Managed Strategy

Statement of Work

ArmorPoint Managed Strategy Service Scope

DESCRIPTION OF SERVICES

ArmorPoint will conduct a Business Impact Analysis, Risk and Security Assessment of Clients Technology Environment. The assessment will focus on safeguarding Client's information and systems from internal and external threats and vulnerabilities including, but not limited to, procedural, software, hardware, and/or policy. The audit will produce an analysis of Client's infrastructure and policies with a focus on ensuring data security compliance. The findings will enable Client to operate, plan, and secure the infrastructure and applications in accordance with data security standards. ArmorPoint will follow the National Institute of Standards and Technology (NIST) Framework.

PROJECT SCOPE

EXTERNAL SECURITY ASSESSMENT

- The external assessment will be limited to publicly accessible hosts residing in the Client's network segments deemed to be part of the DMZ or Transaction Zones (TZ) that provide shared hosting environments. This includes underlying Network Management and Out of Band zones and segments that provide network communications and services to the publicly accessible hosts.
- Network addresses in scope for this assessment will be provided by Client during project initiation
- ArmorPoint will conduct penetration testing for publicly accessible systems when initial vulnerability scanning identifies potential high impact vulnerabilities.
- In the event penetration testing gains access to a system, further assessment will be performed to determine the ability of the attacker to leverage the system for access to additional systems and networks.
- ArmorPoint will perform a Security Reputation Assessment against public domain/s to assess publicly-available information and data accessible
- ArmorPoint will review firewall and border router configuration for use of security best practices.

INTERNAL SECURITY ASSESSMENT

- ArmorPoint will meet with members of the systems team to understand the overall application architecture, design, and its related development processes.
- ArmorPoint will perform a review of security tools and technology with the objective of understanding in-place controls and identifying technology gaps including Antivirus, Firewall / Intrusion Prevention, Network Monitoring, Encryption, Multi-Factor Authentication, Privileged Access Management, Data-Loss Prevention and Security Information & Event Management.
- Review the application security architecture documentation including cloud services, security controls, and procedure documentation.
- Review email security controls, including encryption and architecture documentation.
- Review wireless security controls, including encryption and architecture documentation.
- Provide vulnerability scan against internal systems using industry standard tools in gathering information specific to vulnerabilities and weaknesses.
- Analyze at a high level the security services of the operating system platform used by the application for security vulnerabilities.

RISK ASSESSMENT

PHASE I – DISCOVERY AND DATA GATHERING

- Review project scope and requirements with Client's business and technology leaders.
- Schedule meetings with the business and technology leaders as well as DR - BCP planning team or stakeholders
- Review critical business processes by interviewing technical and business leaders.
- Prioritize these business processes and document the risk that may impact them, i.e., cybersecurity, natural disaster, backup/technical and resources.
- Document Recovery Time Objective (RTO), Recovery Point Objective (RPO) and Maximum Tolerable Downtime (MTD) expectations and categorize by priority.
- Review Client's current policies for backup, replication, and retention
- Review critical vendors and partners, in-place contracts, and service level agreements
- Review Client's current network architecture and topology, provide gap analysis between Client's current state and industry best practices.
- Gather any existing documentation/diagrams/budgeting
- Review all current documentation for application, systems, services, and applications
- Conduct a review of current systems in production and methods to recover these systems
- Identify and confirm information specific to data classification/prioritization
- Identify risks within the critical business processes, applications, and service

PHASE II DOCUMENT FINDINGS AND RECOMMENDATIONS

- Identify and document current risks within the business and technology environment.
- Complete a Business Impact Analysis identifying and prioritizing critical business processes and applications.
- Document client expectation for protecting critical business processes, applications, and services.
- Review and document gaps in client expectations and current capabilities and controls to protect those business processes.
- Develop final recommendations for mitigating findings and risks from our discovery process.
- Schedule a document review meeting with the appropriate leadership team.

ONGOING CONSULTING, LEADERSHIP AND SUPPORT

- Development of security policies and procedures to close gaps in documentation
- Attendance and representation in board meeting discussions, as needed
- Plan and guide security tabletop exercises
- Represent Client during any audits and/or related activities
- Provide strategic guidance to client on matters related to cybersecurity and risk management
- Hours will be based on the executed order form; If hours are exceeded, additional time will be billable as T&M
- Travel is excluded and would be the responsibility of Client

DELIVERABLES TO BE PROVIDED AS PART OF THIS STATEMENT OF WORK:

- A completed Security Posture Assessment with a full review of the internal and external security posture of the Client's network environment.

- A completed Business Impact Analysis and Risk Assessment identifying critical business processes, in-place controls, and capabilities for protecting these processes.
- Recommendations for improving resiliency for the client's critical business processes.
- A Security and Risk Roadmap including risk ratings, likelihoods and impacts for all critical business processes.
- An executive review with a summarization of findings including a delivery meeting/presentation to review both documents.
- Ongoing strategic consulting sessions.

ITEMS NOT INCLUDED WITHIN THIS STATEMENT OF WORK:

- Implementation of technology services is not included within this Statement of Work.
- Security Remediations are not included.
- Creation of application or network drawings, application dependency mappings, and as-built application, system and network documentation is not included.
- Configuration Assessment of Existing Security Tools is not included.
- Any Managed Services, and Managed Security Services are not included.
- Any Professional Services not stated in this SOW are not included.

CONTRACTUAL CHANGES

Changes are a natural thing and Client is a continuously evolving business. To facilitate the change process, Trapp Technology has designed the following Governance structure:

Change To	Vehicle	Process
Service Scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than $1,000 will require further Executive Approval through A Contract Change process.	CCR
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Client Dashboard / Real Time
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum

Change to the MSA	Each change or group of changes will be reviewed and discussed with each party's legal team until final agreement. No change will be presented for approval that has not met with joint agreement first.	Contract Change

EXCLUSIONS

The following exclusions apply to the scope of the work stated above and have been incorporated as assumptions into the pricing stated below.

- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on premise needs
- Any migration or upgrade of infrastructure (servers, network, etc.)
- Any actual implementation of the recommendations made by Trapp Technology unless specified in this document
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus
- Any work related to being crypto-locked. Trapp Technology will work to mitigate the spread by blocking at the edge and/or taking machines offline
- Any data recovery and forensics work due to purposeful or malicious client or application errors
- Any software license or physical hardware expenses
- Any software license that's not explicitly mentioned, and not covered by Trapp Technology
- All Travel and lodging costs.
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Client Change Request ("CCR").

MISCELLANEOUS

This Agreement and all corresponding schedules, quotes, exhibits, the Terms of Service, and/or Change Orders comprises the entire agreement between the parties and replaces any oral or written agreements between ArmorPoint and Client.

APPROVAL AND AUTHORIZATION

This Agreement shall be binding and effective as of the date upon which both Parties being fully authorized have signed. This Agreement may be executed simultaneously in one or more counterparts, each of which shall constitute one and the same instrument.

ARMORPOINT

(Name)	(Title)
(Signature)	(Date)

CLIENT NAME

(Name)	(Title)
(Signature)	(Date)