Comprehensive Audit Support Services

Audit, Compliance & Privacy Services

Audit, Compliance & Privacy Protection Services offers a variety of services designed to help organizations address internal audit, state, federal, and international laws and regulations. Our services specialize in Audit, Compliance & Privacy Planning, Assessments, Awareness Training, and Compliance Programs.

Benefits

Our Compliance & Privacy Protection Services (PCI, SOX, GLBA, ISO 27001/2, FISMA, HIPAA, SCADA, SAS70-1, etc.) can help you address industry and legal requirements.

Our services can benefit your organization in multiple areas:

Mitigating IT Risk

- Aligning regulatory compliance and risk management
- Managing risk on an enterprise basis
- Improving IT governance
- Tightening security and privacy safeguards

Improving Business Performance

- Increasing revenue growth by retaining loyal customers
- Increasing market share by decreasing damaging exposures
- Delivering controls that support high quality customer service
- Maintaining and building upon reputation and brand

Increasing Operational Efficiency [reducing cost and complexity]

- Supporting secure, available and accessible data and applications
- Improving operational efficiency and productivity by reducing the cost and complexity from proliferation of data and applications
- Implementing operational resilience strategies to ensure continuity of business and minimize business disruptions

Comprehensive Audit Support Services

Comprehensive Audit Support Services offers a variety of services designed to help organizations address internal audit, state, federal, and international laws and regulations. Our services provide a structured methodology to ensure that all audit needs are identified and met.

Benefits

Our Comprehensive Audit Support Services (PCI, SOX, GLBA, ISO 27001/2, FISMA, HIPAA, SCADA, SAS70-1, FTC Identify Theft Red Flags, etc.) can help you address industry and legal requirements using a structured methodology.

The following table presents Emagined Security's proposed seven-phase methodology to manage the audit activities:

Phase	Description
1	Audit Preparation
2	Pre-Audit Documentation
3	Audit Management
4	Management Remediation Support
5	Technical Remediation Support
6	Evidence Documentation
7	Post Audit Support

Audit Preparation

While performing Audit Preparation, Emagined Security attends on-site meetings to gather specific audit requirements from client representatives. This is the most critical phase in the overall methodology. It is important to gather as much pertinent data as possible from key personnel to accurately identify audit needs prior to allowing auditors to begin assessing the environment.

Pre-Audit Documentation

While performing Pre-Audit Preparation, Emagined Security will document the design and create necessary support documents. The following are sample documents that may need to be created in preparation of the audit:

Security Policies:

- Statement of Policy on IT Security
- Information Security Policy
- Acceptable Use / User Security Standards
- Data Classification Guides
- Etc.

Compliance Documentation:

- Privacy Compliance Guide
- State and Federal Law and Regulations Compliance Guide
- Etc.

Security Architecture Documentation

- Remote Access Security & Controls
- Mobile Access Security Architecture
- Etc.

Audit Management

While performing Audit Management, Emagined Security will lead the audit on our client's behalf. During this phase, Emagined Security will help establish the scope of the audit with the auditors. This will allow the Emagined Security to govern the allowed access to systems and the infrastructure based upon the pre-defined scope. Emagined Security will work to ensure that all information is presented from the most beneficial perspective in order to pass the audit.

Management Remediation Support

While performing Management Remediation Support, Emagined Security will perform Management Remediation Support. Upon receipt of a draft audit report, Emagined Security identifies any of issues where misunderstandings or representations may exist in the Audit report. This will help to minimize any inappropriate finds where our client may be meeting audit requirements.

Technical Remediation Support

While performing Technical Remediation Support, Emagined Security will perform Technical Remediation Support. Upon receipt of a draft audit report, Emagined Security will provide a technical review of the audit report and assist with the technical remediation activities. Emagined Security will interface with the company management to develop the best approach for remediation activities.

Evidence Documentation

While performing Evidence Documentation, Emagined Security will create necessary documentation needed to close out the audit findings. The following are a sample of document categories that may need to be quickly created in support of audit closure:

- Various Security Policies
- Various Compliance Documentation
- Various Security Architecture Documentation
- Etc.

Post Audit Support

While performing Post Audit Support, Emagined Security will conduct a post-mortem to determine the best approach for future audits. Emagined Security will conduct a post-mortem review of the audit activities to support future reviews. This review is critical to ensure that future audits are conducted in a streamlined and methodical manner. This review can also be used to provide management necessary information that will support budgetary cycles and streamlining operations.