G-Cloud 14

Service Definition - Wipro Enterprise Risk & Cyber Resilience Assessment Services

Wipro’s Focus areas for Cyber Resilience

1 Data security controls

Data Leak Prevention and PAM have continued to be the security controls that organizations find most effective

35% of respondents felt that PAM was the most effective data security control

2 Cloud Security

Customers are migrating PCI data and customer PII to the cloud. The ‘Cloud-first’ strategy is well laid out over 2 dimensions; poly-cloud and hybrid cloud approach

69% of organizations are moving customer PCI to the cloud

3 IoT security

Organizations are likely to look for an approach that blends traditional enterprise IT with the convergent needs of IoT

60% of the organizations will have an asset base of 10% connected devices within 2 years

4 Application security

Digital transformation is using DevOps to reduce the cycle time and increase the velocity of builds. Organizations need to adapt their security practices with the ongoing digitization drive

25% of the respondents said that they are carrying out the security assessment in every build cycle

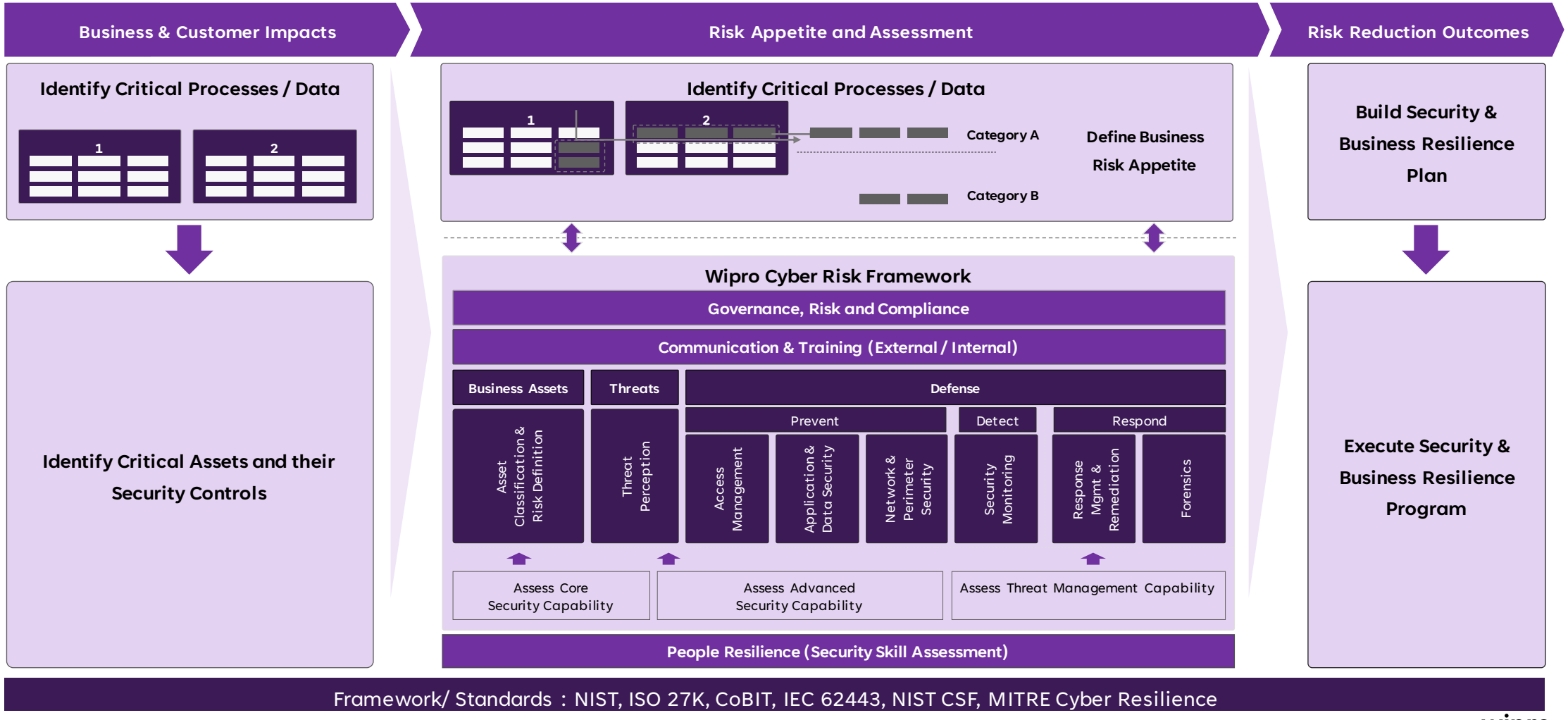
5 Security Monitoring & Analytics

ROI driven management is seeking faster detection and resolution.

78% of respondents said that SOAR tools are key to improving threat detection

Wipro's Approach to Cyber Resilience

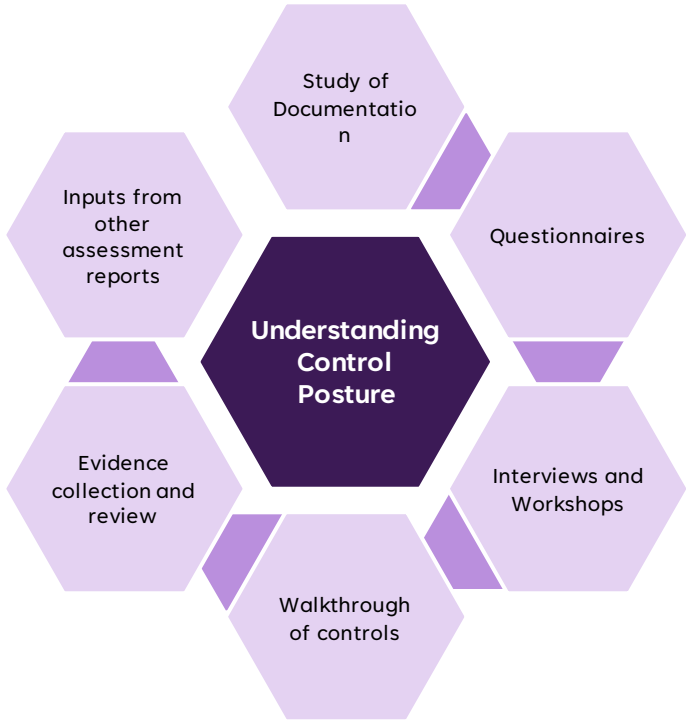
Wipro proposes a Cyber Resilience approach including identification of critical assets/ resources, baselining the cyber resilience maturity level through resilience maturity assessment leveraging the Wipro Cyber Risk Framework, followed by the Business Resilience program for ongoing continuous improvement as depicted below



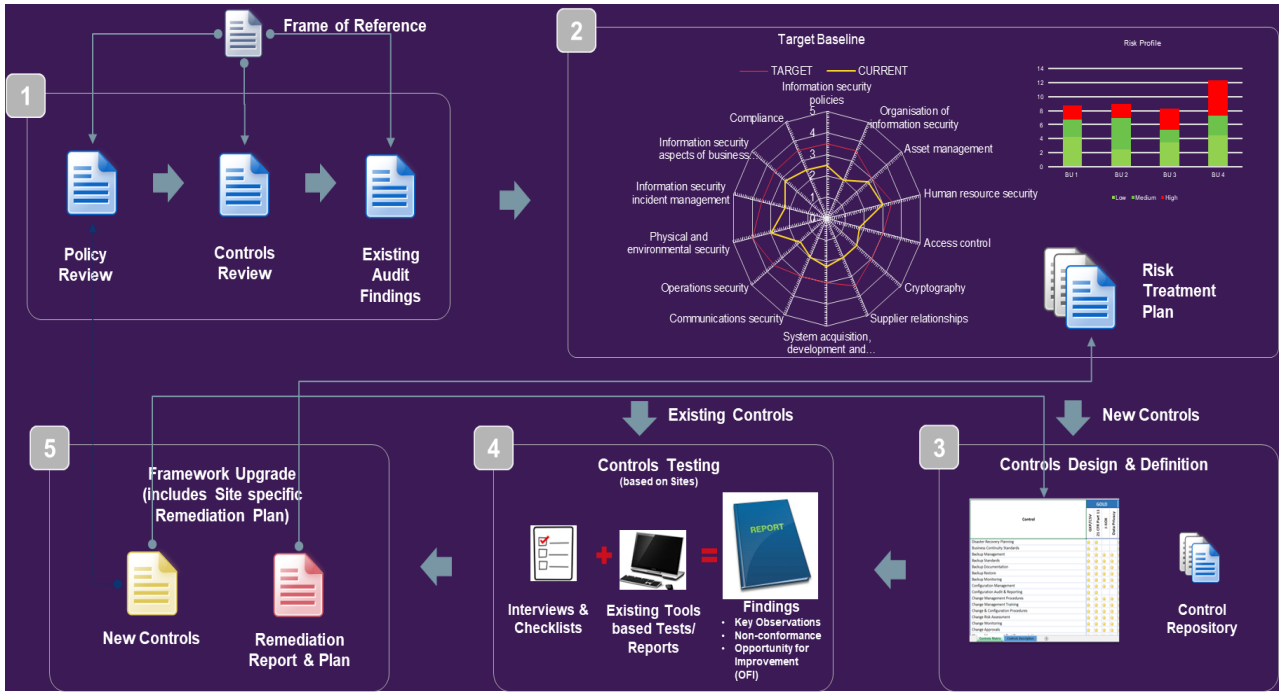
Proposed assessment methodology to baseline Cyber Resilience maturity level

Wipro consultants shall use various assessment techniques like inquiry, observation, examination, etc. to understand the control posture within the organization to assess the cyber resilience to identify gap areas in the maturity level from the current state to the desired state for addressing the gaps.

Approach



Activities : Cyber Resilience Maturity Assessment



In scope domains : Resilience, Security architecture, technical security, compliance assurance, leadership and operational governance, information risk management, human factors, third parties

Outcomes

- Cyber resilience maturity report
- Recommendations
- Road Map
- Capability building

Accelerators

IEC/ IS 62443 CSF Questions
Benefits : Provides the areas of improvement and current strengths based on the responses from the users.

Cyber Resilience Maturity framework
Benefits :Provides the current state maturity dashboard and target state for maturity improvement

Key Assessment Types for Cyber Resilience Maturity Assessment

Holistic and metrics-based views to Client stakeholders

1 Standards based Cyber Resilience Assessment

Assessment of landscape to identify architectural deficiencies against recommended baselines. Ex.: NIST 800-53, NIST 800-160, NIST CSF ISO 27001, SOX,HIPAA, GDPR,NIS2, etc. applied to IT landscape

2 Attack Surface Analysis & Assessment

Assessment of the Enterprise Attack Surfaces from an Outside-In perspective by reviewing the existing Vulnerability assessment, PEN Reports , other assessment reports and the remediation progress

3 Threat Exposure Analysis & Assessment

Review the existing quarterly phishing assessment campaigns, effectiveness of phishing related training programs and simulations , remediation measures for addressing the identified risks . Review of existing phishing related policies and process to have a robust employee aware environment.

4 Quantifiable, Evidence based Cyber Effectiveness Assessment

Assessment of current state maturity level of information security related controls and other frameworks /standards to identify the gaps in the maturity level compared to current state vs desired state

5 Architectural Assessment for Critical Application Stacks

SABSA led and TOGAF principles driven full stack Architectural Analysis. Zones and Conduits for OT networks.

e.g. Key Execs on target lists, Spoofed websites, External Ratings

6 Business Continuity/Disaster recovery Assessment

- IT-DR Gap Assessment, Site Audit
- BC Benchmarking Exercise based on BS25999), review of recovery Strategy Design & Documentation, Crisis management plan & procedure, Review current emergency procedures
- Crisis communication, response & management plans

Cyber Resilience Maturity Assessment for a leading Telecom Company

Challenges

- Evaluate the risk posture of the organization
- As part of Enterprise Risk Management (ERM) initiative wanted to assess the risks associated with application processing, product design and marketing, fraud monitoring, etc.
- Perform the maturity assessment and identify the risks and gaps with respect to maturity
- Benchmark with industry standards like ISO and NIST
- Provide roadmap to mitigate and manage the risks and increase the maturity level of the enterprise

Solution Highlights

- Gather inputs from self assessments, audit reports and various other initiatives like security review and access control management
- Analyze the risks and rate them as per their ERM matrix and create a risk register
- Prioritize the risks based on their rating and work out the remediation plan with the owners
- Monitor the risks to ensure that appropriate risk treatment is carried out and Implement risk assessment before any major change to the systems
- Deliver a roadmap to increase the overall maturity of the organization

Value Delivered

- Established information security risk management framework to assess, track and remediate information security risks on an ongoing basis
- Developed roadmap to manage the risks and increase maturity level in alignment with the organizational objectives and industry best practices
- Improved security process and monitor and manage risks effectively for improving the cyber resilience posture to achieve the target level

Thank you.

Kindly contact us at the following Wipro email id for any further information and engagement related details.

Email - publicsector-uki@wipro.com