cost of compliance and security. Just know that while the information outlined here provides a solid foundation, whatever method you choose to use, implement and manage to it diligently. Dealing with the consequences of not having an established risk assessment methodology will distract you from your business growth plan and most likely be more costly as a reactive measure.

If you chose to adopt all or a portion of what is outlined here, you will find that the premise of your program will align well with industry practices. These categories are well recognized by risk and audit personnel and should help as you maneuver through various reviews that ensure the business you engage in is sound and reliable.

Our industry is embarking on a journey of dramatic change, from the intense level of risk to the extraordinary level of opportunity. If we recognize both and take appropriate action, then we can continue to grow, prosper, and instill confidence in those merchants and consumers who participate in the payments chain.



APPENDIX A - RISK ASSESSMENT WORKSHEET

Category: I. Strategic Risk

Definition: The risk involved with pursuing one business strategy over another. Strategic risk may exist in the products or services offered, the types of merchants or partners with which business is conducted, the adoption of certain policies or practices, the use of certain types of technology or even the markets in which a company expands.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
I.a.1	Moderate	The company has a formal strategic plan and market positioning guide	
I.a.2	Moderate	Company management holds weekly staff meetings with direct reports	
I.a.3	Moderate	Strategic initiatives go before the board of directors	
I.a.4	Moderate	The Product Council develops product strategy based upon industry knowledge	
I.a.5	Moderate	The company is involved in industry organizations, such as board member of Electronic Transactions Association (ETA), to stay abreast of market trends	
I.a.6			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
I.b.1	Strategic plans have been prepared by management and positioning guides have been distributed to all employees		
I.b.2	Management meetings are taking place on a regular basis as evidenced by meeting minutes		
I.b.3	Board meetings are taking place on a regular basis as evidenced by meeting minutes		
I.b.4	Product Council Meetings are taking place on a regular basis as evidenced by meeting minutes		
I.b.5	Other governing bodies such as Enterprise Risk Council or Compliance & Control boards should have appropriate membership and are meeting as outlined in their charter as evidenced by meeting minutes		
I.b.6			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT

RISK ASSESSMENT WORKSHEET



Category: II. Credit Risk

Definition: The risk considered if a party to a payment transaction may be unable to provide the necessary funds for settlement of the payment or transaction.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
II.a.1	Moderate	Underwriting procedures	
II.a.2	Moderate	Collections procedures	
II.a.3	Moderate	Risk monitoring procedures	
II.a.4			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
II.b.1	Internal audit performed of the underwriting processes and found the processes to be operating effectively.		
II.b.2	Internal audit performed of the collections processes and found the processes to be operating effectively.		
II.b.3	Internal audit performed of the merchant monitoring processes and found the processes to be operating effectively.		
II.b.4			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



RISK ASSESSMENT WORKSHEET

Category: III. Market Risk

Definition: The risk that industry market forces, such as competitors, partners, new entrants, technological developments, etc., could adversely affect the company. This includes price erosion, commoditization, and technological disintermediation.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
III.a.1	Moderate	A Product Council is in place to assess technological requirements and prioritize product development.	
III.a.2	Moderate	The Product Management Group researches and analyzes competition and provides information to the Product Council.	
III.a.3	Moderate	Involvement in industry organizations such as ETA results in awareness of market trends.	
III.a.4	Moderate	Employee industry training.	
III.a.5			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
III.b.1	The company has demonstrated the effectiveness of the product council by rolling out new revenue-enhancing products.		
III.b.2	The company has achieved growth in revenues while gaining market share during the past year.		
III.b.3			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT

RISK ASSESSMENT WORKSHEET



Category: IV. Systems Operational Risk

Definition: The risk of systems failure or compromise. This includes transactions being altered or delayed due to an unanticipated incident, event, or problem affecting the systems operations. This could involve changes to payment processor interfaces as dictated by the third-party processors. This also includes natural disasters, software bugs, and unauthorized access to the system.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
IV.a.1	Moderate	Compliance with the Payment Card Industry Data Security Standard (PCI) requirements that establish specific system security requirements.	
IV.a.2	Moderate	A Business Continuity Plan (BCP) is in place that includes a redundant recovery site.	
IV.a.3	Moderate	IT operations policies and procedures are in place over key areas and are reviewed and updated annually.	
IV.a.4	Moderate	Re-certification of payment processor connections occur annually.	
IV.a.5			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
IV.b.1	A Qualified Data Security Company (QDSC) assessed the company's compliance with the PCI requirements.		
IV.b.2	A verified report of compliance (ROC) that has been submitted to Visa.		
IV.b.3	A Business Continuity plan exists and is regularly updated/tested including a remote "hot-site" recovery facility that is available and tested.		
IV.b.4	Operating policies/procedures governing key systems operations areas exist and are updated annually. These policies should be reviewed by the QDSC in conjunction with their PCI assessment and found to be adequate.		
IV.b.5			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



RISK ASSESSMENT WORKSHEET

Category: V. Business Operational Risk

Definition: The risk that a significant policy or procedure doesn't exist, is unclear, inaccurate, outdated, or just as importantly, not enforced. This includes failure to properly follow policies and procedures and the risk that inaccurate information is communicated as a result.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
V.a.1	Low	Documented policies and procedures and documented desk procedures.	
V.a.2	Low	Managers have responsibility to instruct staff on policies and procedures affecting their job and conduct training.	
V.a.3	Low	Mandatory Internal training for employees, managers, and new hires.	
V.a.4	Low	Established employee goal and annual review process in place.	
V.a.5	Low	Physical Access Controls including card key access, security cameras, and visitor access policy.	
V.a.7			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
V.b.1	Process documentation was prepared for Sarbanes Oxley. All team members reviewed and approved the SOX documentation for their respective areas.		
V.b.2	Policies exist for manual processes in IT Operations. These are updated annually and were reviewed by the QDSC in conjunction with their PCI assessment.		
V.b.3	Based upon inquiry and observation the internal training appears to be adequate.		
V.b.4	Based upon inquiry and observation the employee goal making process appears to be effective.		
V.b.5	Based upon observation, the data center sites have adequate physical access controls in place.		
V.b.6			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT

RISK ASSESSMENT WORKSHEET



Category: VI. Internal Fraud Risk

Definition: The risk that an employee, merchant, reseller, or other partner commits fraud against the company. This includes misappropriation of assets (including theft of funds), consumer information or intellectual capital.

Note: Merchant fraud may be considered Internal for risk assessment purposes as merchants are using the service provider's systems to process payments.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
VI.a.1	Moderate	Background checks are performed on all employees and consist of criminal and credit checks.	
VI.a.2	Moderate	Annual ethics training - Corporate Ethics Policy available on the intranet and reviewed and signed as part of new hire process.	
VI.a.3	Moderate	Sensitive credit card data and banking information is masked when viewed in the system and encrypted in the database.	
VI.a.4	Moderate	Every 6 months all employees are required to take Computing Security training and pass a written test.	
VI.a.5	Moderate	Credit underwriting process evaluates merchants.	
VI.a.6			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
VI.b.1	Internal Audit selected a sample of 25 employees and verified that background checks were completed.		
VI.b.2	All employees are required to attend Ethics training.		
VI.b.3	In conjunction with PCI assessment, the company's QDSC reviewed encryption of sensitive data. Sensitive data is encrypted using 128-DES encryption. Access controls to sensitive data and system interfaces exist and are monitored frequently.		
VI.b.4	All employees take the computing security training. HR ensures all employees take and pass the exam.		
VI.b.5	Credit underwriting process was reviewed during SOX testing and was deemed to be effective.		
VI.b.6			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



RISK ASSESSMENT WORKSHEET

Category: VII. External Fraud Risk

Definition: The risk that an unauthorized entity/individual(s) commits fraud against the company or uses the company system to commit fraud. This includes compromised merchant or reseller accounts, theft of card account numbers, bank account numbers, or other sensitive information; extortion, theft of intellectual capital, etc.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
VII.a.1	Moderate	Physical access controls limit access to facilities.	
VII.a.2	Moderate	System Access controls limit access to data.	
VII.a.3	Moderate	Sensitive credit card data and banking information is encrypted and masked.	
VII.a.4	Moderate	All employees are required to take the Computing Security training.	
VII.a.5	Moderate	A limited and highly scrutinized group of employees have access to sensitive information.	
VII.a.6	Moderate	Full time employees are dedicated to external fraud monitoring and prevention processes.	
VII.a.7			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
VII.b.1	Tested by the company's QDSC in conjunction with their PCI assessment of the company. Based upon the most recent assessment the physical and system access controls appear to be operating effectively and cardholder data is properly encrypted using 128-DES encryption.		
VII.b.2	Same as VII.b.1		
VII.b.3	Same as VII.b.1		
VII.b.4	All employees take the computing security quiz twice each year. HR ensures all employees take and pass the exam.		
VII.b.5	Same as VII.b.1		

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT

RISK ASSESSMENT WORKSHEET



Category: VIII. Reporting Risk

Definition: The risk that inaccurate financial and non-financial information is used to make business decisions or is reported to external sources. This includes the financial report risk associated with Sarbanes Oxley.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
VIII.a.1	Moderate	Key financial reporting processes are documented.	
VIII.a.2	Moderate	Key controls are identified and tested.	
VIII.a.3	Moderate	Any gaps noted are reported to management for remediation.	
VIII.a.4	Moderate	Corporate whistle blower hotline is available and published as a detective control.	
VIII.a.5			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
VIII.b.1	Key processes have been documented as part of Sarbanes Oxley 404 Compliance.		
VIII.b.2	Key controls have been identified and tested. Gaps identified in testing have been communicated to management.		
VIII.b.3	Key controls have been identified and tested. Gaps identified in testing have been communicated to management.		
VIII.b.4	Ethics training and Sarbanes Oxley training were conducted during the year.		
VIII.b.5			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



RISK ASSESSMENT WORKSHEET

Category: IX. Compliance and Legal Risk

Definition: The risk that the company, or an affiliated third party (for example, a processor, bank, merchant or reseller), involved with a payment system does not comply with statutory or regulatory requirements resulting in discontinuance of operations, losses or fines to the company, affiliated third parties, or to merchants.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
IX.a.1	Moderate	Compliance and Risk Management Group has identified key areas of compliance and meets weekly.	
IX.a.2	Moderate	In-house legal reviews significant contracts and consults with management on issues.	
IX.a.3	Moderate	All employees are required to take the Computing Security training to instruct employees on PCI and other key rules and regulations.	
IX.a.4	Moderate	Sarbanes Oxley Training done annually.	
IX.a.5	Moderate	PCI training	
IX.a.6			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
IX.b.1	The risk and compliance group has developed a risk assessment process to identify the summary risks noted here as well as to understand the specific risks within the 11 different risk categories.		
IX.b.2	Based upon observation and inquiry, issues are being properly escalated to legal counsel.		
IX.b.3	Employees completed computer security training twice during year.		
IX.b.4	Employees have received compliance training on Sarbanes Oxley, and PCI compliance. The company's QDSC confirmed company satisfied PCI requirements during their most recent assessment.		
IX.b.5	PCI training conducted/verified.		
IX.b.6			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT

RISK ASSESSMENT WORKSHEET



Category: X. Systemic Risk

Definition: The risk that another entity in the processing chain fails, is shut down, or terminates business relationships resulting in the inability of the company to process transactions. Examples include regulatory failure, system failure, data security compromise or other market-related factors.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
X.a.1	High	All parties involved in the payment processing network are required to comply with PCI standards.	
X.a.2	High	The company has contracts with key third parties who are required to comply with industry standard rules and regulations.	
X.a.3	High	Diversified partnerships exists to mitigate risk of single point of failure (e.g., multiple processors)	
X.a.4			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
X.b.1	The company relies on card issuer credit card systems as well as Visa's list of PCI compliant service providers. The company's key partners appear to be in compliance with the PCI standard. Adequate controls exist to monitor compliance of third parties.		
X.b.2	Same as X.b.1		
X.b.3	Same as X.b.1		
X.b.4			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



RISK ASSESSMENT WORKSHEET

Category: XI. Reputational Risk

Definition: The risk of adverse publicity and the possible resulting loss of business from an incident event or problem within the payments industry or within the company directly.

- *The loss of business confidence from an incident may, in many cases, far exceed the direct financial loss or other damage incurred.*
- Note: All other risks, individually or combined, could lead to Reputational Risk.

Assessment Controls:

Ref#	Risk Indicator ¹	Assessment Criteria	Comments/Notes
Xa.1	High	Company policies and procedures	
XI.a.2	High	Consumer and partner education	
XI.a.3	High	Employee training	
XI.a.4	High	Legal team handles issues and reviews contracts.	
XI.a.5	High	PR team handles correspondence with media.	
XI.a.6			

Control Effectiveness:

Ref#	Effectiveness Criteria	Comments/Notes	Assessment ²
XI.b.1	Policies and procedures exist to deal with unexpected and adverse incidents.		
XI.b.2	Consumers and business partners are advised how to report potential adverse incidents.		
XI.b.3	Employees throughout the company’s organization understand what should be done, and who should be contacted in the event of a potential adverse incident.		
XI.b.4	Policies and procedures include representative from legal in responding to potential adverse incident.		
XI.b.5	Policies and procedures include representative from PR team in responding to potential adverse incident		
XI.b.6			

¹ Risk Indicator: HIGH, MODERATE, LOW

² Assessment: STRONG, ADEQUATE, WEAK, INSUFFICIENT



Electronic Transactions Association
1101 16th Street, N.W.
Suite 402
Washington, DC 20036
(202) 828-2635
(800) 695-5509 Toll-free
(202) 828-2639 Fax