

# Work From Home Security Assessment

CyRAACS Approach Document



[cyraacs.com](https://cyraacs.com)

Murari Shanker | +91-9886210050 | [ms@cyraacs.com](mailto:ms@cyraacs.com)



# The “New Normal”

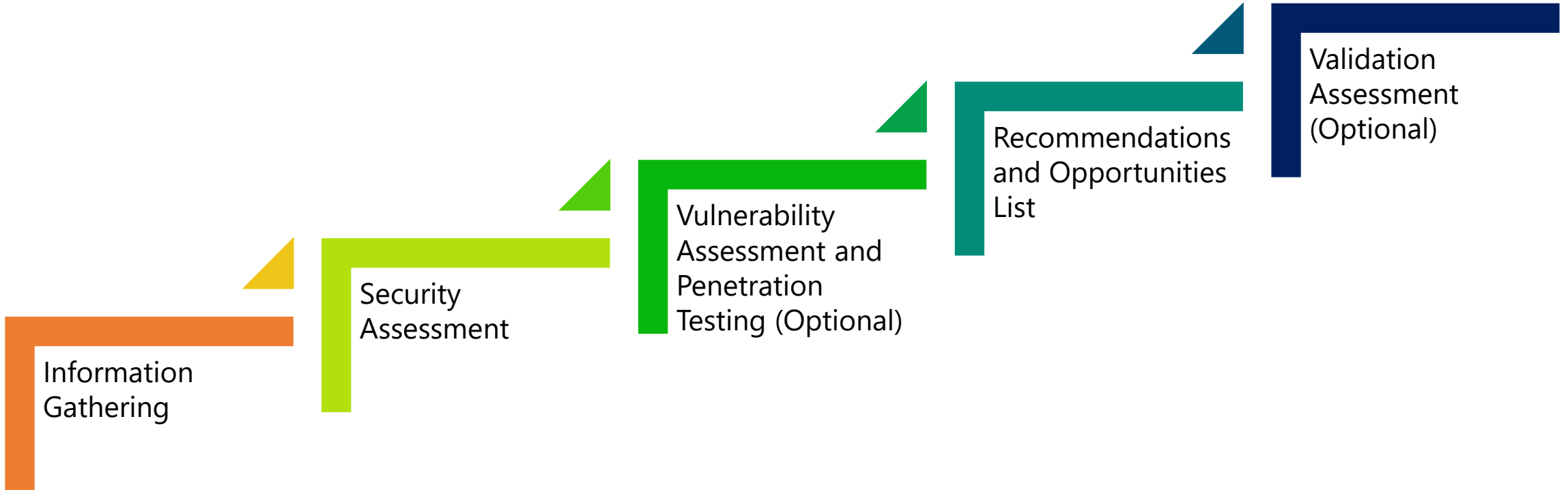
- The rapid global spread of COVID-19 has caused disruption to billions of lives as well as significant and far-reaching economic damage. Organizations have been taking various measures during these challenging times to ensure continuity of services and operations.
- Organizations deploying workforce to work remotely have seen an increase in attacks related to **phishing, malware, spam mails, frauds** etc.
- Over 50% of organizations in a recent survey cited security risks as a key challenge of managing IT in-house, the highest among all factors.
- The prevalence of security on the business agenda is further heightened by the *massive increase in the number of devices remotely connecting to enterprises due to the enforced work-from-home situation.*
- Organizations will need to look at their business strategies with the emergence of the new normal, reevaluate their security and business continuity strategies. This means assessing all contours of security and investing in the right technologies, skillsets, and processes to ensure improved security and resilience.

# Work From Home Security Assessment

- With increasing reliance on Work From Home, a Security Assessment for such a setup is the First Step to ensure appropriate Information Security controls are implemented.
- A Security Assessment can help to identify gaps, vulnerabilities and corresponding risks in the IT Infrastructure, Applications, Security Processes and Governance.
- Our Work From Home Security Assessment framework evaluates organizations' Remote Access/Work From Home security posture using a risk-based approach to information security.
- The study can also incorporate requirements from regulations, clients and standards/frameworks on information security to ensure continued compliance.



# Framework



# Methodology

## Information Gathering

- Collate documentation and other information related to the current IT security architecture
- Identify the business-critical information assets (Applications, Infrastructure, End Points, Mobile devices, etc.)
- Identify contacts from Departments for interviews and discussions
- Obtain needed documentation including policies and procedures.
- Develop Project Plan

## Security Assessment

- Identify applicable legal, regulatory, standard and contractual requirements related to information security and data privacy
- Study policies and procedures related to Information Security and Data Privacy
- Study technology controls implementation for Security for the in-scope areas and its effectiveness
- Understand and review the process for Security monitoring and reporting
- Review process controls and compliance to information security standard/framework requirements (e.g.: ISO 27001)
- Identify gaps and corresponding risks in technology and process controls
- Assess maturity of Security Technology controls

## Vulnerability Assessment and Penetration Testing (optional)

- Conduct Vulnerability Assessment and Penetration Testing for in-scope IT Infrastructure and Application Components
- Identify vulnerabilities and corresponding risks
- Provide Proof of Concept as applicable
- Provide recommendations for mitigation

## Recommendations and Opportunities List

- Identify technology enhancements to enhance maturity
- Categorize the recommendations on the following parameters:
  - Prioritization
  - Effort Complexity
  - Risk Mitigation Index
  - Cost of Implementation
- Develop opportunities list for Information Security
- Advise on the acquisition of additional Security Technology solutions
- Provide advisory on timelines for implementation

## Validation Assessment (optional)

- Conduct validation assessment for the implementation of recommendations provided
- Provide report on the Information Security Posture basis the implementation of recommendations

# Indicative Coverage Areas

## Endpoint Security

- Anti-virus/Anti-malware
- Remote Connectivity
- User Access Control
- OS Hardening
- Device Encryption
- OS Hardening
- MDM

## Firewall

- Firewall details
- Firewall OS/Firmware updates
- Firewall policies configuration
- Whitelisting/Blacklisting
- Anti-spoofing filters
- Firewall rules/policies review
- User Access Control
- Policy usage and Patterns Review

## Data Security

- Data Classification
- Data Leakage Prevention
- Encryption

## Email Security

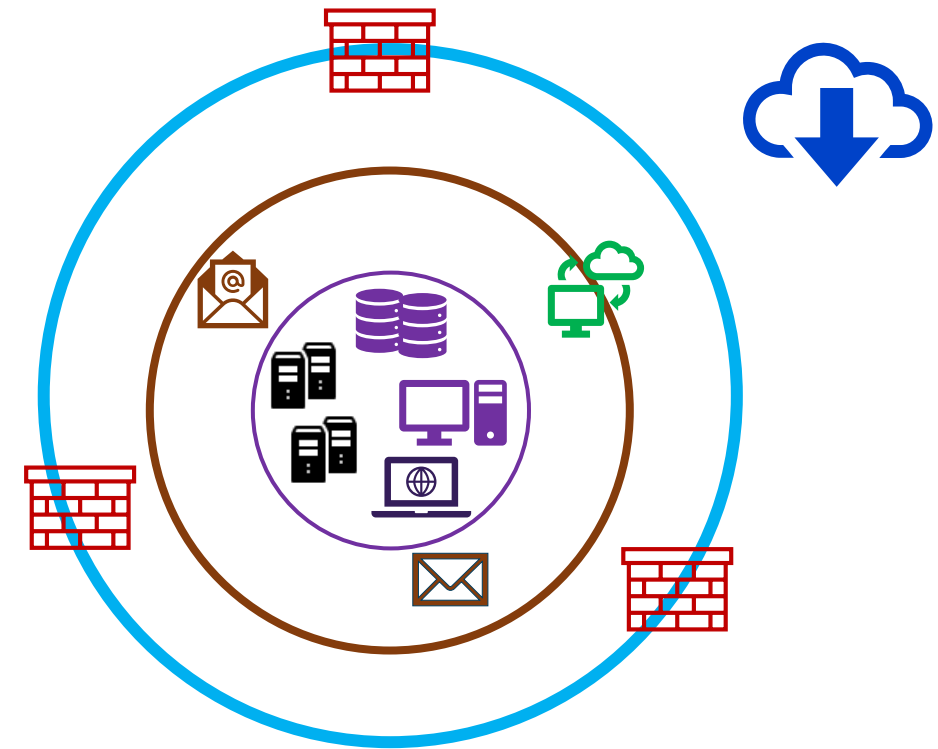
- Web Access
- Spam Filter
- Phishing Filter
- Email Domain Restrictions
- Backup and Archival
- Restrictions on Attachments, File Size
- Email Monitoring
- Encryption

## VPN

- Encryption
- Provisioning, Deprovisioning
- User List
- Multi-Factor Authentication
- Authentication and Credential Management
- Logging

## User Access Management

- Identity and Access Management
- Access Reconciliation
- Role Based Access Matrix



Indicative Coverage Areas

# Indicative Coverage Areas

## Endpoint Security

- Anti-virus/Anti-malware
- Remote Connectivity
- User Access Control
- OS Hardening
- Device Encryption
- OS Hardening
- MDM

## Data Security

- Data Classification
- Data Leakage Prevention
- Encryption

## Email Security

- Web Access
- Spam Filter
- Phishing Filter
- Email Domain Restrictions
- Backup and Archival
- Restrictions on Attachments, File Size
- Email Monitoring
- Encryption

## User Access Management

- Identity and Access Management
- Access Reconciliation
- Role Based Access Matrix

## Network Security

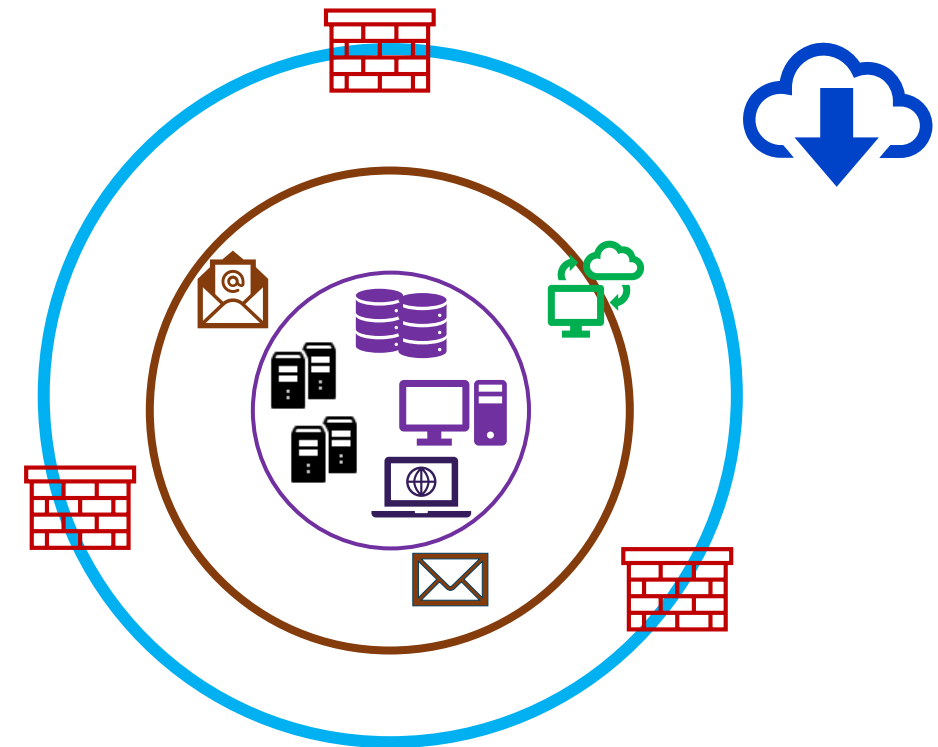
- Network Hardening
- Network Access Control
- Network Monitoring

## VPN

- Encryption
- Provisioning, Deprovisioning
- User List
- Multi-Factor Authentication
- Authentication and Credential Management
- Logging

## Firewall

- Firewall details
- Firewall OS/Firmware updates
- Firewall policies configuration
- Whitelisting/Blacklisting
- Anti-spoofing filters
- Firewall rules/policies review
- User Access Control
- Policy usage and Patterns Review



Indicative Coverage Areas



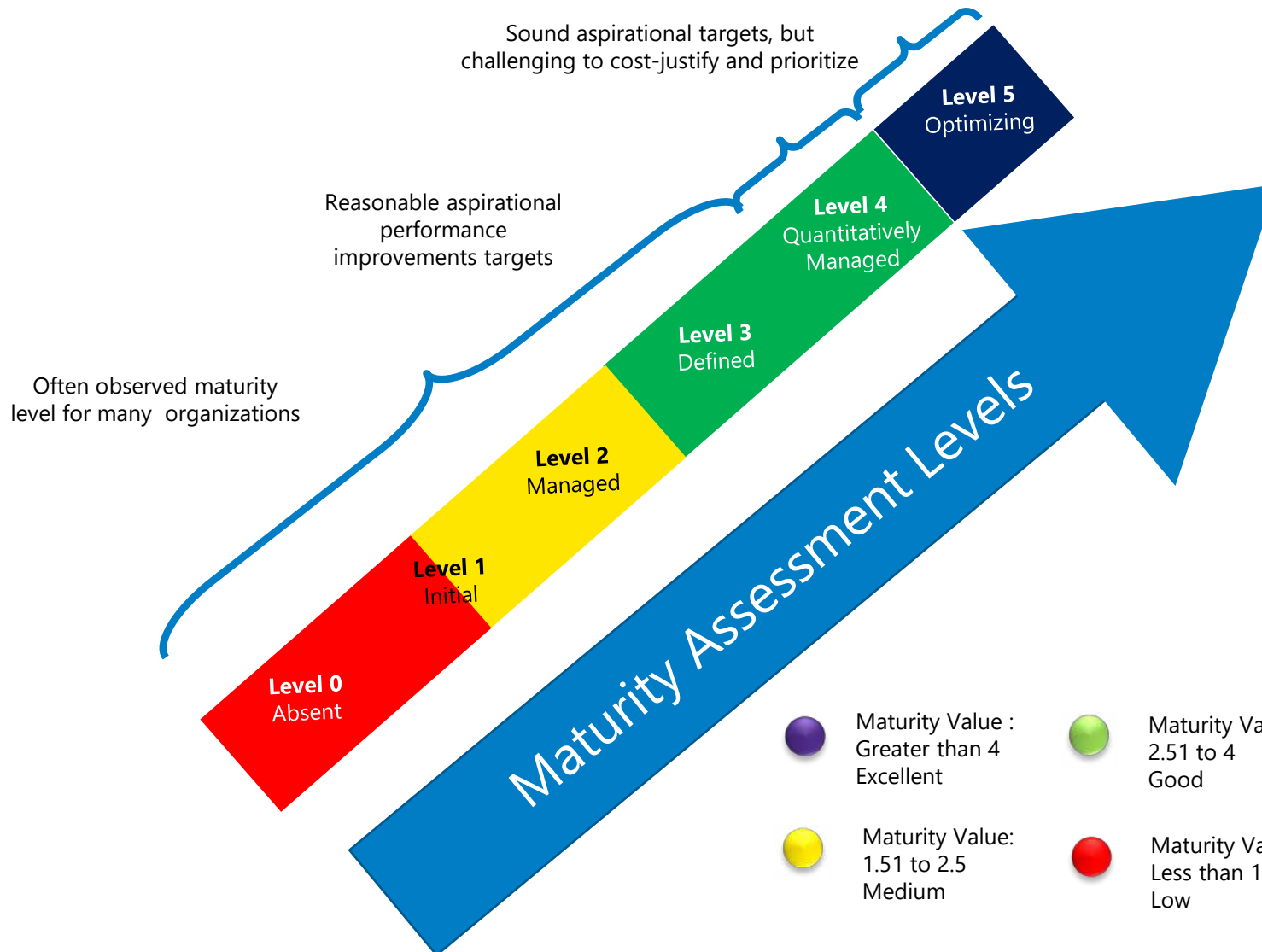
# Deliverables

- Security Assessment Report
  - Opportunities List
    - Technology Enhancements
    - Process Initiatives
  - Advisory on Acquisition of Security Technologies
- Recommendations based on:
  - Prioritization
  - Effort Complexity
  - Risk Mitigation Index
  - Cost of Implementation



# Sample Work Products

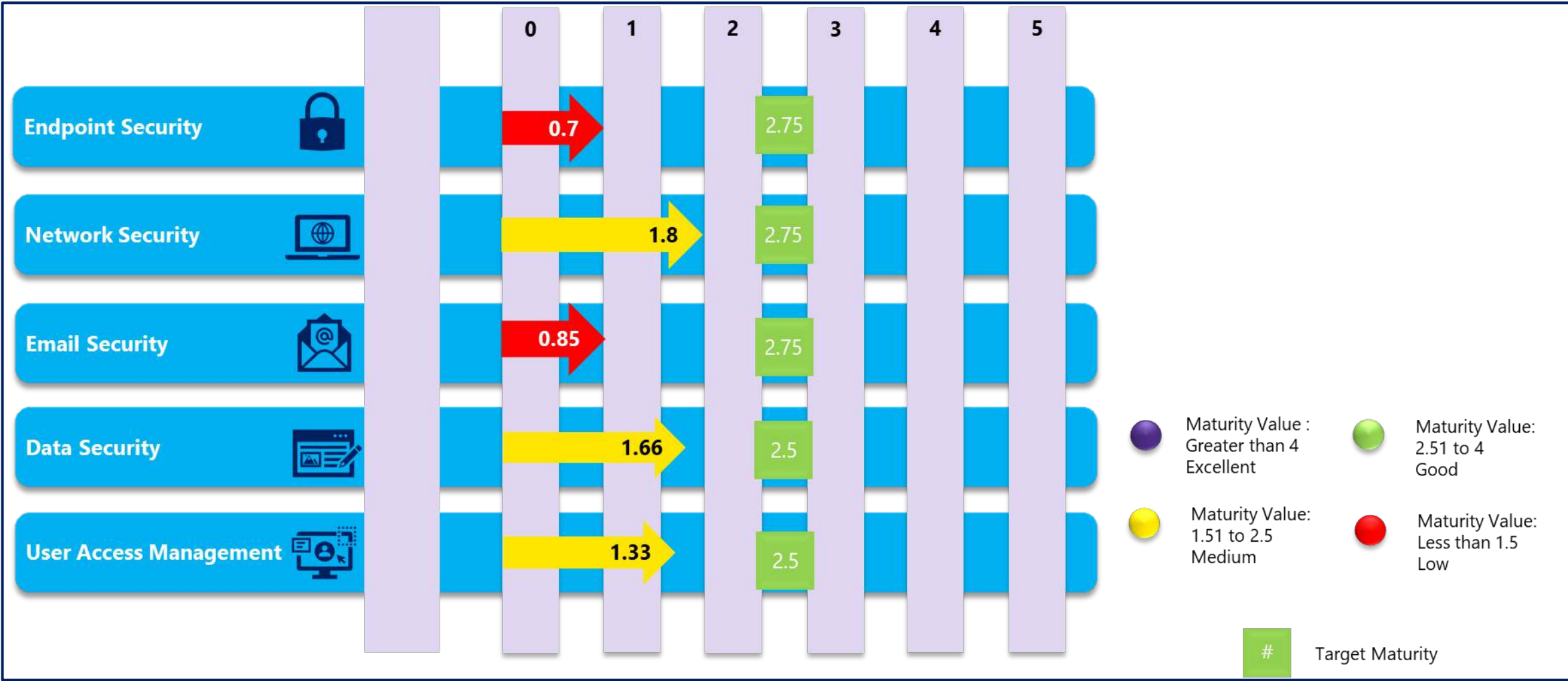
# Maturity Assessment Levels



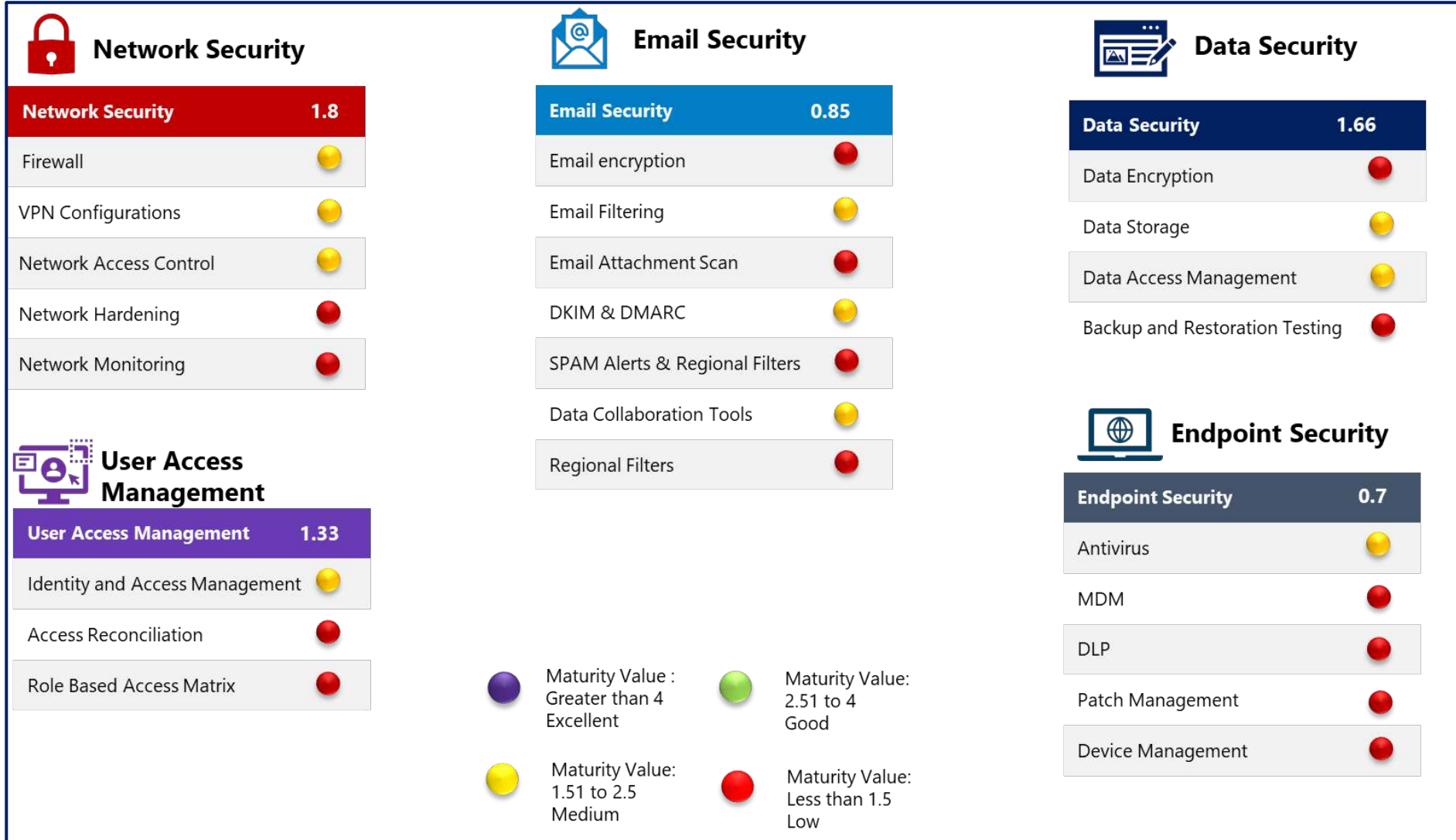
## Assessment Scale and Typical Characteristics

- 0: Absent** - Non-Existent Process
- 1: Initial** - Process is unpredictable, poorly controlled and reactive
- 2: Managed** - Process is characterized by projects and is often reactive
- 3: Defined** - Process is characterized by the organization and is proactive
- 4: Quantitatively Managed** - Process is documented, measured and controlled
- 5: Optimizing** - Focus is on continuous process improvement












# Sample Current State Assessment and Maturity Ratings



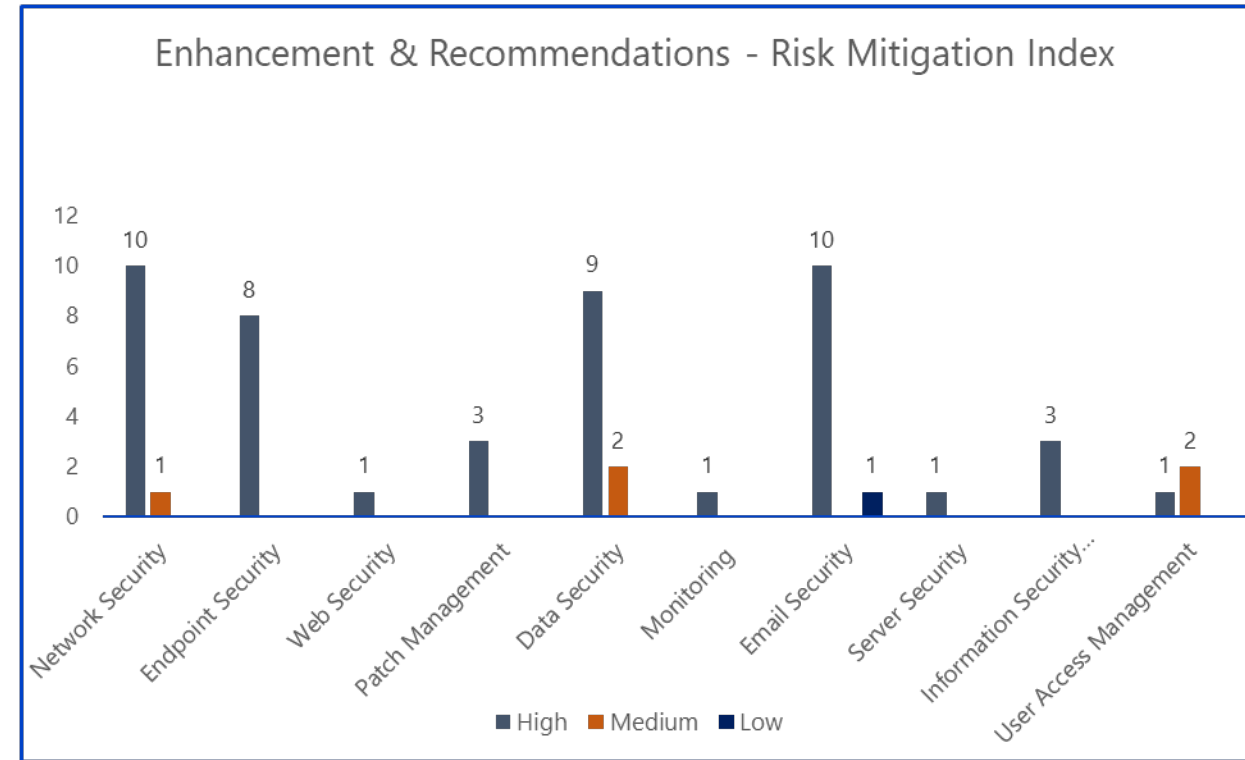
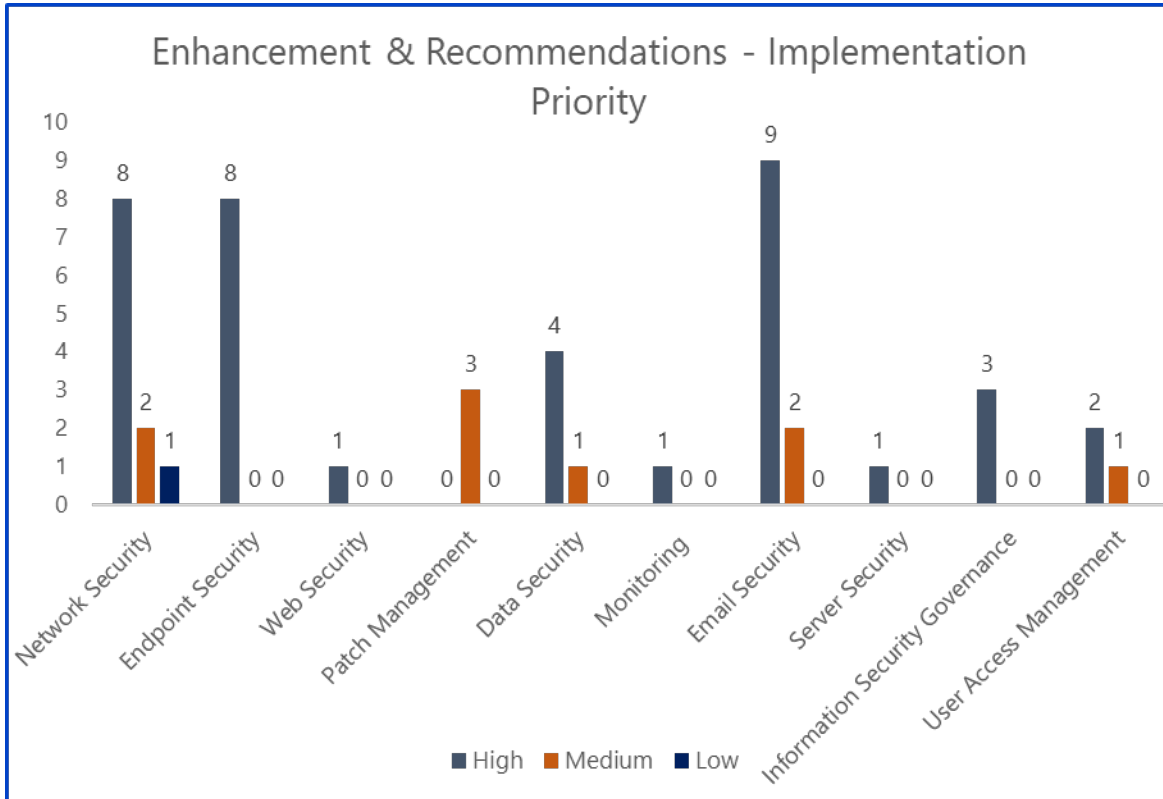
# Sample Current State Assessment and Maturity Ratings



# Sample Assessment – Endpoint Security

 <b>Endpoint Security</b>	Current Maturity	<b>0.7</b>
<b>Endpoint Security</b> <b>0.7</b>	Areas covered	Antivirus, MDM, DLP, Patch Management, Device Management, OS Hardening
Antivirus 	Key Observations	<ul style="list-style-type: none"> <li>The Linux machines do not have an anti-virus installed. A few Linux servers are hosted in the DMZ.</li> <li>The McAfee anti-virus reports denote a compliance of 30% only. There are no follow up actions on the systems missed in the scan report.</li> <li>The EDR capabilities are not implemented in the environment.</li> <li>Resources not available to implement and dedicatedly manage EDR.</li> <li>MDM solution has not been implemented, the solution is planned to be implemented in next 3-6 months.</li> <li>Malware Analysis has detected services/applications installed and configured on endpoint systems which can lead to data breaches or misuse of application to perform unwanted/stealth operations.</li> </ul>
MDM 	ISO 27001 Controls Mapping	A.6.2.1 - Mobile device policy A.6.2.2 - Teleworking A.12.2.1 - Controls against malware A.12.4.1 - Event logging
DLP 	Key Recommendations	<ul style="list-style-type: none"> <li>Implement anti-virus for Linux machines especially hosted in the DMZ.</li> <li>Implement EDR capabilities from Symantec for enhanced and real time threat protection.</li> <li>Identify resources to implement and monitor the EDR capabilities in the organization.</li> <li>Establish a formal process for remediation actions to be taken for any non-compliance in anti-virus compliance scans.</li> <li>Implement MDM solution for all mobile devices.</li> <li>Enable remote Wipeout for all mobile devices.</li> <li>Create standard Operating System (OS) images for all OS types and versions. Complete OS hardening before issuing endpoints.</li> <li>Ensure least privilege access for users on endpoint systems.</li> </ul>
Patch Management 	Target Maturity	<b>2.75</b>
Device Management 		
<p>  Maturity Value : Greater than 4 Excellent   Maturity Value: 2.51 to 4 Good   Maturity Value: 1.51 to 2.5 Medium   Maturity Value: Less than 1.5 Low         </p>		
 # Target Maturity		

# Sample Recommendations and Enhancements

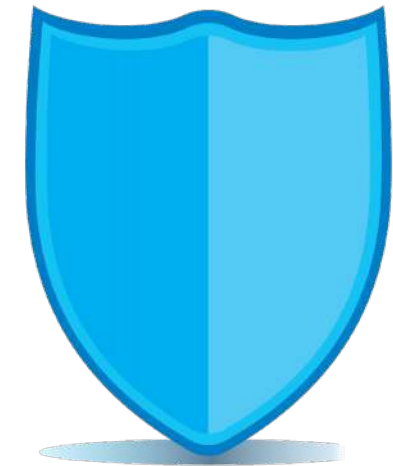


# About Us



# Seamless Security through Collaboration and Innovation

- CyRAACS was established to provide robust and sustainable cyber security solutions to organizations. Our focus is to tailor and integrate our solutions into client environments seamlessly, so they can focus on their core business completely.
- We work as an Extended Arm for our clients, managing their information security objectives and enhancing their posture.
- We accomplish this by **Collaboration, Commitment, Innovation and Passion**.
- We offer the full suite of services in Compliance Lifecycle – Framework, Assessment, Implementation and Audit services.
- Our Technical Services include Vulnerability Assessment and Penetration Testing, Code Reviews and niche services like Malware Analysis, Forensics, Study of Indicators of Compromise and Indicators of Attack.
- We are empaneled with **CERT-In** (Computer Emergency Response Team – India) and **Qualified Security Assessor** for PCI DSS.



Your Trusted Security Partner

# About Us

- Proven track record of delivering complex projects across varied domains such as BFSI, Born-in-the-Cloud, Logistics, IT/ITES, Manufacturing, Pharma etc.
- Extensive experience in Information Security and Data Privacy Standards/Frameworks such as ISO 27001, PCI DSS, SOC 2, NIST 800-53, CSA STAR, GDPR,CCPA etc.
- Over 90 happy clients and 200+ successful engagement deliveries
- Cyber Security Solutions tailor-made to Client requirements
- Consultants with Leading Industry Certifications CISSP, CISA, CEH, CISM etc.



**The Best Cyber Security Consulting  
Company of the Year – CISO  
Leadership Awards 2019**

# Our Leadership



Suresh Iyer  
Co-Founder and CEO

- Over 28 Years of Experience in Technology, IT Security, Risk Management and Privacy areas
- Has served in CXO positions in many global organisations like Ocwen Financials, Altisource, Aditya Birla Minacs, eFunds and Bank of America
- An eminent speaker and panellist in many industry and security forums

- Multi-disciplinary leader with over 30 years of industry experience areas of Technology, Data Centre, IT Operations, Information Security etc.
- Has held CXO positions for global organizations such as Concentrix, Altisource, Convergys, Mphasis, IBM etc.
- **Qualified Security Assessor** for PCI DSS and **Certified Information Security Manager**



Murari Shanker  
Co-Founder and COO

# Signature Services

## Governance and Compliance Services

- Control Assurance Services
- QSA Services for PCI DSS
- Third Party Risk Management
- Policy Management

## Risk Advisory Services

- Information Security Risk Management
- Information Security Maturity Model Assessment
- Business Continuity Management

## Technical Services

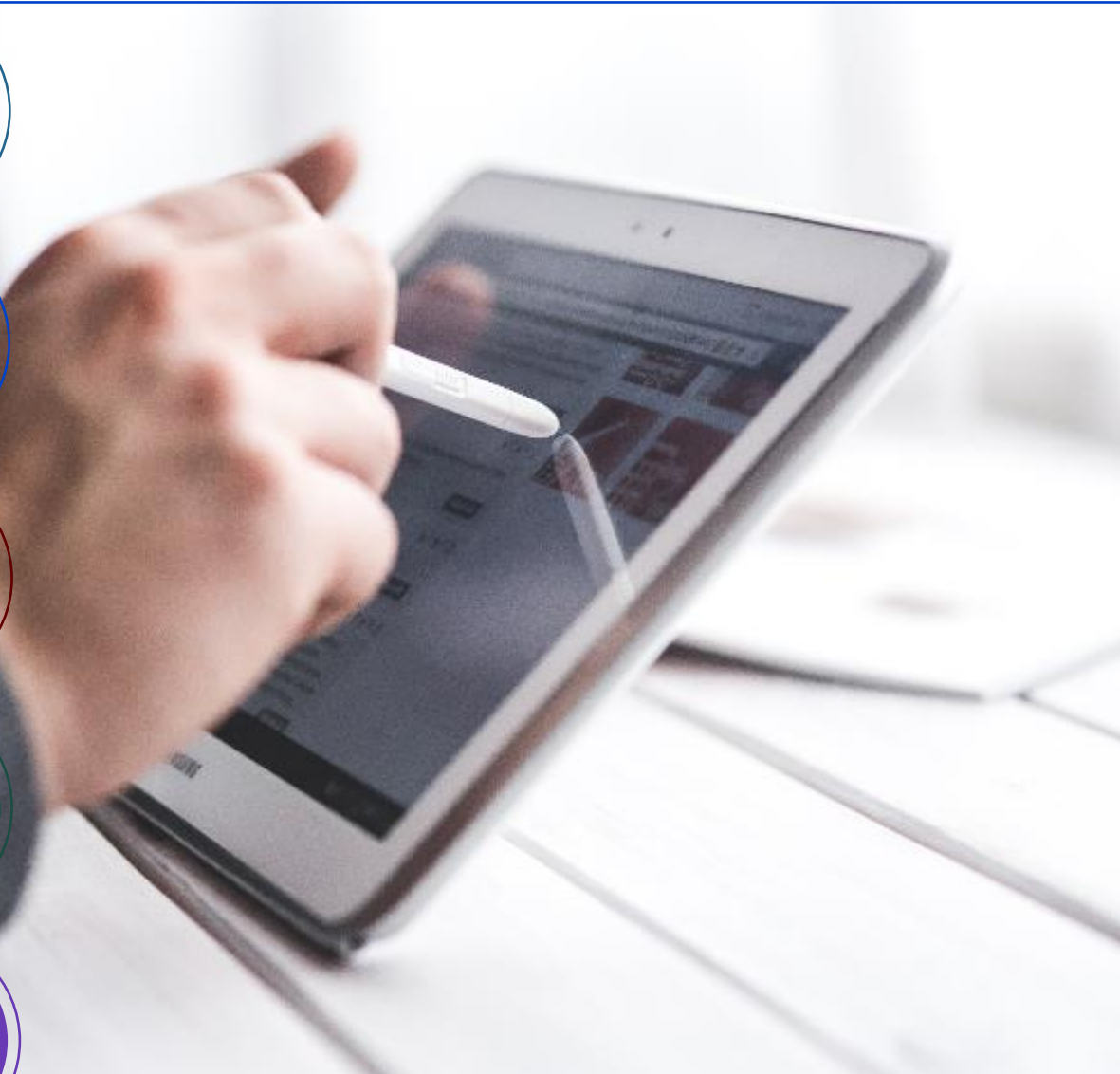
- Data Flow Analysis
- Vulnerability Assessment and Penetration Testing
- Secure Code Review
- Compliance As a Service for PCI DSS

## Managed Security Services

- CISO Services
- Managed VAPT Services

## Other Capabilities

- Cyber Forensics
- Advance Malware Analysis
- Study of Indicators of Compromise
- Study of Indicators of Attack
- Balanced Scorecard for Information Security





# Our Credentials

## Consulting Done Right

- Combination of technology, security and deep industry sector experience
- Offer a unique consultative approach and not a "One Size fits all" one, as every organization is at a unique stage in its cyber security journey

## Qualified Teams

- Requisite blend of functional and technical skills to deliver cyber security assessments for clients

## Technical Proficiency

- Automated assessment tools supported by manual verification
- Controlled service; tests designed to ensure no steps are missed and reduce impact on target systems
- Repeatable service; test parameters recorded to allow retesting under the same conditions



## Rich Experience

- Experience in delivering cyber security and data privacy services, including large-scale security programs
- Pioneer in providing tailored and sustainable cyber security solutions

## Assessment Framework and Methodology

- Comprehensive framework aligning to security industry standards
- Flexible methodologies and tools to meet client requirements

## Deep Domain Expertise

- Well-informed views on the risks and challenges faced by clients
- Knowledgeable opinions backed by experiences and data from earlier engagements
- Insights and best practices specific to client

# Work From Home Security Assessment

CyRAACS Approach Document



[cyraacs.com](https://cyraacs.com)

Murari Shanker | +91-9886210050 | [ms@cyraacs.com](mailto:ms@cyraacs.com)