



Onformonics™

Know your risks? Protect your data!

ProAudit®

Qualified Security Assessor Solution

Features & Benefits

Brief

| | |
|----------------|---|
| Document Name: | ProAudit Features & Benefits Brief v1.4 WEB |
| Distribution: | QSA Community |
| Sales Region: | Web |
| Version: | 1.4 |



Know your risks?
Protect your data!



Table of contents

| | |
|--|---|
| Introduction | 3 |
| Assessor Challenges | 3 |
| Increased competition | 3 |
| Increased assessment & reporting scrutiny..... | 4 |
| Increased responsibility and liability..... | 4 |
| Lower margins - commoditised market | 4 |
| A trend toward unified compliance | 4 |
| Spreadsheets don't cut it..... | 4 |
| Our Solution | 5 |
| Features and Benefits | 5 |
| Evidence Collection | 5 |
| Workflow and program management | 5 |
| Reporting | 5 |
| Quality Assurance | 5 |
| Flexibility | 5 |
| Off-line Capability | 6 |
| Security | 6 |
| Reduced costs | 6 |
| RoC Module..... | 6 |
| Value Add Throughout All Stages | 6 |
| Value Add for Your Customers..... | 8 |
| Key Benefits | 8 |
| Conclusion..... | 8 |

© Onformonics Ltd 2011. All rights reserved.
Mount Carmel House, Firhouse Road, Dublin 24.
Registered in Ireland company number 45503.

Trademarks: The Onformonics name and logos and all other names, logos, and slogans identifying Onformonics' products and services are trademarks and service marks or registered trademarks and service marks of Onformonics Ltd or its affiliates in Ireland and/or other countries.



Introduction

Onformonics is an established provider of compliance, risk and audit management solutions with a specific focus and experience in the card payments industry. Since 2008 Onformonics has been providing innovative and flexible web based solutions to Qualified Security Assessors (QSAs). These solutions provide benefits such as:

- **Reduced operational costs**
- **Increased productivity**
- **Improved quality assurance capabilities**
- **Centralised audit management**
- **White label portal integration**
- **Enhanced services to your clients**

By leveraging our industry experience we have created a unique set of tools which are tailor made to meet the challenges that QSAs face today. This in-house expert knowledge is further confirmed by the fact that both Visa Europe and Visa International have exclusively used Onformonics experts to deliver over ten, two full day training courses on PCI DSS to an audience of acquirers, issuers and large merchants.

Assessor Challenges

As with most businesses you maybe experiencing increased pressure on your cost base as well as new challenges associated with operating in a maturing market where PCI DSS services are becoming increasingly commoditized. Onformonics has identified the following key challenges that may affect QSAs.

- **Increased competition**
- **Increased assessment and reporting scrutiny**
- **Increased responsibility**
- **Lower margins and commoditisation**
- **A trend towards unified compliance**

Increased competition

The number of certified QSAs has grown from 12 in 2005 to over 250 in 2011. Additionally the number of companies offering PCI DSS compliance related services such as remediation and project management is also growing, with many ICT companies adding PCI DSS compliance services as part of their existing service offerings.

Audited organizations are also becoming competent in managing their compliance requirements and in the current economic climate have acquired an appetite for reducing the cost of compliance in conjunction with increasing the business value. Therefore only providing an annual audit service may not be enough to ensure adequate customer retention.

Increased assessment & reporting scrutiny

The PCI SSC Quality Assurance program which was launched at the end of 2008 and took effect in Q2 of 2009 requires QSAs to increase the level of scrutiny, evidence collection and detailed findings during the assessment process. This has resulted in the significant increase in the level of detail required in the formal 'Reports on Compliance' (RoC).

Failure to adequately validate and provide the necessary level of detail within the RoCs can lead to a QSA company being warned, placed into remediation status or ultimately have their QSA status withdrawn. The PCI SSC publishes a full list of all QSA companies in which they highlight in red QSAs in remediation, making it clear that such companies have not met the required level of work quality. The impact of being placed into remediation may include loss of reputation, customer trust and ultimately loss of business and revenue.

Increased responsibility

In the past Payment Brands made a final decision on the compliance status of an organization based on an internal review of the submitted RoC. This process has been changed and except in extraordinary cases Payment Brands no longer review submitted RoCs which place more responsibility on you to pass a judgment regarding the compliance status of your clients.

Lower margins - commoditised market

An increasingly competitive market requires that you must ensure that you are taking advantage of new technologies and streamlined practices which keep the underlying costs of providing a compliance service efficient. Consultants' remuneration, travel and administrative costs have remained relatively fixed while the overall cost of a PCI DSS compliance service has dropped, putting pressure on margins. Lastly, increased levels of internal knowledge coupled with compliance maturity (and ISA certification for Merchants) within your clients organisation may result in less of a reliance on you to conduct pre-assessments, gap analysis exercises or remediation projects which have traditionally been part of a your revenue stream.

A trend toward unified compliance

As the demands on companies to be compliant with a growing number of standards increase, so do the resources and costs required to meet these demands. Many organizations are also seeking a way of unifying their compliance efforts by integrating them into a larger GRC program to ultimately reducing cost. QSAs who only offer PCI DSS assessment services in isolation of these other demands and without the added value of helping their customers achieve cost savings across multiple compliance standards may face challenges in retaining customers.

Spreadsheets don't cut it

You maybe are realizing that using spread sheets or in-house developed solutions that are no longer suitable for purpose due the increasing complexity of the compliance process and the inherent low visibility of such tools. This is also compounded with the increased regulatory oversight and the need to comply on an ongoing basis against a rising number of compliance standards which are continually growing in complexity and level of detail.

Onformonics ProAudit solution is a comprehensive audit execution tool, specifically designed to assist you realize the full benefit of assessment opportunities by providing an end-to-end management of the assessment lifecycle as it relates to a PCI or an ISO 27000 compliance program.



Our Solution

Features and Benefits

To address the challenges detailed in the previous section, Onformonics have developed an innovative and flexible web based compliance, risk and audit management solution which delivers real value to you.

Evidence Collection

The centralised collection and retention of compliance evidence is a key feature in our solution which allows your clients to provide you with information about their environment, internal departmental structures, system components and distribution of compliance responsibilities internally. Costs can be reduced if you can incentivise your clients to populate the required evidence for compliance including but not limited to policies, procedures, diagrams, configuration standards, screen shots, log files, vulnerability scans, system components and interviewees. Along with the storage of audit notes, this feature assists in meeting the PCI SSC requirement to retain evidence data for three years.

Workflow and program management

Managing a compliance program and ensuring the uniform consistency of security controls across an organisation can be a real challenge. Our solution provides workflow and program management functionality which can help your clients to implement an effective compliance program. By using the solution an assessor can assist a compliance manager in translating controls and requirements into granular, bite size tasks and assigning them to relevant individuals or departments. The functionality to centrally track progress against multiple attributes means that standard project management processes can be employed to ensure that compliance is an ongoing process. The ability to measure risk, cost and time of each individual task enables audited entities to intelligently prioritise the execution of remediation or maintenance activities.

Reporting

Our solution takes much of the pain out of creating the formal RoC as well as intermediate Gap/Remediation reports. Assessors can export a full RoC report in Microsoft Word format based your company branded template. This reduces much of the post audit administrative work that an auditor typically does at present.

Graphical, executive level dashboard reports enable the assessor to present the audited entity's managers with a variety of reports, presenting consolidated statistics of various program attributes such as time, effort, cost, risk, etc.

Quality Assurance

Our solution provides features that allow you to ensure that you are complying with the PCI SSC Quality Assurance guidelines v2.0 and that a RoC contains the required information and level of detail. This is achieved through the support of role based access model which supports among others an auditor, auditor manager and QA analyst profiles. ProAudit provides complete visibility into the assessor's quality of work by enabling the QA analyst role to score assessor performance against the PCI SSC QA Matrix.

Flexibility

Our solution is web based and supports multi-user interaction, providing a team of assessor's simultaneous access to all relevant information regardless of their location. This functionality enables multiple assessors to



work together on a single project or to flexibly reassign auditor resources between multiple compliance projects.

Off-line Capability

To operate properly web based applications requires the availability of a reliable Internet connection. That is not always the case at the locations where assessors perform their duties. To continue providing audit execution benefits in off-line scenario's ProAudit enables road warriors to check-out a specifically structured document, populate it off-line with comments, notes, evidence, etc. and check it back-in once connectivity is made available.

Security

We have ensured that our solutions meet and exceed the security requirements in the Data Security Standard. A full audit history is maintained which provides the ability to track all user interaction from log-in through to comments, statements, status changes, document management, etc.

Our internal software development methodologies include security throughout the lifecycle from design to test and each release of our application is externally assessed by experienced web application vulnerability assessors to the CREST standard (<http://www.crest-approved.org/>).

Our solution also has enhanced security features such as input and output white-listing, dynamic session IDs, dynamic global identifiers (GIDs) and anti-virus sweeping of uploaded files, all of which seek to reduce the attack surface of the application.

Support of leading 2-factor authentication solutions and Active Directory provides the ability to integrate the solutions into the organisation's existing, central user account management system.

Browser activation and IP address access control lists along with customisable password and account lockout settings enable security administrators to finely tune the balance between risk and security according to the organisation's risk appetite.

Reduced costs

Our solution provides features which empower you to assist your clients in managing their compliance program while reducing the overall cost to you of up to 25% in delivering your assessment services.

RoC Module

Value Add Throughout All Stages

ProAudit has been designed to support an assessor's activities throughout all 5 compliance lifecycle stages as they relate to the assessment activities. Furthermore it can be introduced during any of the 5 stages, as it brings unique benefits for the auditor throughout each one:

1. Gap Analysis

- ProAudit can be populated during or following the Gap analysis with all relevant qualitative or quantitative findings along with **detailed recommendations** against each control, testing procedure or validation requirement so that the organization can ensure **appropriate coverage** and **comprehensive plan** for all remedial actions.

2. Remediation

- ProAudit can be used to communicate and assign suggested remedial activities to your clients as well capturing evidence and reports of remediation activities. This workflow system facilitates the review of these responses remotely, removing the need to be always onsite to interact with the client and further more can be reviewed before the start of an assessment. This enables the assessor to accept or reject these activities with the possibility to offer further clarification or remediation steps, ensuring that the client is fully prepared prior to beginning the assessment process.
 - Remedial actions and evidence which can be assessed remotely through ProAudit enable you to allocate and manage your assessor resources in a more flexibly way.
3. The Evidence Repository can assist the assessor and client to correctly scope the entire cardholder data environment and reduces the work normally taken on by the assessor to populate relevant evidence of compliance and link it to the requirement compliance.
- 4. Assessment**
- For those already using ProAudit, the tool provides a mechanism for sharing collected evidence with the assessor ahead of the audit.
 - For those new to the tool and intending to use ProAudit from the point of assessment forward, the tool provides validation workflows which streamline the assessment process.
 - The use of pre-defined compliance statement templates brings in the following benefits:
 1. A baseline that provides an approved structure for a full compliance statement.
 2. Time saving composing compliance statements and comments.
 3. Consistent use of terminology and level of detail in expressed findings, observations and compliance statements among assessors.
 - Additionally for PCI DSS, the tool supports the QA Scoring Guidelines issued by the PCI SSC, which enables the you to verify that all required validation activities have been met and documented.
- 5. Ongoing Maintenance**
- Using ProAudit's Evidence Repository in combination with cyclical tasks can be an effective way to ensure that fresh compliance evidence is supplied throughout the annual lifecycle to demonstrate that compliance is been maintained.
 - The solution can also be used to perform internal mid-term compliance assessments and generate snapshot reports.
6. Renewal Assessment
- Any updates to the content of a compliance standard will be appropriately introduced in the application including relevant migration functionality and Summary of Changes highlighting.
 - Having already completed one assessment using the solution, the compliance manager can utilise the evidence repository to supply the assessor with updated evidence documents.
 - The assessor can use the historic sample records to ensure different systems are sampled.
 - Time can be saved in documenting findings and observations regarding controls or evidence documentation that have remained static or unchanged since the previous assessment.



Value Add for Your Customers

While the solution is packed with features which benefit you, there is a great deal to be said about added value when the solution is used in conjunction your clients. A number of features and functions have been specifically built to facilitate the internal program of work that your clients must manage during the compliance process.

By providing your clients with access to the solution you can deliver significant value add to the your service offering and engagement model. ProAudit provides a structured workflow based **Compliance and Risk Management Solution** which will assist your clients in transitioning their compliance into a structure program that can be measured and tracked. By leveraging the compliance activities it can also provide a platform to implement a risk management program which can be used to meet other regulatory and industry requirements and which will increase the business value of compliance. As a result you can increase customer retention and help you to move away from the more commoditised pure play QSA business and into a one-stop-shop for compliance and risk management services.

Key Benefits

Our solution is an industry leader in the area of compliance and risk management for the card payments industry. Among the key benefits your clients will enjoy are the following:

- The ability to translate a compliance standard into a clearly defined set of measurable actions.
- Adoption of a strategic programme management approach to achieving and maintaining compliance.
- Removing low visibility tools such as spreadsheets, or pen and paper to, manage a complex compliance program and replacing them with a solution built for the purpose.
- Ability to measure and report on current compliance levels or progress towards compliance.
- A single platform allowing multiple users in diverse locations to collaborate simultaneously on the same goal.
- The ability to rapidly execute internal audits, making it practically possible to formally checkpoint the compliance status throughout the compliance life cycle.

Conclusion

The ProAudit solution provides you with the ability execute an assessment while your clients with a complete compliance management solution covering all compliance life cycle stages. This can help increase customer affinity and reduce the cost of service for the assessors while at the same time increase the quality and value of the service. The solution can also assist with maximising the accountability and productivity of each individual assessor by increasing the number of client companies they can service.

For more information email us at sales@onformonics.com, call us on +353-14407576 or visit us at <http://www.onformonics.com>.