Master Plan

Risk Intelligence and Countermeasures (RIC)

[DATE]

Prepared For:
[CLIENT NAME]
[CLIENT ADDRESS]
CLIENT ADDRESS]

Prepared By:
SupportMax

CHALLENGE

[CLIENT NAME] faces significant financial, legal, and reputational risks from diverse threats—including cyberattacks, social engineering, and misuse of digital assets. **[CLIENT NAME]** must effectively and efficiently mitigate these risks to protect both its present operations and its prospects for future growth.

SOLUTION

[CLIENT NAME] will comprehensively address threats posing the greatest risk to **[CLIENT NAME].** using technologies, services, processes, and policies proven to provide proactive protection from threats, discover and remediate vulnerabilities, and enable continuous improvement of **[CLIENT NAME]'s** governance, risk, and compliance (GRC)—while minimizing impact on its financial and human resources.

MASTER PLAN STRUCTURE

The Risk Intelligence and Countermeasures (RIC) Master Plan for **[CLIENT NAME]** presented here has five (5) primary components:

- **Great Start**
- **Secure IT Foundation**
- **Advanced Security 2023**
- **Compliance-as-a-Service (CaaS)**
- **vCSO**

SupportMax also strongly advises **[CLIENT NAME]** to utilize an independent third-party cybersecurity assessment service as an integral sixth component of its RIC Master Plan.

Great Start

Great Start™ initiates the RIC Master Plan launch by using the results of an independent third-party cybersecurity assessment to uncover and remediate deficiencies in **[CLIENT NAME], Inc.'s** environment.

DELIVERABLE	OUTCOME
CVE discovery and remediation	Updates security-related patches based on published common vulnerabilities and exposures (CVEs)
Privileged account review	Finds and fixes critical issues that could compromise administrative access to critical systems
PII scan	Addresses issues that may put personally identifiable information (PII) at risk
Roles and responsibilities	Clearly defines appropriate contacts at both [Prospect Name] and [MSP Name]
Communications and workflow	Sets guidelines and expectations for response times, incident reporting, trouble-ticket escalation, etc.

GREAT START™ BENEFITS

- Launch RIC Master Plan with healthy, stabilized computing environment
- Prevent confusion, chaos, and stress during initial RIC rollout
- Direct rapid mitigation of highest-risk vulnerabilities

Secure IT Foundation

Secure IT Foundation fulfills **[CLIENT NAME]'s** fundamental requirements for secure, reliable digital operations by providing a core set of ongoing IT management services.

DELIVERABLE	RESULT
Endpoint maintenance	Keeps systems running optimally and properly patched with security updates - includes warranty management
Endpoint detection and response (EDR)	Detects, identifies, and isolates common threats to endpoints devices—including viruses and malware
Microsoft 365 management	Administration of user accounts, standard SharePoint configuration, and data backup up to 200GB
Cloud backup	Hourly backups off-premises with rapid restoration capabilities that are periodically tested/validated
IT support hotline	Skilled technical support including remote assistance within response-time SLA parameters

SECURE IT FOUNDATION BENEFITS

- Provides optimal productivity all day, every day
- Reduces exposure to technology-related risks
- Protects against extended business interruption and/or data loss
- Reaps higher technology return-on-investment (ROI)
- Offloads non-strategic IT-related work

*Note: Secure IT Foundation does not include support for **[CLIENT NAME]**'s business applications—which include [list excluded applications]. **[CLIENT NAME]** will continue to utilize the technical support provided by those software vendors directly. However, in situations where a business application issue may involve [Prospect Name]'s IT infrastructure, **[MSP NAME]** will collaborate with those vendors to help resolve the issue.*

Advanced Security 2023

Advanced Security 2023 provides **[CLIENT NAME]** with the ongoing enterprise-caliber cyber defense that every organization needs to protect itself against the ever-escalating volume of attacks being perpetrated by relentlessly inventive hackers, malicious state actors, and cybercriminals who can now inexpensively resource ransomware, reputational blackmail, and other exploits via open markets on the dark web.

DELIVERABLE	RESULT
Extended Detection and response (XDR)	Complements endpoint protections with 24x7 coverage of networks, cloud, and other IT infrastructure
Microsoft 365 hardening	Adds anti-phishing intelligence, removal of insecure legacy protocols, detection of forged sender IDs, etc.
Password management vault	Facilitates best practices: password encryption, strong passwords, password generation, frequent password changes, off-device password storage, etc.
Advanced firewall controls	Detection and alerts for suspicious traffic, proactive blocking of known malicious websites/hosts, etc.
Dark Web vigilance	Monitors criminal marketplaces for PII, user account passwords, exfiltrated data, etc.
Zero-trust application whitelisting	Blocks installation of unauthorized software to prevent both malicious and unintentionally harmful user behavior

ADVANCED SECURITY 2023 BENEFITS

- Reduces financial, operational, and reputational risk significantly
- Minimizes window of opportunity for attackers who penetrate perimeter defenses
- Enhances defense against insider threats
- Protect customers, supply chains, partners, and others more effectively
- Fulfills requirements for superior cyber insurance coverage
- Makes security best practices easier for employees

Compliance-as-a-Service (CaaS)

Compliance-as-a-Service (CaaS) enables **[CLIENT NAME].** to achieve and maintain compliance with the growing range of increasingly complex and wide-ranging operational requirements mandated by government agencies, industry certification authorities, and others.

DELIVERABLE	RESULT
Customized controls framework	Provides foundation for implementing 218 key controls required to support Top 20 regulatory mandates
Plain-language policy templates	Customizable documents designed to fulfill requirements in a way that's easy for everyone to understand
Workflow/approval tracking	Records approval process to document what, when, who, and why policies have been implemented
Employee attestation	Tracks/reminds employees to accept relevant policies and provides evidence of required employee attestations
One-button reporting	Quickly generates required evidence/documentation of compliance for external auditors and internal reporting
Security training content	Provides required compliance-related cyber/physical security education for all employees and IT administrators
Update management	Prompts for required changes when new mandates are issued and provides version control/validation

COMPLIANCE-AS-A-SERVICE (CaaS) BENEFITS

- Dramatically reduce the burden of complying with expanding mandates
- Avoid fines, Code of Conduct, and other penalties
- Proof of due diligence and best efforts mitigates penalties even in the event of a violation
- Keep compliance current
- Qualify for superior cyber insurance coverage
- Improve on-boarding of new employees

vCSO

vCSO enables **[CLIENT NAME]** to reap the benefits of having a Chief Security Officer while avoiding the costs and risks associated with executive search, recruitment, compensation, retention, and turnover. These are especially significant given the extreme global shortage of experienced, qualified cybersecurity professionals at this level.

DELIVERABLE	RESULT
Executive oversight	Unified command-and-control of critical security, compliance, and related RIC functions
Transformational leadership	Elevates efforts from operational/tactical to instill a true organizational culture of security and compliance
Risk-driven prioritization	Helps ensure that resources are allocated to the most important/pressing compliance first
C-level strategy and roadmapping	Enables upper management and board to make strategic fact-based decisions about risk appetite, risk/reward, etc.
Management perspective/collaboration	Go-to resource for managers who need to factor expert insights about threat and risks into their decision-making

vCSO BENEFITS

- Essential business advantages of a CSO without the costs of a CSO
- Proactive, strategic approach to mitigating organizational risk
- Security and compliance integrated into executive-level decision-making
- Maximum value from internal and external resources
- Improved insurability profile
- High-impact item checked off on audit/regulatory scorecard

Independent Third-Party Assessment

[MSP NAME] strongly recommends that **[CLIENT NAME].** utilize an independent third-party cybersecurity assessment service in conjunction with this Risk Intelligence and Countermeasures (RIC) Master Plan. Our preferred assessment service is CyberWatch™ from Galactic Advisors*.*

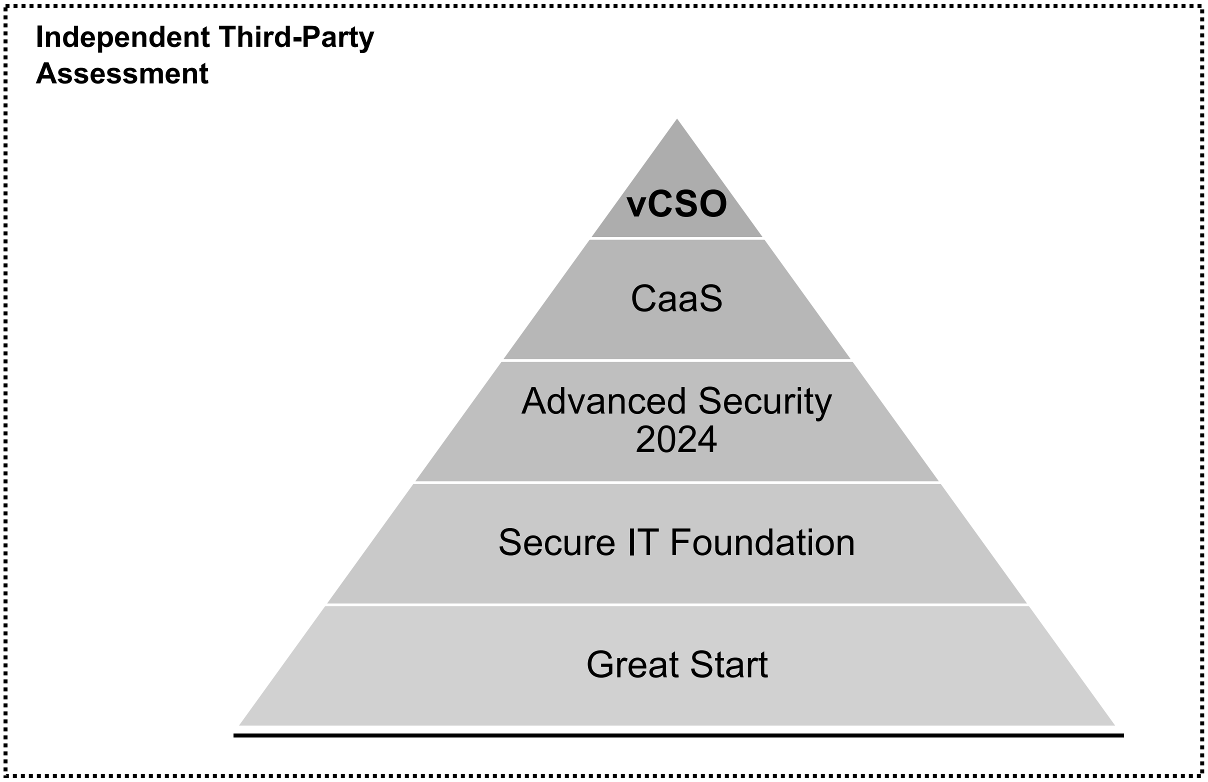
DELIVERABLE	RESULT
CyberWatch™ penetration test	Tests cyber defenses by performing emulated hacker attacks via external vectors and/or as a malicious insider
CyberWatch™ vulnerability analysis	Thorough inspection of digital environment to detect shortcomings in settings, configurations, and policies
CyberWatch™ CVE analysis	Detects failures to apply software patches and updates that are necessary to prevent known exploits
CyberWatch™ PII analysis	Scans for unencrypted personally identifiable information (PII) that poses security and/or compliance risk
CyberWatch™ user hygiene analysis	Looks for indicators of problematic user behaviors such as weak passwords, website cookies, stored tokens, etc.
CyberWatch™ digital health report	Provides detailed, itemized documentation of discovered issues along with checklist of suggested remediations

THIRD-PARTY ASSESSMENT BENEFITS

- High-value diagnosis of current security posture
- High-value guidance for Great Start™ execution provided by initial assessment
- Periodic assessments measure RIC Master Plan performance/progress over time
- Objective third-party audit is a plus for regulators, insurers, customers, and others

RIC Master Plan for [Prospect Name]

Support Max



Thank you for the opportunity to submit this proposal for a Risk Intelligence and Countermeasures Master Plan. **[MSP NAME]** is committed to helping **[CLIENT NAME]** continue growing and evolving safely and successfully in an increasingly digital-centric world that constantly presents our clients with new opportunities and new dangers. We believe that this Master Plan offers [Prospect Name] the optimal approach to managing its digital risk going forward in terms of both effectiveness and value. Please do not hesitate to reach out to us if you have any questions at all about the material presented in this proposal.

Submitted by:

____ _________________

[Name] Date