INTRODUCTION AND PURPOSE

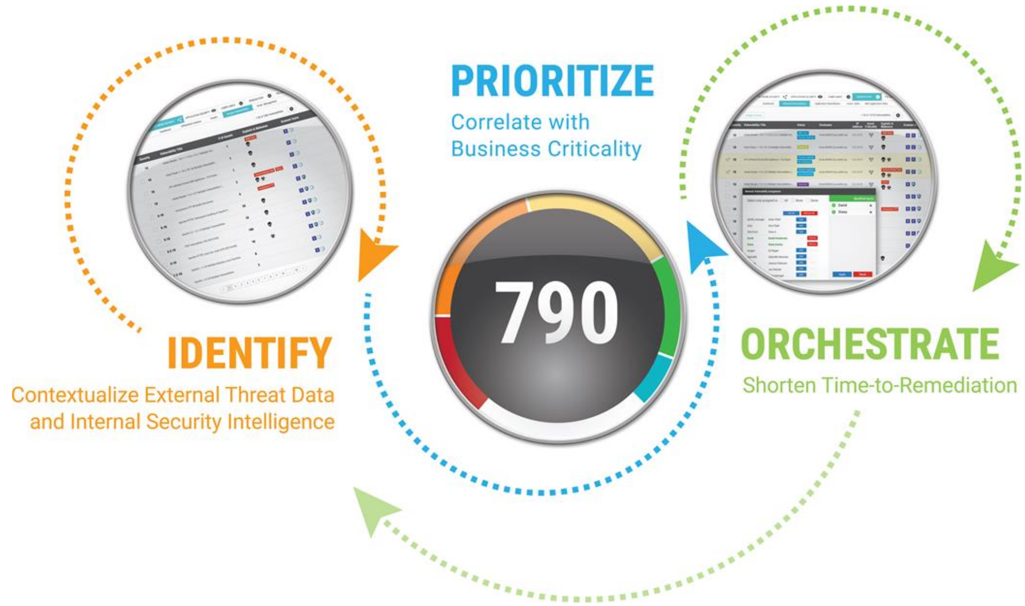
RiskSense is a national leader in Cyber Risk Management; the management of cyber threats with a data-driven, threat-centric, and intelligence-based approach that allows organizations to become more proactive using the predictive prioritization of risk.

The focus of this document is to help organizations assess their current level of cyber security threat management and prioritization, not simply at an IT level, but at an enterprise management level. The operational assumption is that all organizations are in the ongoing process of evaluating the use of resources and budget to address the accelerating cyber threat environment.

The purpose of this ***Cyber Risk Management Assessment and Analysis Tool*** is to provide a means of determining organizational need for development of a higher level of cyber risk management.

1. OVERVIEW

The objective of this assessment tool is to enable an effective and thorough self-assessment and collaborative discovery process concerning the current state of your organization's cyber security posture. The focus of the questions is to help uncover unrealized and/or emerging gaps in your organization's current and future level cyber risk management. The questions are centered on the common elements of organizational and operational models including People, Platforms, Processes and Performance. These "4 Ps" offer a useful way to consider the current state of your organizations cyber security posture and how you can move to a cyber risk management approach.


PRIORITIZE
Correlate with
Business Criticality
790
IDENTIFY
Contextualize External Threat Data
and Internal Security Intelligence
ORCHESTRATE
Shorten Time-to-Remediation

2. CURRENT STATE/PEOPLE

A. Who in your organization is responsible for managing (?) cyber risk?	
B. Who will ultimately be held accountable in the face of a cyber-attack that jeopardizes your customers' trust and your brand?	
C. How well aligned do you feel your current skill/capability levels are with your current and future cyber risk exposure?	
D. What areas of performance do you feel could be enhanced or gap needs to be addressed? - Management of all threats? - Prioritization? - Threat intelligence? - Remediation management?	
E. Expertise: With the expansion of your operational IT footprint (e.g. web, wireless networks and applications, IoT, etc.) do you have enough of the right people to keep up with the expanding attack surface?	
F. As the scale, scope and sophistication of the cyber threat landscape advances, how will you recruit and retain the people with the skill sets and experience to keep pace?	
G. Do you see recruitment and retention of qualified cybersecurity professionals as a challenge for your organization? Why?	
H. How will you keep them up to date with the new skills and tools required by a far more challenging cyber threat environment?	
I. In the event of a cyberattack, who comprises your "Crisis Response Team" and do they have the availability without compromising their day-to-day responsibilities - and do they have the skills and experience - to handle the potential size and scope of the impact to your organization?	

3. CURRENT STATE/PLATFORMS

“Platforms” refers to the physical, virtual, internal and external resources that are available for addressing the cyber security risks. The core platform is the IT infrastructure which refers to all the IT components; desktops, laptops, tablets, mobile phones, routers, printers, retail networks, consumer facing websites, applications, etc. (everything with an IP address). Often called the “Attack Surface”.

A. Has your organization created an inventory of your IT assets? What do you include in the definition of assets/ How often is this updated? How has your organization mapped your enterprise attack surface?	
B. Has your organization mapped your attack surface?	
C. How does your organization or another agency conduct external threat analysis? If so, how up to date is it (e.g. do you subscribe to commercial threat feeds such as iSIGHT, Verisign iDefense, CrowdStrike, etc.)?	
D. How do you know whether the threat analysis is fully comprehensive and complete?	
E. What is the coverage area for your vulnerability scans (i.e. sampling, 100% coverage, etc.)?	
F. What is your strategy for scaling up your cyber risk management strategies and resources in a cost-effective manner?	
G. With the expansion of your operational IT footprint (e.g. web, wireless networks and applications, IoT, etc.) how do you confirm that you have the right tools to prioritize the remediation of the expanding attack surface?	
H. How is your organization using current scanner technologies (e.g., Qualys, Nexpose, Nessus Network Security, IBM, HP, Intel Security) and what level does this go to (Web Apps, Databases, Gaming Operating System, etc.)?	
I. Do you use dual scanners to gain the better view of the data/as a cross-check?	

4. CURRENT STATE/PROCESSES

A. Do you have a Cyber Risk Mitigation Plan?	
B. What is your process for evaluating and prioritizing all your risks across all your IT assets?	
C. What threats do you consider the most serious and what criteria is used to make those judgments?	
D. Does your criterion include "threat-centric" or "business criticality" based factors?	
E. How does your organization categorize or prioritize remediation actions (e.g., by the database of Common Vulnerabilities Exposures (CVE), business criticality, or risk)?	
F. How are cyber risk issues escalated?	
G. How do you handle remediation "ticket management" (e.g. Excel spreadsheets, email, or is it automated)?	
H. How does your organization track the outcome of an action that the Security Operations team initiated or the status of an action plan?	
I. Who determines the overall organizational cyber risk level? How is this used to communicate to the board, commission, management (e.g. Governor/CEO)?	

5. CURRENT STATE/PERFORMANCE

A. How does your organization benchmark your performance in terms of managing cyber security risk? What is the standard of performance you deem applicable?	
B. How often do you benchmark your cyber security status (Annually, quarterly, monthly, etc.)?	
C. How are you incorporating industry standards or regulatory mandates for your cyber security performance assessment?	
D. If you are using services from another organization/agency what are their cyber risk performance metrics? How do they adequately cover the scope and scale of your unique operations (e.g. People, Platform, Processes and Performance requirements)?	
E. How is the frequency and scope of your cyber risk monitoring keeping pace with the threat trends?	
F. How many open vulnerabilities does your IT/Security team have and what is the aging trend?	
G. Do you currently have or are you considering insurance to cover a cyber attack? How is the cost of your premium determined, and how can you take action to lower the cost?	
H. Does your overall organizational risk assessment include the cost and impact of a cyber attack/breach?	

6. FUTURE STATE

A. What are your objectives for the coming year, and can the current People, Platforms, Processes and Performance support those objectives?	
B. What successes and issues are you encountering as you move forward with you cyber security plans?	
C. How are you prioritizing the areas in need of more resources and budget?	
D. What are the attitudes and beliefs of your superiors/management/board regarding your cyber security journey?	
E. How do report to them regarding the scope and scale of your attack surface and the trend toward faster weaponization of vulnerabilities?	

7. PROOF OF CONCEPT CONSIDERATIONS

A. What will be the expected attitude toward evaluating your current cyber risk management posture?	
B. How much resistance or objections about the subject do you expect? What would be the key issues?	
C. How would your organization use the output of a confidential assessment?	
D. With the results of a limited penetration test and proof of concept assessment being provided through our RiskSense platform, how would your organization utilize the credit score-like risk scoring?	
E. What form of business case budget planning does your organization require?	
F. What type of Return on Investment (ROI) does your organization require?	

8. OTHER COMMENTS, OBSERVATIONS, OR CRITICAL INFORMATION

____

____

____

____

____

____

____

____

____

____

____

9. KEY FINDINGS AND RECOMMENDATIONS

____

____

____

____

____

____

____

____

____

____

____