

## PCI Compliance Management Portal

### ACHIEVING AND SUSTAINING PCI DSS COMPLIANCE

All merchants must be fully compliant with the PCI DSS, including assessing compliance against 226 requirements and executing approximately one hundred unique security tasks on a daily, weekly, monthly, quarterly, and annual basis. Some examples of these recurring tasks include:

- Daily: Audit log review, Backup media, Anti-virus updates, Physical security access logs, etc.
- Weekly: File integrity monitoring, Firewall management, etc.
- Monthly: Password changes, Patch management, Configuration review, etc
- Quarterly: Internet vulnerability scans, User account review, Firewall rule set review, etc.
- Annual: On-site audit, Penetration test, Policy and procedure review, Third-party contracts, etc.

All too often, organization's either fail self-assessments or audits or spend far more time and money preparing for them than necessary because:

- Unclear expectations are set about what is required
- Required tasks are not performed
- Evidence is not centralized and organized to support the audit process
- Reporting is not available to identify compliance problems on a timely basis

FishNet Security's PCI Compliance Management Portal is an annual subscription service that helps clients properly interpret and apply PCI requirements, assess their compliance status, and then track their compliance status throughout the year. As a result, clients are able to more efficiently and effectively mitigate risk to cardholder data and achieve and maintain compliance.



### SIMPLIFYING COMPLIANCE MANAGEMENT

The PCI Compliance Management Portal is an annual subscription service that helps clients:

- Self-assess their compliance status
- Identify all PCI DSS required compliance tasks as they relate to in-scope IT assets and business processes
- Automate compliance task notifications, tracking, capture and secure storage of compliance evidence, escalation, and management reporting
- Better understand requirements and keep up with changes.

## KEY FEATURES

### Compliance Task Management

FishNet Security's compliance task management functionality enables users to identify PCI-mandated compliance tasks, assign them to users or groups, notify users or groups via e-mail, collect status updates, and generate management reporting. By automating compliance task management, organizations gain efficiencies and reduce the risk of unintentionally falling out of compliance.

### Evidence Capture and Secure Archival

For every requirement and associated compliance task, FishNet Security has identified what compliance evidence should be captured as a default. Recognizing that each organization is different, FishNet Security provides clients with the capability to customize these recommendations to better fit their IT environment and business processes. Compliance evidence can be required for users to complete a task or optional. All evidence is encrypted using two key components, one of which is only stored by the client, significantly increasing security over alternative solutions.

### Automated Self-Assessment Questionnaire

FishNet Security provides an automated, easy-to-use process for completing the PCI DSS Self-Assessment Questionnaire. Organizations can research relevant PCI DSS requirements and associated FishNet Security guidance, answer each question, and generate reports on compliance for internal review and submission to their acquirer. If a deficiency is identified, a remediation task can be created and assigned right away, taking advantage of all the notification and workflow features described in Compliance Task Management above.

### PCI DSS Knowledge Base

FishNet Security's peer reviewed knowledge base provides detailed guidance on each PCI requirement. In addition, it is searchable, enabling users to significantly reduce time spent on compliance administration. For example, users can sort the requirement by role, by test type, by free text search and generate predefined reports.

### News

FishNet Security provides daily news updates on cardholder data related topics such as security incidents, legal cases, card brand updates, new reports and threat trends, etc. A quarterly newsletter provides more in-depth analysis of important legal trends, incidents, and technical compliance topics.

### Program Plan

FishNet Security's program planning template can be used to refine the PCI DSS program management processes. The template covers organization, risk analysis, scoping, internal assessment, remediation, testing, and maintenance.

### Risk Analysis Model

The risk analysis model enables organizations to quantify their annual loss expectancy from a cardholder data breach. Whether the model is used qualitatively or quantitatively, it helps executives size the risk posed by cardholder data.

### Other Resources

FishNet Security maintains links to a variety of helpful resources from the PCI Security Standards Council, the card brands, the FTC, states, etc.

### Inquiries

FishNet Security recognizes that while Portal Resources will answer most compliance questions, some issues require in-depth consultation. Client inquiries are answered by one of FishNet Security's Qualified Security Assessor (QSA). FishNet Security's QSAs are leaders in payments security who provide our clients with practical, real-world guidance, enabling them to get to compliance faster with less resource.



## PCI Compliance Management Portal

### FISHNET SECURITY PCI COMPLIANCE MANAGEMENT PORTAL PROGRAM OPTIONS

FishNet Security offers a suite of services designed for organizations of all sizes.

SERVICE FEATURES	STARTER PACK	BASIC	PREMIER	ENTERPRISE	CUSTOM
<b>Access to FishNet QSA</b>					
# of Inquiries Per Year	2	5	10	15	TBD
<b>Portal Access</b>					
Admin Licenses	2	5	7	15	TBD
Task Management Licenses	5	10	25	50	TBD
<b>Features</b>					
Automated Task Mgmt	X	X	X	X	X
Inquiry Tracking System	X	X	X	X	X
Knowledge Base	X	X	X	X	X
DSS Implementation Guidance	X	X	X	X	X
Guided Self-Assessment Questionnaire	X	X	X	X	X
Financial Risk Analysis Modeling	X	X	X	X	X
DSS Query Interface	X	X	X	X	X
<b>News Bulletins</b>					
Quarterly Newsletters	X	X	X	X	X
Flash Updates	X	X	X	X	X
Analyst Blogs	X	X	X	X	X

## WHY FISHNET SECURITY?

### THE FISHNET APPROACH

Our unique risk-based approach to compliance deploys strategic methods only a risk management firm can offer. FishNet Security is not a 'checklist audit' firm. Instead, our consultants utilize time-tested, adaptable and scalable compliance methodology that starts with a strategic risk management framework and incorporates technology insight to drives out tactical execution plans and action items.

### OUR EXPERIENCE

FishNet Security's history as a dedicated security firm and reputation for client advocacy lends perspective in communicating risk to business leadership, while mapping objectives for meeting technical requirements. Our 11 years of experience in a variety of industry verticals, a broad

clientele base, and matured methodology positions FishNet to pursue risk management in ways audit firms, VARs and integrators simply cannot. Because of our broad clientele base, our understanding of different vertical industries, and our mature methodologies, we are able to report risk information in a way that makes business sense to executives and creates roadmaps for meeting technical compliance requirements.

### ABOUT FISHNET SECURITY

At FishNet Security, our common goal is to be your trusted Information Security solutions provider and advisor. From multi-disciplined compliance auditing and assessment, to training, integrating, and supporting complex multi-vendor enterprise security solutions, Fishnet Security can help with all of your information security services and infrastructure needs.