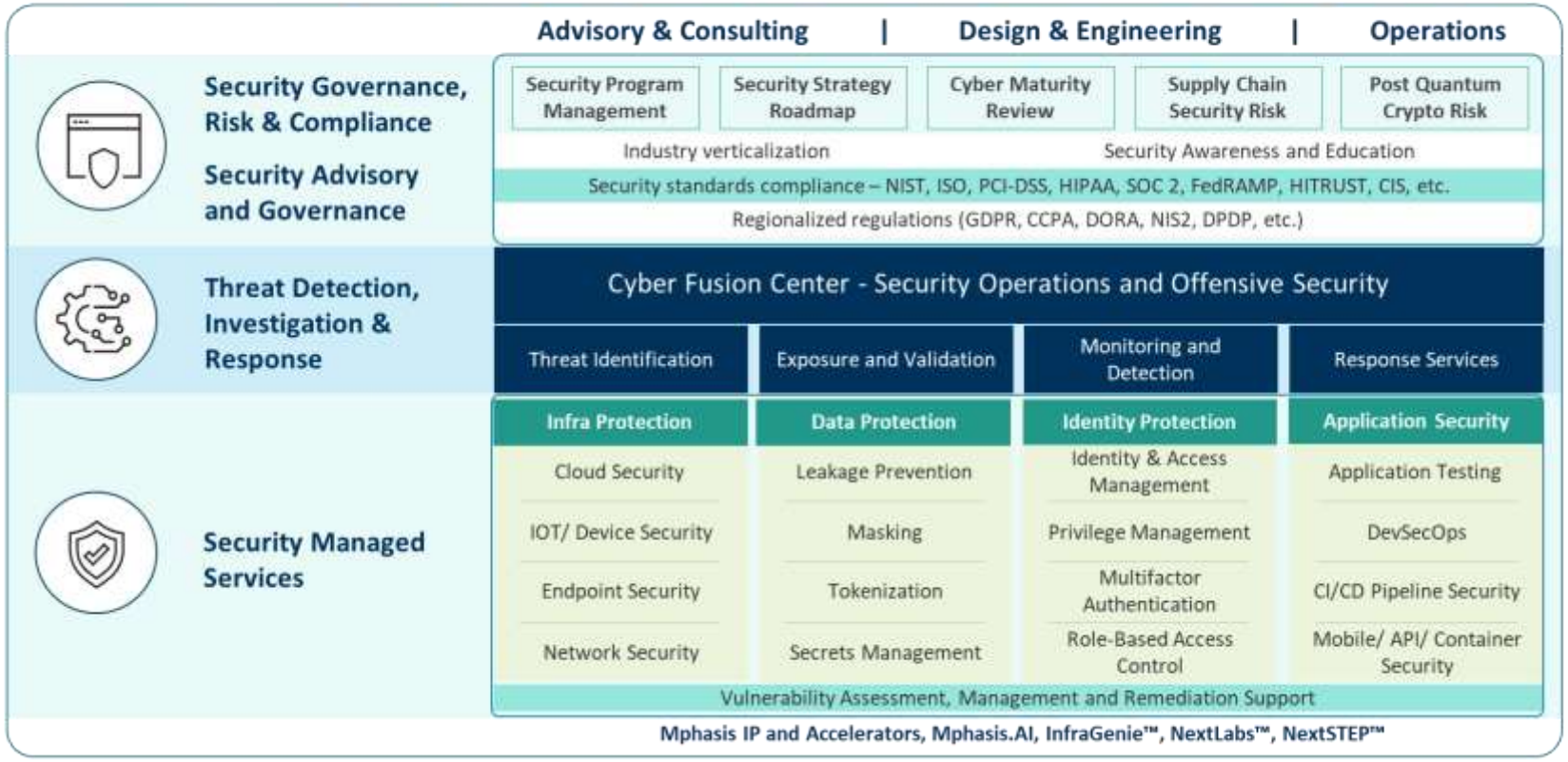
Mphasis
The Next Applied

Cybersecurity Briefing

Mphasis Cybersecurity Services

Mphasis provides end-to-end cyber security services, strengthened by IP, accelerators and a broad partner ecosystem



1,000+
Security professionals

75 M+
Identities managed

10,000+
Investigating suspected events per day

500,000
Endpoints covered under Data & Infrastructure Security

750,000
Number of IP addresses managed for Vulnerability Assessment

 29-01-2026

AI & Automation Cyber Initiatives

1 Vulnerability Remediation
AI code analyzer to find, auto fix, and prioritize vulnerabilities, and manage tech debt

2 IDAM
Automated Application onboarding & Integration testing accelerator

3 IDAM
Gen AI based manager access review assistant

4 3rd Party Vendor Cyber Risk
Gen AI based third party vendor cyber assessment and continuous monitoring agent

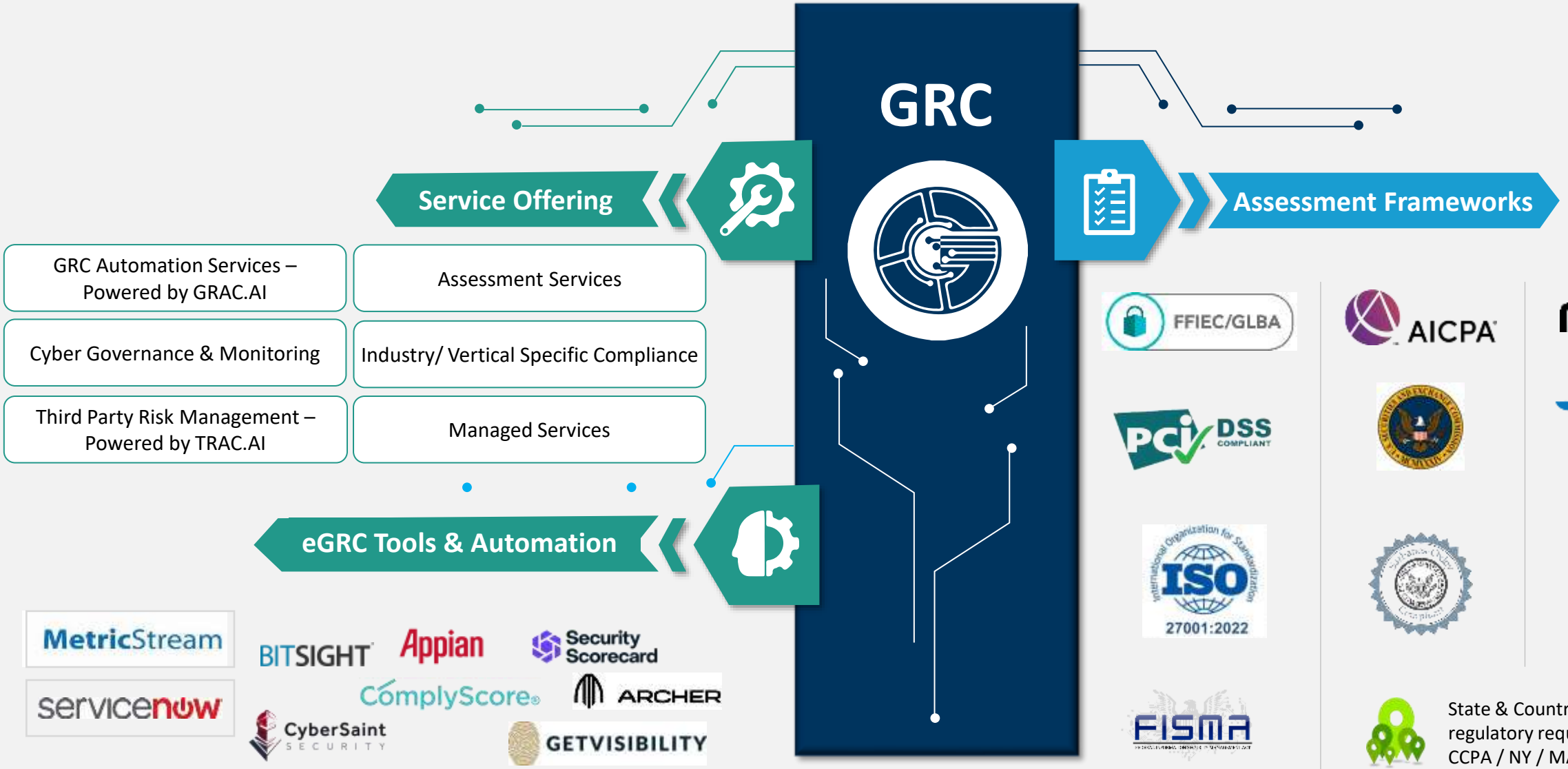
5 TDIR (SOC)
Autonomous Agentic AI reviews threat intel sources, correlates and takes actions

6 Data Classification
Identify unstructured data using AI and classify them

7 RPA Automation
Automation in the security operations using RPA

8 Internal Audits & Compliance
Gen AI based audit assistant for continuous audits & IT Controls compliance monitoring

Governance Risk & Compliance Services



Mphasis Cyber Fusion Center Services

THREAT IDENTIFICATION

- Deep and Dark Web Activity Monitoring
- Intelligence Curation and Management
- Threat Hunting

EXPOSURE & VALIDATION

- External Attack Surface Management
- Continuous Threat Exposure Management
- Breach and Attack Simulation (BAS)
- Penetration Testing as a Service
- Automated Red Team
- Deep Fake

MONITORING & DETECTION

- Threat Monitoring & Detection
- Identity Threat Detection and Response
- Endpoint Detection and Response
- Network Detection and Response
- Supply Chain Detection and Response
- Detection Engineering

RESPONSE

- Containment
- Incidence Response Remediation
- Digital Forensics

AI Enablement

Discovery of novel attack methods

Identify suspicious devices or user activities

Rapid response decisions

Rapid Incident Investigation

Mphasis Identity Security Capability

Identity Security

- Advisory
- Implementation
- Operations

WORKFORCE IAM

- Identity Lifecycle Automation, HR JML Workflows
- App. Onboarding, SSO, App. Password Mgmt./Sync
- ZT Least Privilege Access, MFA, Time-Bound Access
- Identity Access Governance /Compliance, RBAC, SoD

CUSTOMER IAM

- External / Social Identity Federation
- Customer Journey, Prog. Profiling
- SSO, MFA, Authorization & Consent Mgmt.
- Customer Identity Protection, Lifecycle Mgmt.

PRIVILEGED IAM/PAM

- Admin, Superuser, Service Account Discovery
- Privileged Access Control, Monitoring & Alerting
- ZT Just-In-Time, Time-Bound Privileged Access
- Privileged Access Governance /Compliance

IAM FOR CLOUD

- Cloud Infrastructure Entitlement Management (CIEM)
- Cloud Privilege Access Monitoring & Alerting
- Cloud Identity Lifecycle Automation, RBAC, SoD
- Cloud Identity Authentication, SSO, MFA, Federation

IAM FOR APPS/APIS

- Centralized Authentication, SSO, MFA
- Apps/APIs Authorization, Access Mgmt.
- Federation, SSO for B2B, B2C
- Adaptive Authn., ZT Identity Protection

PRODUCT EXPERTISE

SailPoint, SAVIYNT, Microsoft, okta, ForgeRock, PingIdentity, CYBERARK, thycotic, BeyondTrust, ORACLE, IBM, ca

AT A GLANCE

- Vendor agnostic
- In-depth Identity and Access domain expertise
- On-premise, hybrid, cloud and multi-cloud environment
- Simplify Processes, Consolidate Tools, Automation
- Identity Transformation and Cost Optimization
- Improve user experience and satisfaction
- Seamless and frictionless Access
- Higher levels of compliance to Identity security regulations and best practices

AUTOMATION

- Robotic Process Automation for low touch operations
- Connector plugin library for application integration
- Integrated CI/CD pipeline for continuous build, automation , testing
- Automated Role Based Access Control Framework
- ServiceNow workflow automation framework and templates
- Factory-based model applied for application onboarding

Application Security Services

Mphasis
The Next Applied

Plan	Develop	Build	Test	Release	Deploy	Operate
• Threat Modeling • Secure Coding Practices • Manual Code Review • Architecture Risk Analysis (ARA) • Security Training and Awareness • IDE Security Plugins • Compliance	• Static Application Security Testing (SAST) • Interactive Application Security Testing (IAST) • Software Composition Analysis (SCA) • Infrastructure as Code Analysis • Secrets Scanning • SBOM and OSS Governance	• Dynamic Application Security Testing (DAST) • OS Hardening • Container Hardening • Mobile Application Security Testing (MAST) • API Security Testing • Vulnerability Management	• Vulnerability Correlation & Security Orchestration • False Positive Analysis • Penetration Testing • Fuzz Testing • Container Security Testing • Infrastructure Security Testing • Zero Trust Framework	• Remediation Services • Configuration Management • Secrets Management • Reporting & Dashboards • Security Posture Management • Runtime Application Self-Protection (RASP) • WAF and DDoS Protection

How we can help

➢ Assess, setup &/or improve AppSec program ➢ Consulting services ➢ Security training & best practices ➢ Risk assessment & minimize attack surface ➢ Security principles and Threat Modeling	➢ Setup & configure DevSecOps/ CICD pipeline ➢ Setup & configure security tools ➢ Source code & open-source testing & remediation guidance ➢ False positive analysis & risk assessment ➢ IaC & configuration analysis	➢ Setup & configure DevSecOps/ CICD pipeline ➢ Setup & configure security tools ➢ Runtime & API security testing & remediation guidance ➢ False positive analysis & risk assessment ➢ Vulnerability management	➢ Penetration testing ➢ Setup & configure security tools ➢ Security testing & remediation guidance ➢ False positive analysis & risk assessment ➢ Vulnerability management ➢ Container security assessment	➢ Vulnerability management & remediation of open vulnerabilities ➢ Ongoing security testing ➢ Ongoing application protection – setup, configure and manage ➢ Track & improve security posture ➢ Compliance monitoring ➢ Dashboards and reporting

Sample Tools

Fortify, WhiteHat Security, Fortify, invicti, AppScan, KENNA Security, ThreadFix, Vault, CloudCheckr
Microsoft, CHECKMARX, VERACODE, Burp Suite, tenable, Qualys, DEFECTDOJO, WIZ, ArmorCode
ThreatModeler Security Starts Here, BLACKDUCK by synopsys, OWASP, aqua, RAPID7, WIRESHARK, Fortify, VERACODE
SECURE CODE WARRIOR, HackEDU, sonatype, CONTRAST, CodifiedSecurity, Twistlock, CHECKMARX, SYNOPSYS
IriusRisk, dependency track, snyk, kiuwan, TRACEABLE, metasploit, aqua, Twistlock

Third-Party Risk Management (TPRM)

"...Implement a proactive, end-to-end vendor cyber risk management program across an enterprise..."

- Large 3rd party non-compliance backlog
- Audit non-compliance
- Un-acceptable exposure
- Low stakeholder confidence
- Manual processes
- Lack of scalability
- Siloes

Areas of concerns

- InfoSec Accountability
- Effective Policies & Processes
- Security Controls
- Cyber Attack Surface Strength
- Stable Cyber Posture Trend
- End-user Awareness & Training
- Regular Monitoring

Mphasis TPCRM

Onboard	Specialist team
Tier & Classify	Hybrid, Factory model
Assess	Risk Management Platform
Report Risk	Risk Intelligence For Exposure Visibility
Remediate	Monitor

Value proposition

- Specialists team & Client university
- Scalable to Bus Cycles
- InfraGenie – TPRM Platform
- Workflow driven, Persistence
- Pre-built checklists for NIST, ISO

Risk intelligence for continuous 3rd party monitoring and proactive & rapid exposure/ Vuln response

- Monitor vendors for Internet facing supplier exposure
- Rapid assessment of Zero Day exposure across supply chain
- SW supply Chain intelligence (auto discovery): OEM/Product/ Shadow IT discovery
- Vendor concentration discovery

30% FASTER

45% COST EFFICIENT

60% REDUCTION IN EXPOSURE

Best practices

NIST SP 800-53

ISO 31000

Partners

Security Scorecard

GRX

servicenow

MetricStream

Powered by TRAC.AI

Cloud Security Services

Increase ROI

Optimize security tools to deliver best outcomes

Improve Collaboration

Enable faster decision making and deliver consistency and Improve Productivity

Drive Innovation

Reduce time spent on mundane task and drive eco system towards business enablement

Assessment

- Cyber Security Maturity Benchmarking Assessment
- IT Process assessment
- Tech Stack analysis
- Vulnerability assessment and penetration testing

Sec Ops

- EDR
- Vulnerability Management
- Identity Security
- Data Security
- Key Management
- Container Security
- Application Security
- Email Security
- Configuration Management

Monitoring

- Security Monitoring
- Alert Management
- Managed Detection & Response
- Deep and Dark web Monitoring
- Take down service
- Threat Intelligence
- Threat Hunting

Governance

- Security Governance
- Technology Risk Assessment
- Third Party Risk Management
- Security Awareness
- Compliance Assessment
- Disaster Recovery
- Policies & Regulations

Data Security

Data-Centric Security Model	• Instead of solely protecting networks and endpoints, organizations must secure data at its source, whether at rest, in transit, or in use. • Encryption, tokenization, and rights management , Data Discovery and Classification DLP are critical for safeguarding sensitive information. • Aligning controls with frameworks like NIST, ISO 27001, and Zero Trust Architecture to ensure a layered defense.
Zero Trust & Least Privilege Access	• Zero Trust security models enforce continuous verification, ensuring that access is granted based on identity, behavior, and context rather than implicit trust. • Identity-Centric Security: Strong authentication via MFA, conditional access, and Just-In-Time (JIT) privilege elevation.
Compliance as a Baseline, Not a Strategy	• Regulations like GDPR, CCPA, and HIPAA mandate baseline controls, but compliance does not guarantee security. • Organizations must go beyond compliance to adopt a risk-based approach, continuously monitoring and refining data protection strategies. • Automated compliance reporting and governance solutions can reduce audit burdens and strengthen security
Human-Centric Security & Insider Risk Management	• Employees are often the weakest link in data security. security strategies must address insider threats, privilege misuse, and accidental data exposure. • Behavioral analytics, security awareness training, and automated risk-based access controls can mitigate insider threats
AI-Driven Security and Automation	• Detecting anomalies in data access patterns to prevent insider threats. • Adaptive Security Policies: Using machine learning to adjust access control dynamically based on user risk profiles.

Overall Impact

Better Regulatory Compliance & Reduced Legal Risks

Reduced Data Breaches

Future-Proof Security Strategy with Automation & AI

Case Studies

IAM Remediation Program - a Multinational Bank

IAM Remediation Program

CUSTOMER

Customer is an American multinational investment bank and financial service company

SCOPE OF WORK

- Evaluate questionnaire responses and discovery session outcomes to determine application entitlement alignment to IAM Privileged Access definition.
- Develop remediation plans and socialize with relevant stakeholder teams
- Conduct impact assessment on “non-compliant” applications and distribute remediation communications and support FAQs
- Validate compliance after Application team completes remediation

TOOLS/ PLATFORM/ BEST PRACTICES/ STANDARDS

- Oracle Identity Management Solution

BUSINESS CHALLENGE

- Customer wanted to remediate Privileged and Elevated access given to end user on the application landscape with the customers organization for meeting the over program timelines.

MPHASIS SOLUTION

- Design Thinking-Led Agile Approach: Our approach brings the full expertise of Mphasis together, setting the stage for scalable remediation through targeted accelerators and focused application onboarding.
- Automation-First Mindset: Leveraging Mphasis IAM process accelerators to streamline creation, management, and tracking for effective remediation and seamless application onboarding.
- Day 1 Ready - Efficient, Staggered Squads : High-efficiency squads working in parallel tracks, featuring a well-balanced team of IAM Specialists to ensure robust, skilled, and scalable delivery from the outset.
- Continuous Backlog Management: Ensuring a continuous backlog throughout the project lifecycle to drive sustained progress.
- Focused Governance and Tracking Mechanisms: Strong governance oversight for precise tracking and accountability.
- Value-Driven Pricing and Commitment: A fixed fee model, excluding add-on discount for volume and early payment. Mphasis is also investing a percentage in Cyber COE, buffer resources, and governance oversight to drive program success.

CUSTOMER BENEFITS

- Identity Security CoE infused with strong technology enablement
- In-house Identity Security innovation labs
- Pool of Identity Security Architects and Consultants to digitally transform businesses, cut complexity and cost, improve customer service and drive growth
- Strategic OEM partnerships with Leading IAM Product partners
- Dedicated research & development centers enabling us to deliver impactful, next-gen IAM solutions
- Innovate with low code development and automated processes

Third-Party Cybersecurity Risk Management – a Private Equity Company

Third-Party Cybersecurity Risk Management

CUSTOMER

Client is an American private equity company headquartered in New York City. It is one of the oldest private equity investments firm in the world.

SCOPE OF WORK

- Third-Party Cybersecurity Risk Management assessments using CyberGRX/ BitSight or manual questionnaire
- Review/ validate responses and submitted evidence against customer standards
- Document findings, support material and recommendations
- Reporting

TOOLS/ PLATFORM/ BEST PRACTICES/ STANDARDS

- CyberGRX
- MS SharePoint
- Customer due diligence questionnaire
- BitSight

BUSINESS CHALLENGE

- Timely completion of Cybersecurity risk assessments of existing and potential vendors
- Achieve organizational efficiency by managing third-party risk assessment proactively
- Ensure compliance and governance requirements are met and mitigate vendor risks
- Reduce effort in manual process of risk assessment and bring in automation

MPHASIS SOLUTION

- Gather vendor information from customer
- Prioritize vendor assessments based on the urgency
- Check if Cyber assessment report is available on GRX for the vendor and complete the assessment
- For vendors where report is not available on GRX, share them the manual customer DDQ and request for responses
- Setup meeting with vendors and stakeholders to explain the scope and timelines of assessment
- Prepare and share the assessment plan and request for initial artifacts
- Co-ordinate with vendors for additional evidences or responses to complete the assessment
- Conduct assessment based on GRX report or Due diligence questionnaire shared (DDQ) and response/ evidence/ artefacts shared
- Discuss and share the final report with Customer

CUSTOMER BENEFITS

- Vendor assessments are evenly spread out across the year and assessed frequently
- Prioritize vendor assessments
- Timely assessment responses from the vendors to ensure assessment timelines are met
- Timely responses to feedback and report review requests
- Ensure compliance and governance requirements are met and mitigate vendor risks

Microsoft Azure Security Services – a Private Equity Company

Microsoft Azure Security Services

CUSTOMER

Client is an American private equity company headquartered in New York

SCOPE OF WORK

- Gap assessment of security policies and controls
- Design, build and improve customer's security posture and Azure cloud security setup
- Azure security and compliance support
- Coverage of the entire Microsoft 365 E5 suite - IAM, MDM/MAM, device encryption, email security, endpoint security, and data security

TOOLS/ PLATFORM/ BEST PRACTICES/ STANDARDS

- Microsoft 365 E5 suite, including Entra ID, Intune, Exchange Online Protection, Defender, and Purview

BUSINESS CHALLENGE

- Customer is in the initial stages of implementing Microsoft Azure security and needed help to assess current controls, make recommendations and assist in the configuration of those recommendations to achieve sustainable security improvements
- Coverage of the entire Microsoft 365 E5 suite and develop a phase wise implementation plan

MPHASIS SOLUTION

- Discover current architecture, infrastructure, applications, and business data being consumed
- Review current security policies across the landscape of Azure and M365
- Review the current issues report by Microsoft compliance portal
- Perform a gap assessment of the current control set against Microsoft Secure Score
- Identify dependencies and document required policy updates
- Assessment and policy updates to improve security score
- Enforcing security policies, best practices, and compliance standards (e.g., CIS, GDPR) within Azure
- Microsoft Purview discovery and initiation for DLP setup
- Phase wise Implementation plan which comprises relevant control testing, client sign-off, policy updates requirements and communications with mutual agreement with the customer

CUSTOMER BENEFITS

- Detailed report that summarizes the findings, gaps, risks, and recommendations for improvement
- Compliance and governance requirements are met and mitigated vendor risks
- Setup security policies, best practices, & compliance standards
- Improved security posture
- Documented security controls and the end use impact
- Microsoft Security Controls Framework

Application Security Testing – a US Investment Bank

Dynamic Application Security Testing and Manual Penetration Testing

CUSTOMER

Client is an American Investment banking services holding company headquartered in New York City

SCOPE OF WORK

- Ongoing dynamic security testing for in scope applications
- Support application development teams to review and remediate vulnerabilities detected during application security testing
- False positive checks to validate identified vulnerabilities

TOOLS/ PLATFORM/ BEST PRACTICES/ STANDARDS

- Burp Suite
- HCL AppScan
- Manual scans - Postman, Nmap or Fiddler
- Jira
- Insomnia
- SoapUI

BUSINESS CHALLENGE

- Support scan issues, improve scan quality & improve coding practices
- Manage high volume of bug tracker tickets & improve the security testing process
- Improve security knowledge of the development teams

MPHASIS SOLUTION

- Review associated Jira tickets for new scan or re-scan requests
- Work with development team to acquire required credentials for scanning
- Schedule the dynamic scans
- Execute automated scans utilizing AppScan Std.
- Validate findings utilizing Burp Suite to confirm true positives
- Perform specific manual scans using Postman, Nmap, Fiddler or similar tools
- Issue the report to development, after all vulnerabilities have been entered into Jira.
- Provide guidance to development teams to understand and remediate any vulnerabilities detected by the scanning tools
- Continue to support the application development team till the vulnerability is remediated and verified through a dynamic analysis re-scan by providing remediation recommendations and walking them through the remediation

CUSTOMER BENEFITS

- Able to identify and fix security issues before release
- Security issues awareness increased among development team (100% coverage)
- Due to continuous pre-testing and code analysis, the security posture of the products has increased
- Improved vulnerability analysis and reporting

Mphasis Compliance Management Practices

Mphasis has industry-wide experience in developing technology solutions, developing safety-critical applications, streamlining IT infrastructure, and is accredited with ISO 9001, Cyber Essentials, CMMI Level 5. Mphasis has a wide experience working with different government bodies in the UK. Our work with the Public Sector organisations helps them align with best practices and use Government Digital Service Standards to deliver Digital Services and follow NCSC Cloud Security Principles in all our cloud engagements.

Mphasis demonstrates robust compliance and governance practices through:

Quality and SLA Adherence:
Clear metrics and SLAs for response times, ticket resolution, customer satisfaction, cost management, and resource retention.

Security Compliance:
Implementation of required controls to comply with client information security requirements, such as those specified by Huawei.

Risk Management:
Detailed risk identification and mitigation plans covering process, people, knowledge transfer, infrastructure, and resource management risks.

Knowledge Management:
Emphasis on effective knowledge transfer, documentation, and validation to ensure compliance and minimize operational risks

Delivery Governance:
Structured reviews at multiple organizational levels (from President Global Delivery to individual managers) with regular frequency (quarterly, monthly, weekly, and as part of appraisal cycles).

Change and Incident Management:
Standardized ITIL v3 processes, change control boards, incident lifecycle management, and continuous service improvement initiatives.

Mphasis Compliance Management Practices (Continued)

Certifications Supporting Compliance

ISO 9001:2015 – Quality Management Systems

ISO/IEC 27001:2013 – Information Security Management

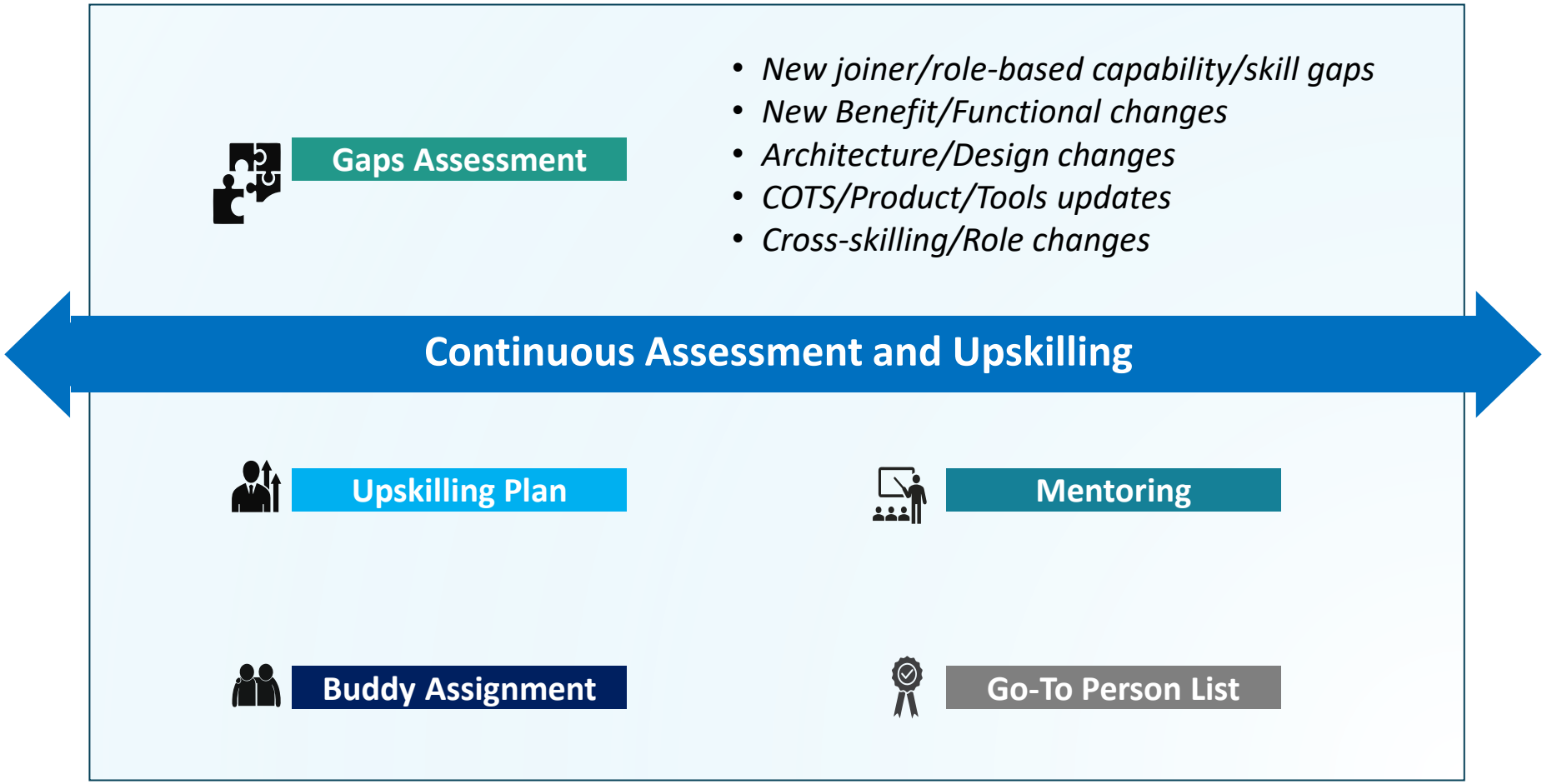
ISO 14001:2015 – Environmental Management Systems

ISO 45001:2018 – Occupational Health & Safety

ISO/IEC 20000-1:2018 – IT Service Management

Continuous Capability and Skill Management

To achieve the overall supplier objective, we will conduct orientation programmes to ensure the alignment of onboarded resources to the business need. Along with the formal knowledge building/transfer sessions, we will ensure informal team building/social sessions (along with the buyer's team) to get to know one another and facilitate interaction.



Service Levels and SLAs, Accreditation at Mphasis

Service Levels and SLAs at Mphasis are designed to ensure predictable, high-quality service delivery backed by clearly defined performance, availability, and support commitments. Mphasis' managed services framework outlines structured service levels—including performance metrics and support-hour definitions—to maintain operational consistency and reliability for clients. Their strong SLA governance is demonstrated through real-world outcomes, such as helping a global insurance firm achieve 100% SLA compliance while simultaneously reducing ticket incidents and improving operational efficiency through automation and application modernization. These practices reflect Mphasis' focus on measurable service quality, proactive management, and continuous improvement aligned with customer expectations

Accreditations

Mphasis holds several globally recognized accreditations that underscore its commitment to quality, security, and responsible innovation. The company is accredited with the ISO/IEC 42001:2023 certification for Artificial Intelligence Management Systems (AIMS), issued by TÜV SÜD South Asia and accredited by the National Accreditation Board for Certification Bodies (NABCB), reinforcing its leadership in responsible and trustworthy AI practices. Mphasis is also certified under ISO/IEC 27001:2022, demonstrating its robust information security management across ICT services, cloud infrastructure, data centres, and global business operations. Additionally, the company maintains ISO 9001:2015 Quality Management System certification through DNV, validating its adherence to high-quality service delivery across applications, BPO, and infrastructure services globally. Together, these accreditations highlight Mphasis' strong governance, operational excellence, and dedication to meeting rigorous international standards.

Service Levels and SLAs at Mphasis (Continued)

Integrated SLAs:

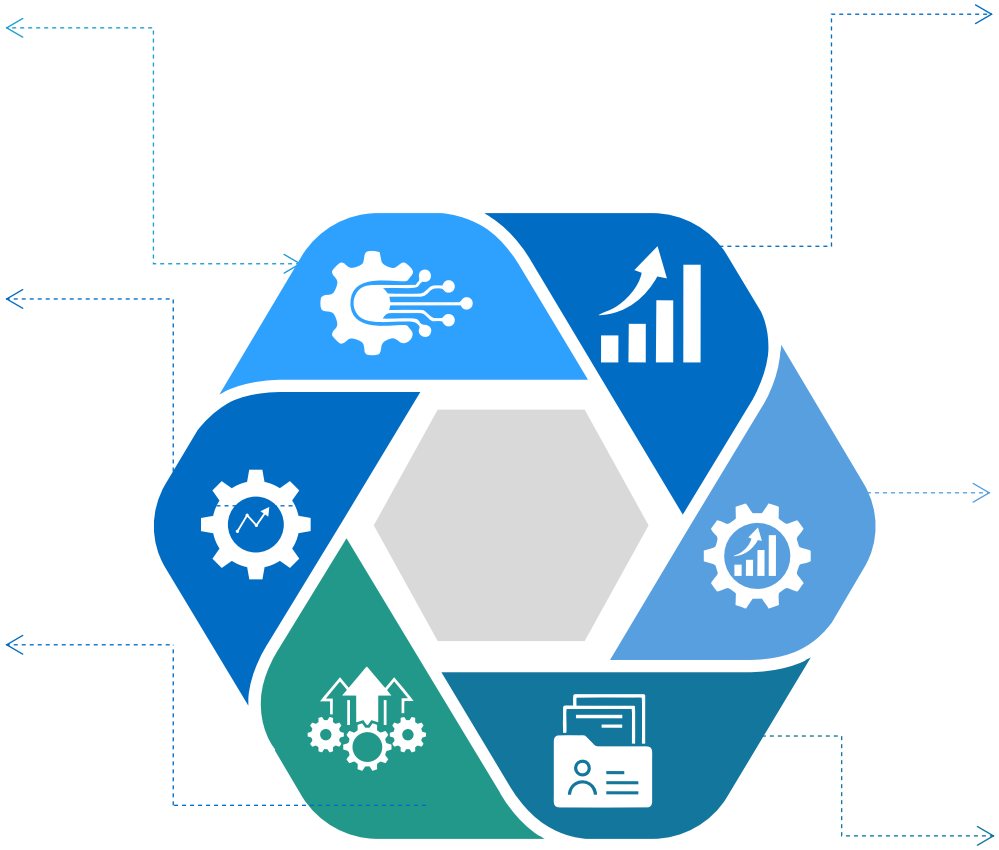
Mphasis implements integrated Service Level Agreements (SLAs) across L1, L2, and L3 support levels, ensuring comprehensive coverage for various support tiers.

KPI-Driven Service Management:

The company sets clear Key Performance Indicators (KPIs), such as creating a joint model to calibrate and estimate changes by the third month, and managing yearly support goals with monthly engagement reviews. Support tickets and enhancement goals are managed with a target of at least 80% being handled by Mphasis.

Operational Excellence

Mphasis emphasizes operational excellence through established frameworks for predictable outcomes, including forecasting, capacity planning, reporting, analytics, talent onboarding, and ticket life cycle management.



Performance Metrics: Examples of achieved metrics include:

- First Contact Resolution rates as high as 87%
- Abandoned call rates below 1% for phone and below 5% for chats
- MTTR (Mean Time to Resolution) improved from 59 hours to less than 4 hours
- Cost per ticket reduced by 30%
- Contact reduction by 30% post-automation
- Password reset elimination by 70%

Continuous Improvement:

Mphasis aligns with client objectives through LEAN methodologies, tools, automation, and continuous improvement initiatives, supporting delivery excellence and predictable, output-based pricing models

Portfolio Analysis:

The company conducts holistic application portfolio analysis, mapping business and IT objectives to deliver actionable roadmaps for transformation and optimization, with a typical analysis duration of 3 to 6 weeks depending on portfolio size and data readiness.

Contact Us

Further Information: For more information about our G-Cloud services, **please contact our Public Sector Team at mphasisukps@mphasis.com**

Thank You!

For more information, please contact:

About Mphasis

At Mphasis, engineering has been in our DNA since inception.

Mphasis is an AI-led, platform-driven company with human-in-the-loop intelligence, helping global enterprises modernize, infuse AI, and scale with agility. The Mphasis.ai unit and Mphasis AI-powered 'Tribes' are focused on client outcomes and embed artificial intelligence and autonomy into every layer of the enterprise technology and process stack. Mphasis built NeoIP™, a breakthrough AI platform that orchestrates a powerful pack of AI solutions and platforms to deliver impactful outcomes across the enterprise IT value chain, as we believe ***'AI Without Intelligence Is Artificial™'***. Mphasis NeoIP™ is powered by the Ontosphere, a dynamic and ever-evolving knowledge base, delivering continuous and constant innovation through perpetual intelligent engineering—driving end-to-end enterprise transformation.

At the heart of our approach is customer-centricity—reflected in our proprietary Front2Back™ transformation framework, which uses the exponential power of cloud and cognitive to deliver hyper-personalized digital experiences ($C=X2C^{2}_{TM}=1$) and build strong relationships with marquee clients. Our Service Transformation solutions enable enterprises to pivot from legacy systems and operations to secure, adaptive, cloud-first operating models with minimal disruption. Continuous investments in platforms, such as the Neo series, enable enterprises to stay efficient, relevant, and ahead in a dynamic AI-first world. Mphasis is a Hi-Tech, Hi-Touch, Hi-Trust company, rooted in a learning and growth culture. Click here to know more. (BSE: 526299; NSE: MPHASIS)

Important Confidentiality Notice