2022

Technical Proposal

Tender No: BPD/2022/RFQ-1442

Technical Proposal For Vulnerability Assessment And Penetration Testing ERP And Non-ERP Applications, Cloud Infrastructure And Network Assessment

Submitted To:	**BRAC Enterprise** BRAC Centre, 75 Mohakhali, Dhaka-1212, Bangladesh
Submitted By:	**Technuf limited** High Tower, 9th Floor, 9 Mohakhali, Gulshan, Dhaka-1212

Contents

1 Technuf Limited

1.1 Company Profile

Technuf is a Dhaka based company providing leading-edge and proven technologies, industry vertical domain expertise and highly skilled and motivated professionals to achieve our customers' mission critical business needs.

We have been singularly focused on achieving customer success and have been rewarded with repeat engagements. We are uncompromising in our quest for delivering the best value and quality that meets and exceeds customers' expectations. Technuf offers a partnership based on knowledge sharing and skill transfers that provide complementary set of capabilities with its partners. Technuf has a global reach of highly skilled professionals able to dynamically assert in problem solving and solution crafting at an extremely competitive cost structure.

- **What We Offer**

Technuf is committed to its employees to ensure that they are highly motivated with the right skills for the job. We pride ourselves for attracting and keeping the very best the industry has to offer in the area of information technology, application development and program management support. We continuously improve our processes to provide the most cost-efficient and optimized solution to our customers. Our approach of customer first has allowed us to develop trusted relationships and organically grow within each one of our engagements.

- **Core Values**

Technuf believes that customer success is built upon making every single employee successful with continuous training and mentoring to ensure that they are able to provide technical excellence in every single engagement. Customer and Employee success are inextricably linked. We attract the very best the industry has to offer in system engineering, software development and management. Our core measurement for employees is their ability to make customers successful. We encourage all employees to maintain a sustainable balance between their work and personal lives. We are here for the long term and want to ensure that our employees are able to provide continuity of their service.

- **Vision and Mission**

Technuf becomes a market leading and professionally recognized provider of Information Technology related products and services as part of a comprehensive solution.

Technuf's mission is to enable:

→ Customer success
→ Delivery of Cost-efficient and optimized solution
→ Empowerment of employees
→ Social responsibility

1.2 Certifications

Technuf understands the standards and requirement of governmental systems in accordance with Section 508 and all other standards. We have implemented multiple government projects successfully and therefore graced with the prestigious certifications. We strive to maintain the quality and standards without any compromise.

ISO :2007-2015	

Global Certification Services LLC

Certificate of Registration

GCS LLC hereby certifies that the organization

Technuf, LLC

12850 Middlebrook Road, Suite 306,
Germantown, MD 20874

Has established and applies a Quality Management System in accordance with

ISO 9001:2015

For the scope of activities :

End to end Software Engineering cycle. Business Analysis, Requirements Gathering, Requirements Analysis & Design, Architecture, Implementation, Quality Assurance, deployment, Operations & Maintenance. Cybersecurity, Software Development, Business Intelligence & Big Data Analytics, Program & Project Management Support. Mobile Application Development as well as Web application development.

Certificate Number : GCQ-171005

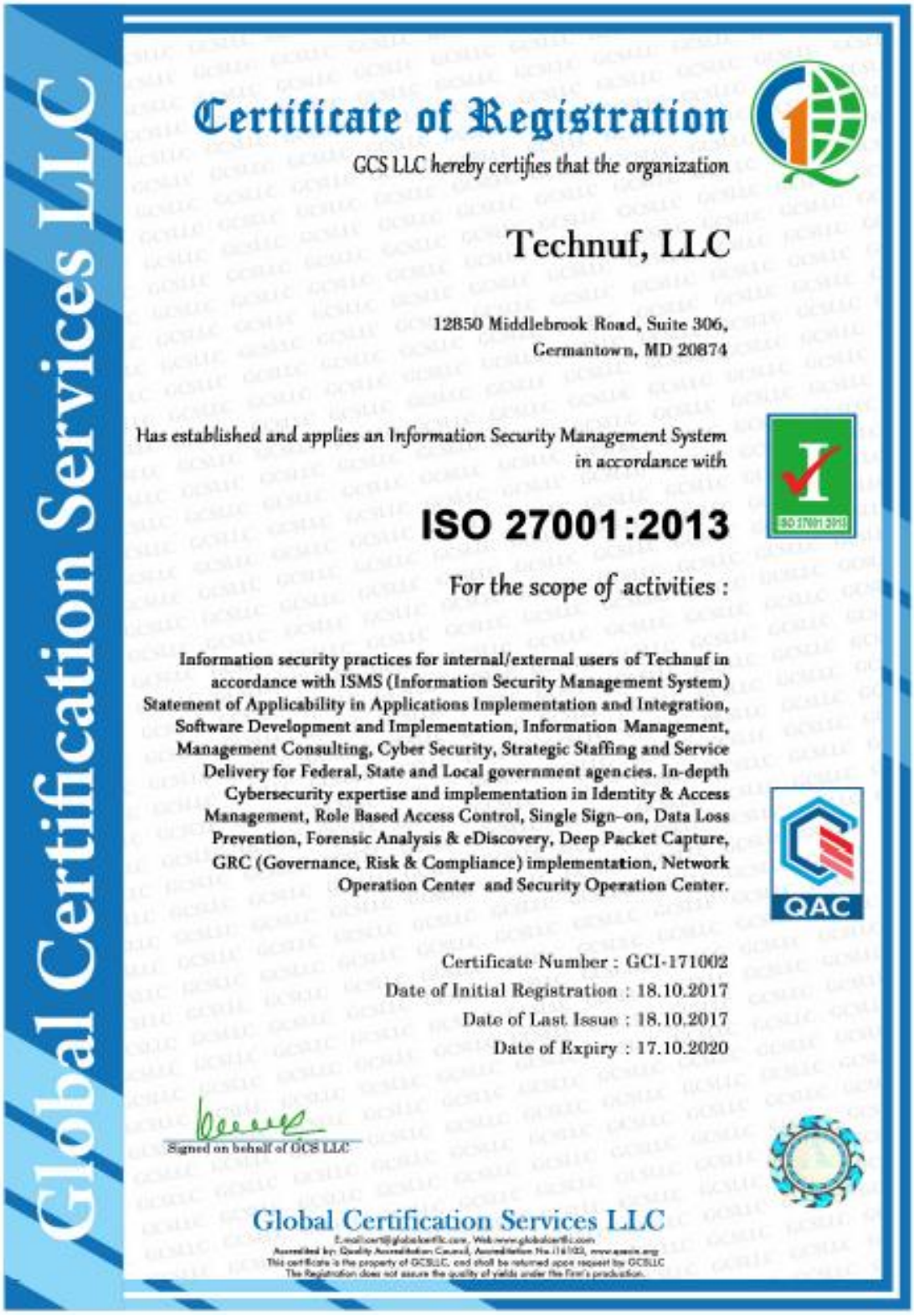
Date of Initial Registration : 18.10.2017

Date of Last Issue : 18.10.2017

Date of Expiry : 17.10.2020

Signed on behalf of GCS LLC

Global Certification Services LLC


Global Certification Services LLC
Certificate of Registration
GCS LLC hereby certifies that the organization
Technuf, LLC
12850 Middlebrook Road, Suite 306,
Germantown, MD 20874
Has established and applies an Information Security Management System in accordance with
ISO 27001:2013
For the scope of activities :
Information security practices for internal/external users of Technuf in accordance with ISMS (Information Security Management System) Statement of Applicability in Applications Implementation and Integration, Software Development and Implementation, Information Management, Management Consulting, Cyber Security, Strategic Staffing and Service Delivery for Federal, State and Local government agencies. In-depth Cybersecurity expertise and implementation in Identity & Access Management, Role Based Access Control, Single Sign-on, Data Loss Prevention, Forensic Analysis & eDiscovery, Deep Packet Capture, GRC (Governance, Risk & Compliance) implementation, Network Operation Center and Security Operation Center.
QAC
Certificate Number : GCI-171002
Date of Initial Registration : 18.10.2017
Date of Last Issue : 18.10.2017
Date of Expiry : 17.10.2020
Signed on behalf of GCS LLC
Global Certification Services LLC

1.3 Product and Services with Emerging Technology

- Cyber Security
  - Zero Trust Security Model
  - Intrusion detection
  - Forensic Analysis and Discovery
  - Authentication and Authorization
  - Identity and Access Management
  - Data Loss Prevention
  - Advanced Persistent Threat (APT)
  - Counter Intelligence
  - User Behavior Analytics (UBA)
- Business Intelligence
  - Artificial Intelligence (AI)/Machine Learning (ML)
  - Robotics Process Automation (RPA)
  - Intuitive Innovative Visualization
- Mobile Application Development
  - IOS Development
  - Android Development
  - Business Intelligence Apps
  - Multi-platform Support
  - Development, Deployment, Operation
- Software Engineering and SDLC Automation
  - Risk Driven
  - Agile
  - Industry Best Practices
  - CICD/Devops

1.4 Technuf's Core Capabilities

Cybersecurity

- Intrusion Detection (IDS)
- Intrusion Prevention (IPS)
- Penetration Testing
- Vulnerability Assessment
- Security Operations Center (SOC)
- Governance and Compliance
- Security Audit - PCI, SAS, NIST
- Forensic Analysis and eDiscovery
- Data Loss Prevention (DLP)
- Privileged Access Management (PAM)
- Authentication/Authorization
- Single Sign-on (SSO)
- Role Based Access Control (RBAC)
- Deep Packet Capture
- Insider Threat Detection/Prevention
- Advanced Persistent Threat (APT)
- Cyber Threat Intelligence (CTI)
- Secure communications
- Certification & Accreditation
- Risk Assessment & Security Planning
- Cybersecurity Training
- Identity and Access Management (IdAM)

Software Engineering and IoT

- Business and requirements analysis
- Architecture management
- Detailed design, implementation, and integration
- Multi-tiered architecture with mobile clients
- Complex real-time incidence response systems
- Safety critical applications
- Real-time solutions
- Fault-redundant systems
- Mission critical applications
- Functionality Testing
- Performance Testing
- Usability and Accessibility (508)
- Customer Acceptance Testing

CMMI Appraisal

- Our in-house team of qualified High Maturity Assessment Team Members (ATMs) conduct CMMI certifications with Third Party partner company,

Business Intelligence

- Interface with unstructured data
- QlikView Business Discovery platform & ETL
- Denormalization, Tagging & Standardization
- Data Warehousing Adapters
- Data Mining
- Advanced Analytics
- Statistical Inference
- Real-time reporting & Alerts

Management Approach

- SDLC and Agile Management
- PMBOK-based best practices
- Requirements management
- Resource management
- Communications
- Risk Management
- Change Management
- Training
- Asset Management
- Scheduling
- Budget and status monitoring + reporting

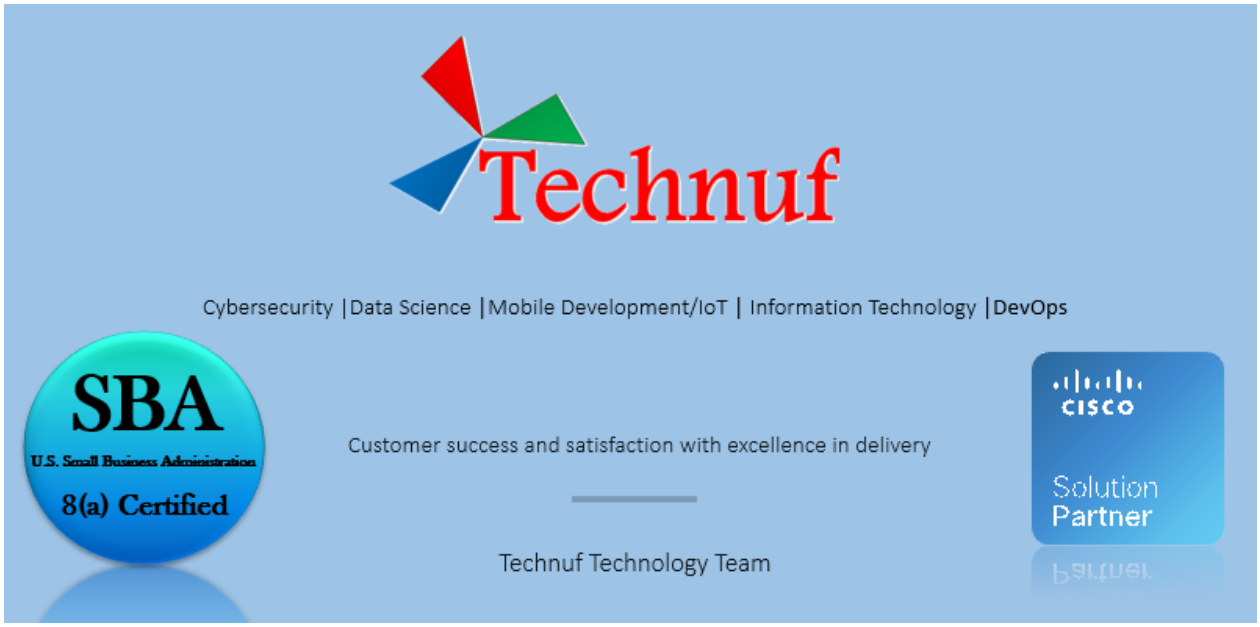
Transportation Tracking System

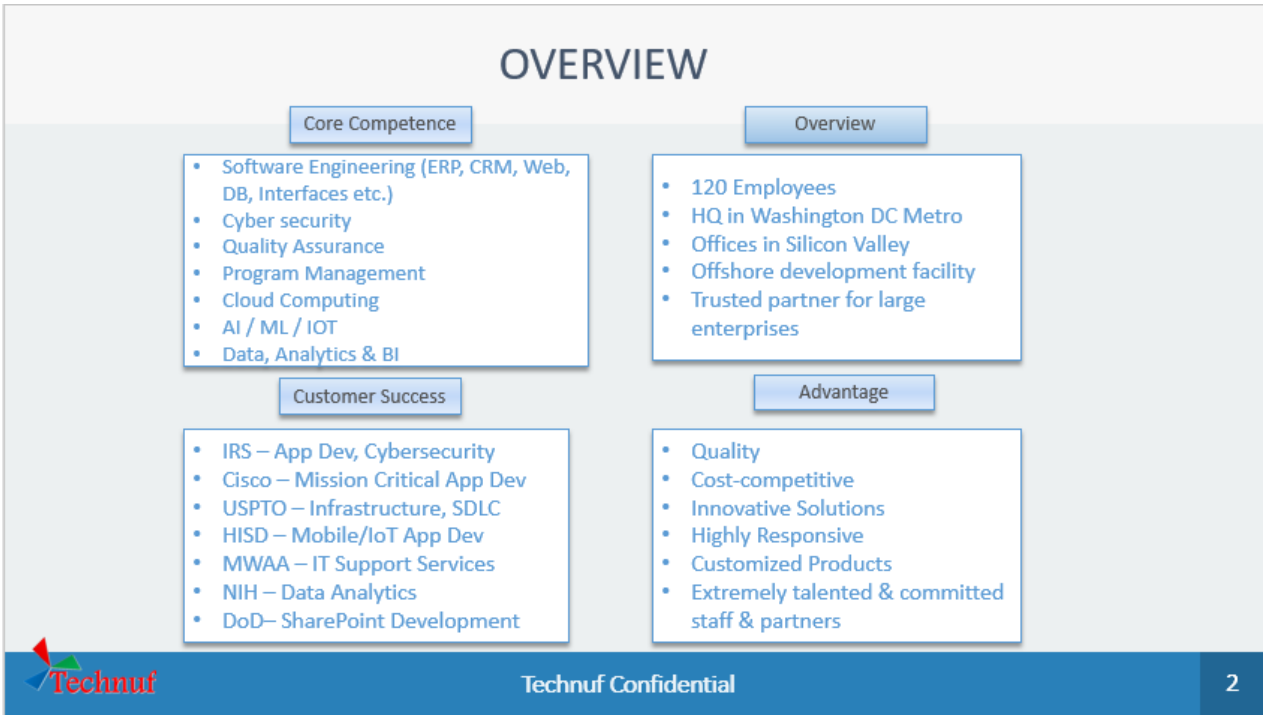
- Child Attendance, Safety and Tracking
- Dispatch and Collaboration System
- Emergency Alert Response System
- Referral Management Method

Health Connect

- Centralized automated system for health care professionals
- EMedNY Integration
- Offline Mode
- Quick Assessment
- Medicaid ID Validation
- Calendar Notification

1.5 Brochure of Technuf





Technuf Certifications

- SBA 8(a)
- GSA IT Schedule 70
- MBE (Minority Business Enterprise)
- SBE (Small Business Enterprise)
- DBE (Disadvantaged Business Enterprise)
- LDBE (Local Disadvantaged Business Enterprise)
- VA SWaM (Small, Women-owned, and Minority-owned Business (SWaM)
- Cisco ATP (Authorized Technology Provider)
- GS PSS (Global Supplier)
- ISO 9001
- ISO 27001
- CMMI Level 3 Certified

Technuf Advantages

Skilled	Scalable	Trusted
• Staff competency and expertise • Supports complex and high visibility projects	• Proven, scalable staffing model with quality retention • Client-partnership and client-advocate strategic approach	• Multiple high-visibility enterprise-wide projects • High customer satisfaction • Account growth

People: Our pledge to our associates' satisfaction allows for high retention rates of our highly skilled associates.

Processes: Our commitment to cost-effective solutions, transparency, and continuous knowledge sharing allows for ongoing process improvements. We are committed to CMMI and ISO 9001 standards.

Customer Satisfaction: This has been the singular most important factor contributing to our past growth.

Where we work

- Internal Revenue Service (IRS)
- DoD (Department of Defense)
- National Institute of Health (NIH/NIDDK)
- U.S. Department of Commerce (DoC/USPTO)
- Metropolitan Washington Airport Authority (MWAA)
- Cisco Systems
- Huntsville Independent School District
- DC Public School
- Presidio
- DISYS
- Davra Networks
- Tait Communications
- Grameen Phone
- Yoga Alliance
- ORA

Service Offerings

S/W Engineering	Program Management	O&M
• ERP, CRM, Web, DB and DI Applications • Big Data Analytics & BI • Cloud Computing • Mobile • Social Media • Cyber Security • VoIP/Collaboration • IoT App Dev • AI / ML	• Project & Program Management • Enterprise Lifecycle Management • Estimation and Budgeting • Training/Mentoring	• Infrastructure O&M • Tier 1, 2, & 3 desktop support • Disaster recovery • Virtualization and private cloud system support

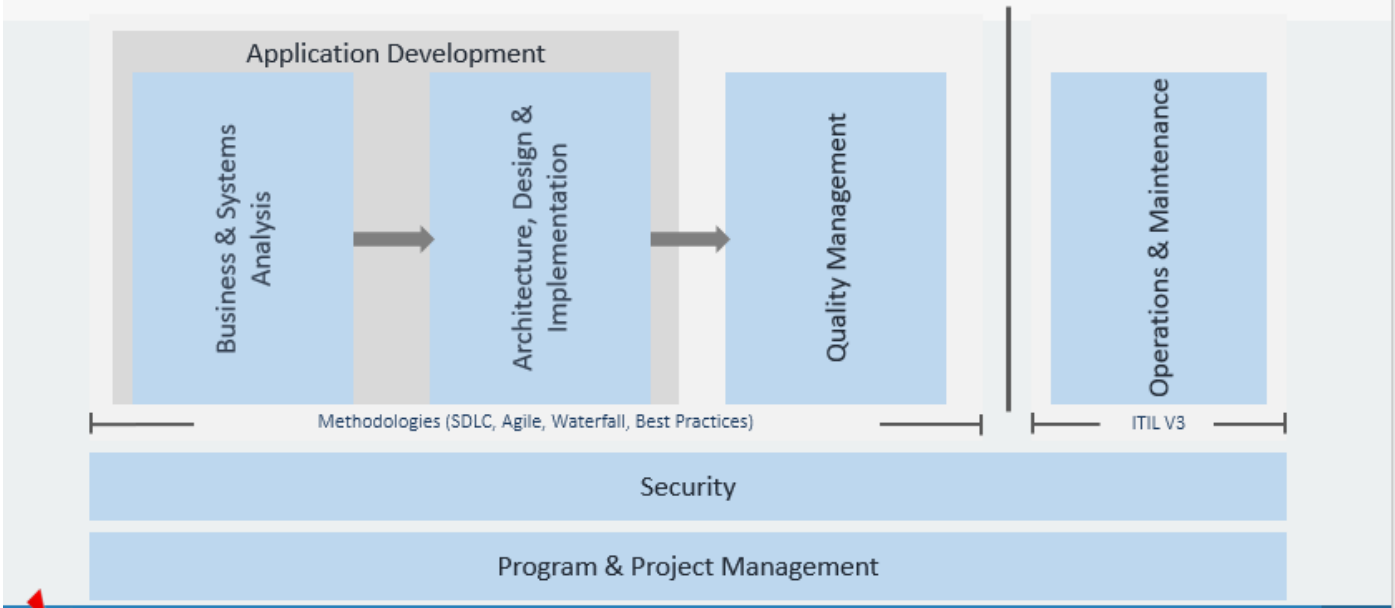
Approach

- Industry best practices
- Agile
- CMMI
- Six Sigma
- Customer adopted SDLC
- Continual development cycle
- Distributed development

- PMBOK-based best practices
- Deliver on-time within budget

- SLA driven
- 24x7 support
- Multi-tier support
- Best practices & standards
- ITIL

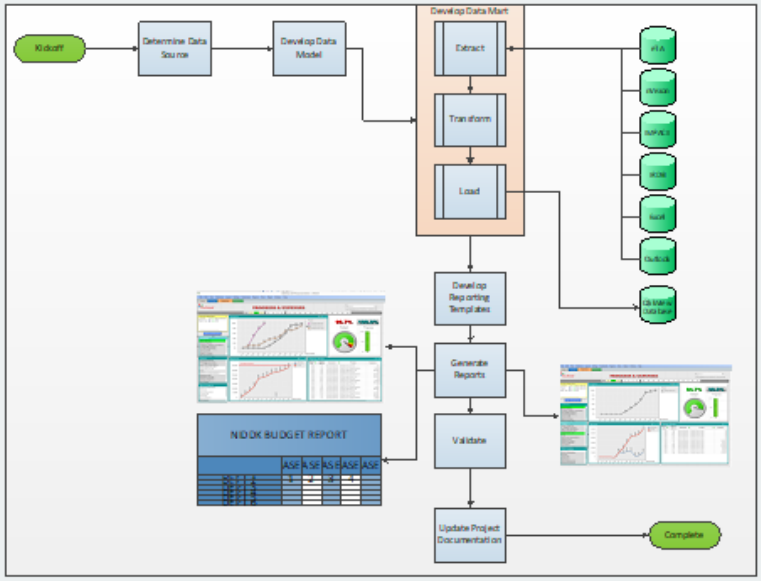
Technuf's Service Capabilities



Technuf Confidential 7

Technology Solutions for NIDDK

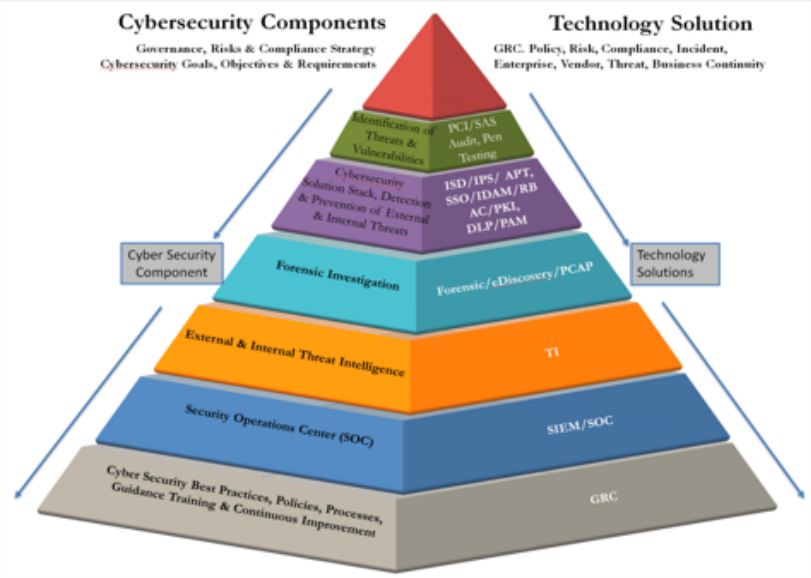
- Interface with unstructured data
- QlikView Business Discovery platform & ETL
- Denormalization, Tagging & Standardization
- Data Architecture
- Data Security
- Data Warehousing Adapters
- Data Mining
- Intelligent Search Engine
- Advanced Analytics
- Statistical Inference
- Real-time reporting & Alerts



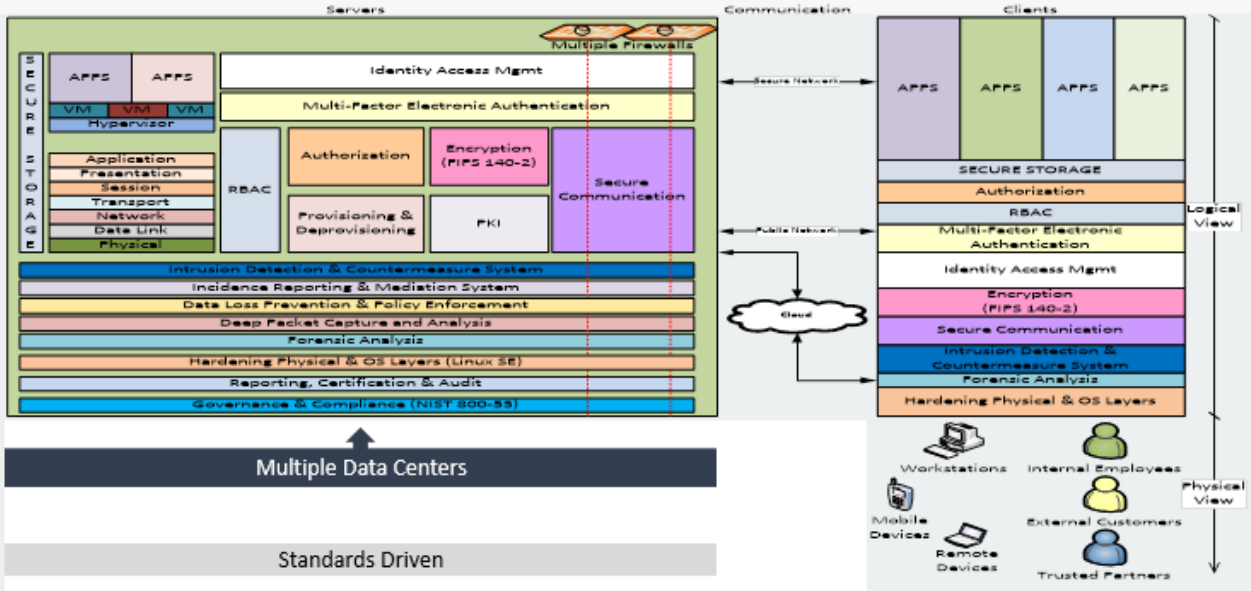
Technuf Confidential 8

Technology Solutions Mapped to Cybersecurity Components

- A cook book to checkup the health of the cybersecurity environment for an agency and the steps to mitigate any risks and vulnerabilities
- Case studies from the world's largest financial institutes (IRS) and show how we secure their IT infrastructure
- In order to protect the enterprise, the organization must take this holistic view that addresses the entire range of threats, vulnerabilities and associated remediation.



Comprehensive Approach to Cybersecurity



Needs-Driven Cybersecurity Solutions

Technuf Confidential 11

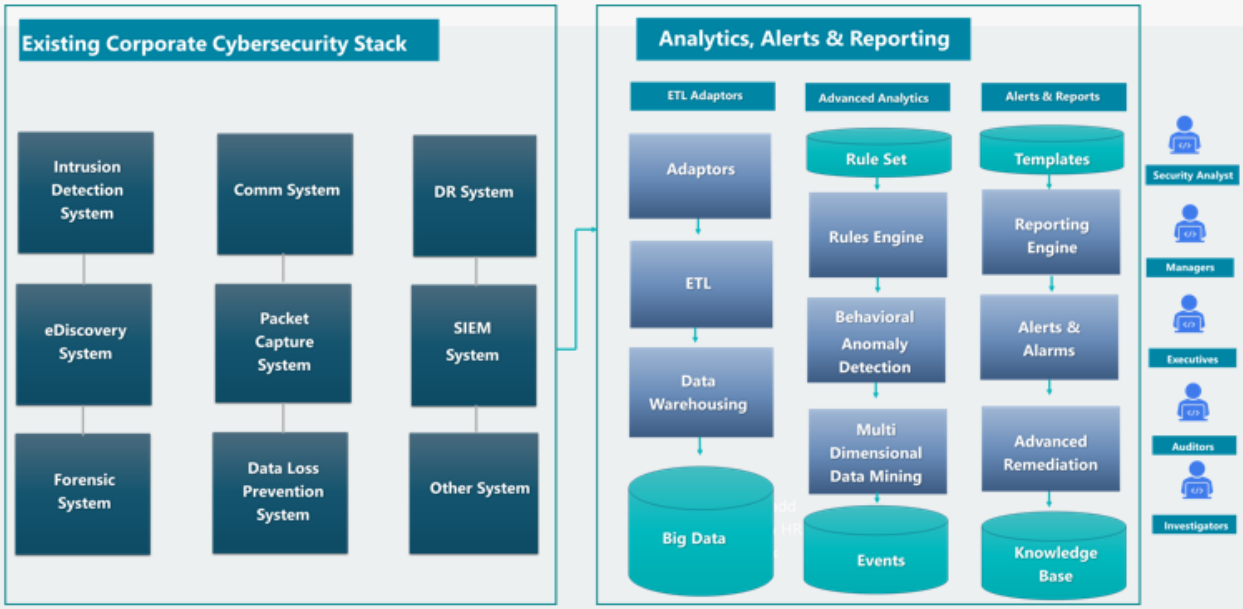
Cybersecurity risk management

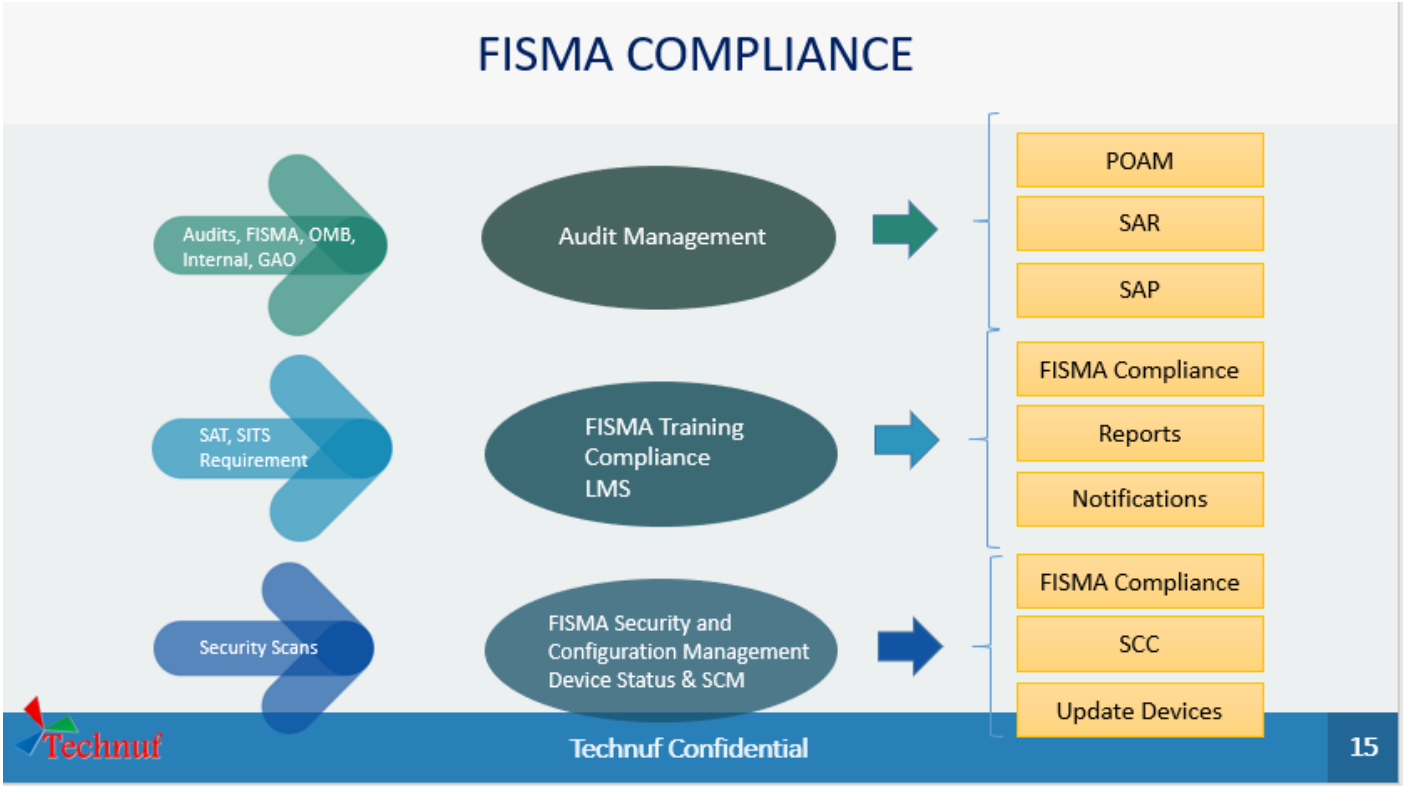
Technuf Confidential 12

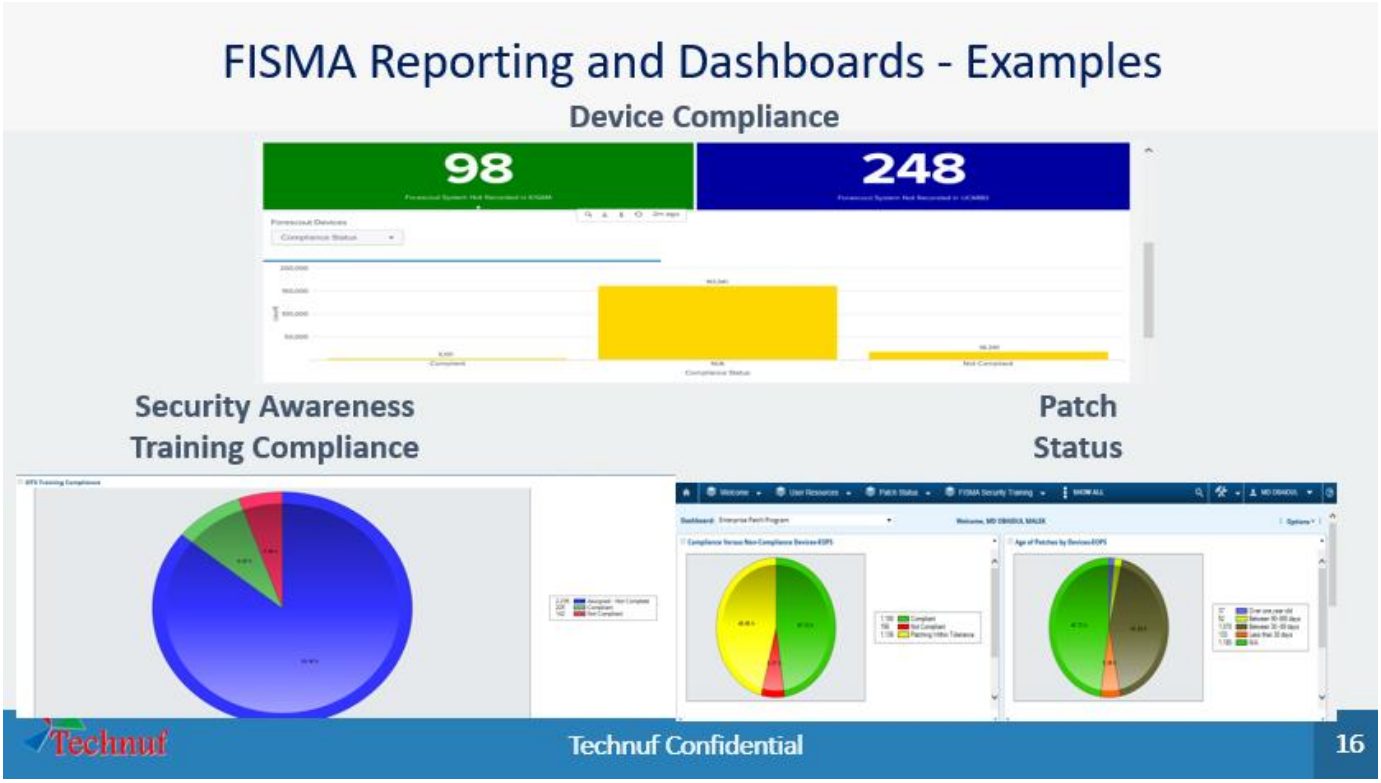
SECURITY TRAINING

1	Presentation, Video & Workbook	• Diverse Training materials for administrators and end-users.
2	Security Awareness Training	• Provide cybersecurity awareness training
3	Role Based Training	• Personalized training for personnel with elevated privileges
4	Specialized IT Security Training	• Deliver training based on emerging technologies. • Training materials support insider threat indicators, with strategic notes on implementation and mitigation best practices.

SECURITY Operations Center




FISMA COMPLIANCE
Audits, FISMA, OMB, Internal, GAO
SAT, SITS Requirement
Security Scans
Audit Management
FISMA Training Compliance LMS
FISMA Security and Configuration Management Device Status & SCM
POAM
SAR
SAP
FISMA Compliance
Reports
Notifications
FISMA Compliance
SCC
Update Devices
Technuf
Technuf Confidential
15


FISMA Reporting and Dashboards - Examples
Device Compliance
98
248
Security Awareness Training Compliance
Patch Status
Technuf
Technuf Confidential
16

Comprehensive Cybersecurity Support to our Customers

- Intrusion Detection (IDS)
- Intrusion Prevention (IPS)
- Penetration Testing
- Vulnerability Assessment
- Security Operations Center (SOC)
- Governance and Compliance
- Security Audit - PCI, SAS, NIST
- Forensic Analysis and eDiscovery
- Data Loss Prevention (DLP)
- Privileged Access Management (PAM)
- Authentication/Authorization
- Single Sign-on (SSO)
- Role Based Access Control (RBAC)
- Identity and Access Management (IdAM)
- Deep Packet Capture
- Insider Threat Detection/Prevention
- Advanced Persistent Threat (APT)
- Cyber Threat Intelligence (CTI)
- Secure communications
- Certification & Accreditation
- Risk Assessment & Security Planning
- Cybersecurity Training

Software delivery is at the heart of today's top technology trends

DevSecOps Model

Accelerate software delivery *faster time to value*

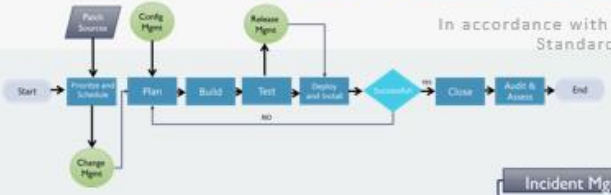
Balance speed, cost, quality and risk *increased capacity to innovate*

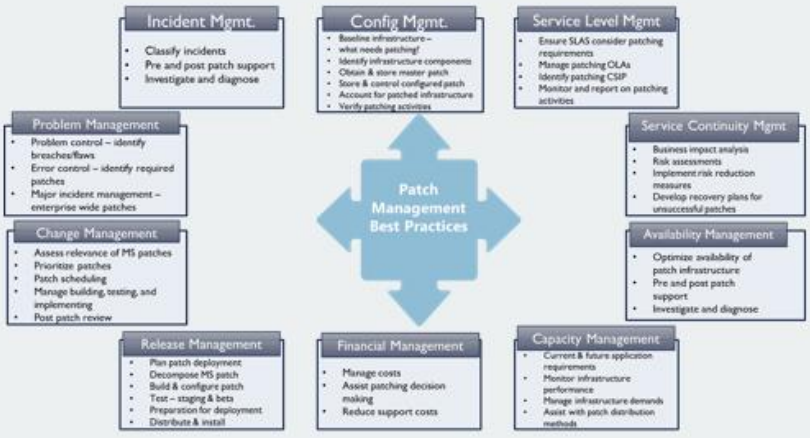
Reduce time to customer feedback *improved customer experience*

Enterprise capability for continuous software delivery that enables clients to seize market opportunities and reduce time to customer feedback

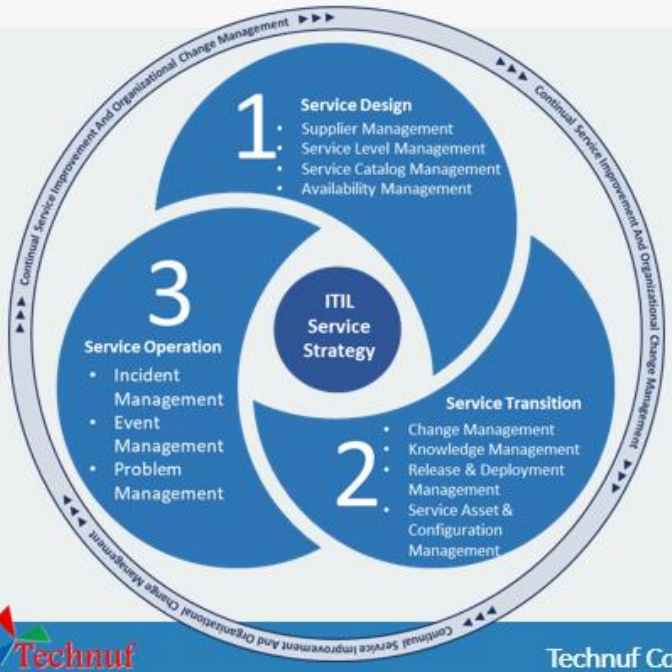
Typical patch management process

In accordance with NIST 800-34 Standards





ITIL BASED O&M



Assessment and Formulation of Overall Cybersecurity Strategy

- Security Audits
- Compliance
- Governance
- Penetration Testing
- Customer Requirements

Security Architecture Solution

- Tools, technologies & cybersecurity solutions
- Policies, Processes, procedures and guidelines
- Development of training

Execute the Solution

- Monitor
- Assess
- Mitigate

Preparing the Organization for solution

- Deploy solutions
- Training

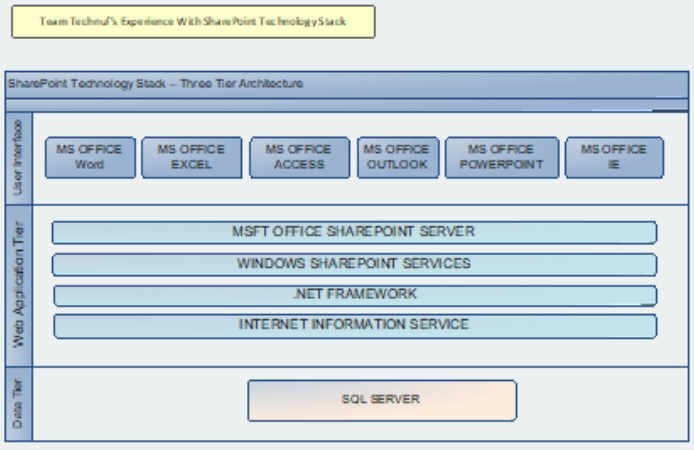
Cloud Migration Experience

- Application and Data Migration to the Azure/AWS cloud
- PCI/PII data masking
- Voltage Encryption (AES 256 FPE)
- Optimize Cloud scaling
- Significant Cost savings
- Mainframe Modernization Experience
- CI/CD approach
- Provide Hybrid Cloud Solutions
- Setup Custom DevOps catalogs
- Automated Testing tools
- Thorough topology review process for future proofing solutions
- Moved over 100TB of data from On Prem to Cloud Storage
- EBCDIC to ASCII conversion
- AWS/Azure Cloud solution – Cost/In-house tools
- Application porting without rewrite
- Application containerizing (Docker, Kubernetes,ACS)
- NSG/Firewall rules for On-Prem to Cloud communication
- Traffic management for most efficient routing
- Iaas/PaaS solutions
- Import/Export experience to lower bandwidth consumption
- Training sessions
- No SQL DB solutions (MongoDB, Document DB)

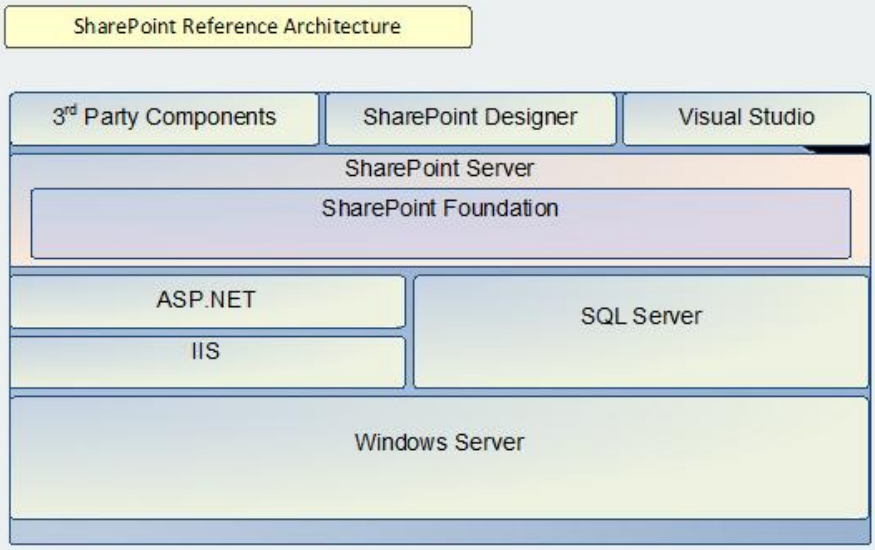
Share Point Development at DoD

- **HQ's SharePoint portal**
  - Supports 15 workflow applications
  - Has an audience of 1200 users
  - 35 SharePoint site pages
  - 4 active Software development projects
- Develop, Administer & Maintain SharePoint Applications & Web Apps
- Administer Learning Management Systems (LMS) functions
- SharePoint technology stack (i.e. the layers of software and services that comprise SharePoint)
- SharePoint custom application development and methodology
- Web Software Development
- Web Design for User Experience (UX)
- LMS Administration
- US Department of Defense Information System security requirements

Three Tier SharePoint Technology Stack



SharePoint Architecture



Technuf Technuf Confidential 25

Application Development

Technuf's Approach

- Industry best practices
  - Agile
  - CMMI
  - Six Sigma
- Customer adopted SDLC
- Continual development cycle
- Distributed development

Expertise Delivered

- Business and requirements analysis
- Architecture management
- Detailed design, implementation, and integration
- Safety critical applications
- Real-time solutions
- Fault-redundant systems
- Mission critical applications
- Business Intelligence

Objectives Met

- Safety critical applications for emergency responders
- Enterprise applications across 140K user base
- Social multi-media applications across targeted to several million end users
- Enterprise data warehouse with advanced analytics and reporting

Technuf Technuf Confidential 26

Testing Strategy

Unit Testing
Black box and White box

Automation
Use of industry standard tools (HP, IBM) and custom scripts

System Integration
Integration testing of end-to-end functionality

Coverage Analysis
Percentage of requirements tested

Development Integration
Integrating testing into development environment

Regression
Verifying defects are not reintroduced in future releases

Impact Analysis
Impact of changes to test assets

Smoke
On-Site application stability

User Acceptance
Formal acceptance testing by customer for a fully functional system

IRS

- Secure Communications Performance Testing
- DLP Functionality, Usability and Accessibility (508) Testing
- PCAP Customer Acceptance Testing
- EnCase Forensic Analysis Functionality Testing

cisco

- Integration & Regression Testing
- Performance Testing
- UAT

Technuf Technuf Confidential 27

Product Offerings

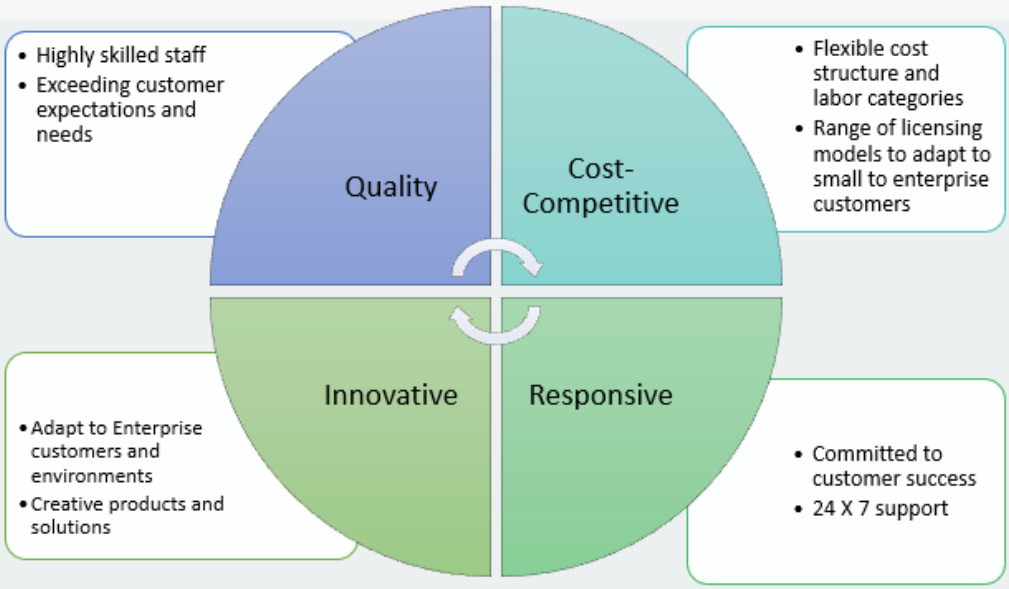
Safety Critical Applications	Mission Critical Applications	Educational Applications
• Cisco's IPICS (IP Interoperability Collaboration System) • First Responders • Army Training System • Air Force Radio Integration	• Aphelia Collaboration System • Utility, Oil & Gas • Real time Surveys and Dashboard • Transportation – School Bus Connect • Physical Security	• Tutor Toolbox • Student Management • Lesson Management • Assessment & Progress • Instructor Management • Online & Collaborative Learning, Literacy

Solves

- Collaboration amongst disparate groups
- Manage emergency incidence and simulation exercises
- Unified dispatching
- Intelligent personnel allocation
- Real-time multi-media and voice communication
- Real-time management reporting
- K12 bus riders' safety
- Comprehensive education lifecycle support
- Rapid enablement in literacy
- Improving life skills

Technuf Technuf Confidential 28

Technuf Advantages

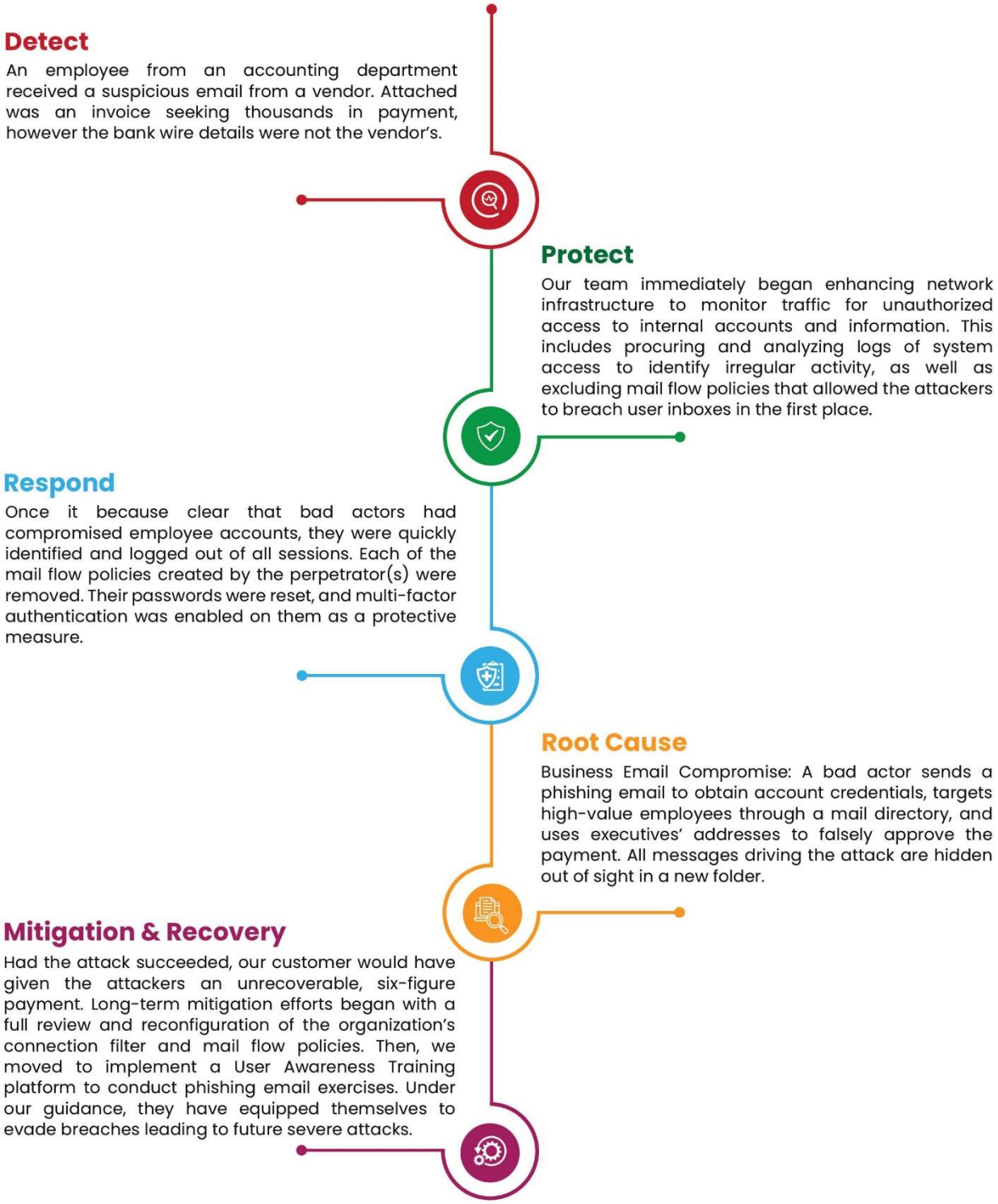


Contact Information

Corporate Headquarters:
40 W Gude Dr., Suite 220
Rockville, MD 20850
Phone: (301) 526-7888
Fax: (202) 627-3002
Website: www.technuf.com
General Info: info@technuf.com

1.6 Client Case Study

Security Incident Response



1.7 Our Clients

CYBER THREAT MONITORING SYSTEM

- 6 A Grade Banks
- 1 Payment Processing Company
- 1 Academic Institution
- 1 Telecom

CYBER SECURITY INCIDENT RESPONSE SERVICE

- 3 Banking And Financial Institutions
- 1 Medical Institution
- Us-based Health Care Service Provider

INFORMATION SYSTEM AUDIT AND GRC

- 18 A Grade Banks
- 1 B Grade Bank
- 1 C Grade Bank
- 3 Mobile Wallet Service Providers
- 1 International Financial Institution
- 2 US-based Health Care Services
- 3 Insurance Companies

PENETRATION TESTING SERVICE

- 6 A Grade Banks
- 5 Mobile Wallet Services
- 20+ Software Development Houses

2 Project Summary

2.1 Leverage Offensive Security Expert To Test Defenses And Uncover Issues

Get an understanding of real-world risks from the attacker's perspective – We Go beyond the limitations of automated scanning to identify the root cause of underlying issues. Our penetration tests simulate real-world attack vectors to provide a point-in-time assessment of vulnerabilities and threats to your network infrastructure and applications.

Quantify and prioritize findings using business-driven criteria – Our post-assessment analysis presents logical groupings of one or more security issues with common causes and resolutions. We provide an actionable findings matrix that can be used as an over-arching workflow plan and tracked within your security organization.

Enable your operations team in tracking the remediation effort – Each finding is categorized according to the relative level of risk posed to your organization. The final deliverable also contains the amount of work and resources required to address each finding, hyperlinked references to resources, and detailed remediation information.

3 Objectives

The main objective of the security assessment is to strengthen the security posture of the BRAC's network, applications and systems for any cyber threats.

4 Scope of Work

The scope of work is to conduct a comprehensive security assessment (VA/PT) on BRAC's mission critical assets, which are follows:

- Vulnerability Assessment and Penetration Testing of mission critical web and mobile applications and its related servers (8 ERP Modules, 10 Non-ERP Applications).
- Vulnerability Assessment and Penetration Testing of Cloud Infrastructure
- Vulnerability assessment and Penetration Testing of Network Infrastructure

The Vulnerability Assessment and Penetration testing will be perform following the industry best practices and guidelines. After completion of each task, we will submit a detail report containing the list of findings with severity ratings, impact and mitigation plan. We will suggest BRAC the deadline to fix the findings and monitor it. After fixing the problem from BRAC concern department, we will perform retest to ensure the vulnerabilities are properly patched.

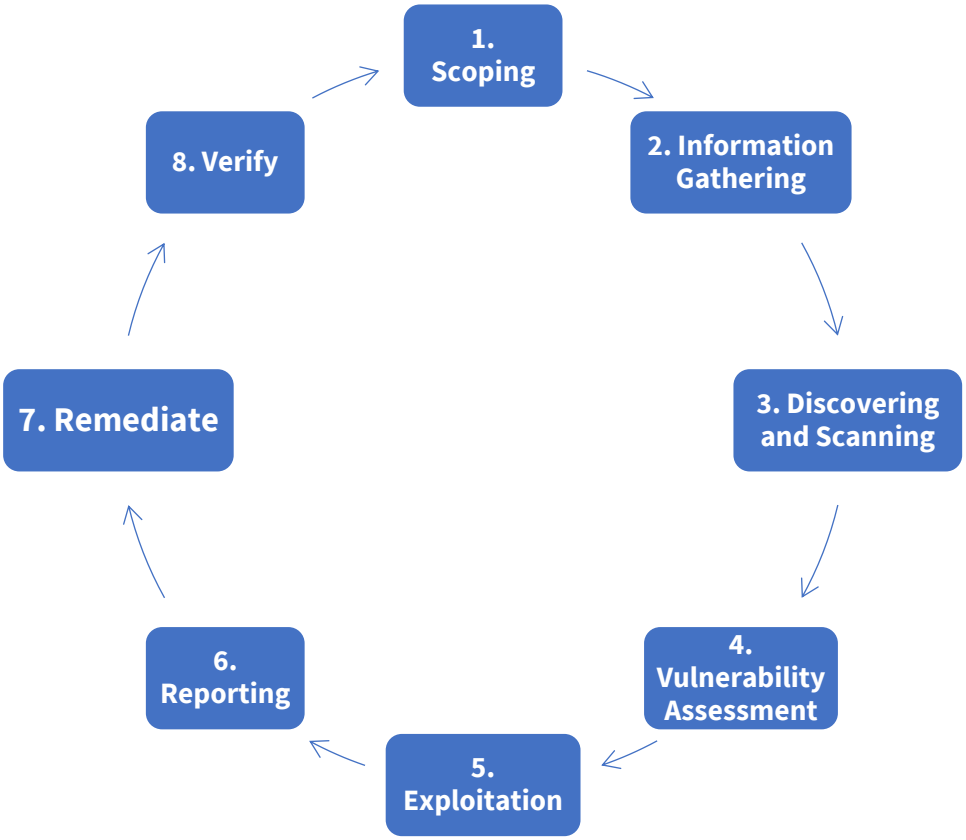
5 Deliverables

- Assessment
  - ❖ Required assessment of the existing network and application infrastructure.
  - ❖ Detailed report outlining the findings from the aforementioned assessment.
- Exercise
  - ❖ The incumbent vendor will do the VA/PT for the aforementioned scopes.
  - ❖ After the successful conduction of the VA/PT, the incumbent vendor will submit reports with their findings.
  - ❖ BRAC will ensure all the CRTICIAL, and HIGH priority issues are resolved in the relevant scope.
  - ❖ The incumbent vendor will retest the fixes and close the issues.
- Output
  - ❖ Detailed list of vulnerabilities in the applications, web services and network.
  - ❖ List of recommendations to fix/ mitigate the vulnerabilities identified.
  - ❖ Severity ratings for the vulnerabilities.
  - ❖ Categorization of the vulnerabilities according to OWASP.
  - ❖ Assist relevant implementation team while fixing the identified issues.
  - ❖ Come up with a future recommendation and plan for BRAC infra-VA/PT.

6 Our Methodology

6.1 Project Life Cycle

The project will be initiated with the preliminary meeting regarding the Terms of Reference and the introduction meeting with stakeholders to understand the gravity of the Terms of Reference. We too will provide requests for information to initiate the planning phase.



6.1.1 Scoping

The planning phase will be initiated with the goals to prepare an inception report and will perform data gathering, methodology of assessment (Black Box, Gray Box, Whitebox), review to understand the current posture of Nepal Bank Limited infrastructure.

6.1.2 Information Gathering

The information gathering phase is obtaining as much information about the scope such as Networks, IP Address, Operating System Version, etc. in the planned scope. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing, and White Box Testing.

6.1.3 Discovering and Scanning

In this phase we will perform the following to determine the posture of network and system

i. Port Scanning
ii. System OS Discovery
iii. Surficial Vulnerability Scanning

6.1.4 Vulnerability Assessment and False Positive Analysis

In this process, vulnerability scanners and custom tools are used, it will scan the scoped application and network and will identify the vulnerabilities.

In this process, defining and classifying output of discovery and scanning phase.

- Defining and classifying network or System resources.
- Identifying and removing false positives reports.
- Assigning priority to the resource (Ex: – High, Medium, Low)
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritized problems first and implementing ways to minimize the consequences if an attack occurs.

6.1.5 Exploitation (Penetration Testing)

After vulnerability assessments, which are used to identify and inventory various exposures within the organization's systems. Penetration testing attempts to exploit any one of the vulnerabilities to

gain unauthorized access. The penetration testing is the manual process to exploit the system in order to pivot in-depth.

The cleanup process covers the requirements for cleaning up systems once the penetration test has been completed. This will include all user accounts and binaries used during the test.

- Remove all executable, scripts, and temporary files from a compromised system. If possible, use a secure delete method for removing the files and folders.
- Return to original values system settings and application configuration parameters if they were modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

6.1.6 Reporting

All the previous Vulnerability Assessment & penetration testing phases contribute to this phase where a VAPT report is created and shared with the client. In the reporting phase, the pentesters provide detailed information about the vulnerabilities such as:

- A brief introduction about the assessment.
- The scope of Assessment
- The description of the vulnerabilities.
- Ratings according to a common vulnerability scoring system.
- Severity and impact of vulnerability.
- Recommendations for fixing the vulnerabilities.

6.1.7 Remediate

Technuf limited will assist Nepal Bank team remediate the identified vulnerabilities.

6.1.8 Verify

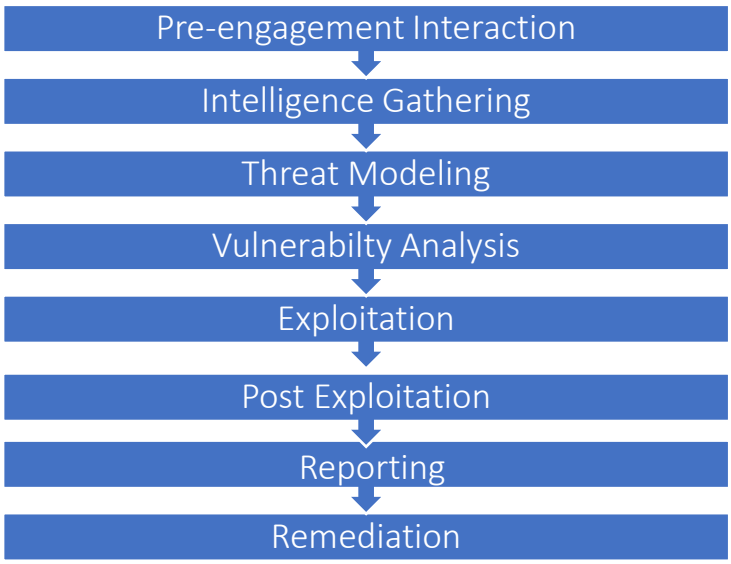
Our team will perform verification testing after the patched has been applied to vulnerable system.

7 Our Approach

7.1 Network Penetration Testing Methodology

The best way to know how intruders will actually approach your network is to simulate an attack under controlled conditions. Network Penetration Testing actually exploits Penetration Testing. the vulnerabilities to determine what information is actually exposed to the outside world.

We use the following methodology for Network



Pre-engagement Interactions

- Scoping Meeting
- Questionnaires
- Specify Start and End Dates
- Specify IP Ranges and Domains
- Rules of Engagement
- Establish Lines of Communication
- Dealing with Third Parties
- Contact List
- Permission Memo
- Commencement and Debrief Emails

Intelligence Gathering

Open-Source Intelligence - OSINT (Intelligence gathered from publicly available sources such as media, websites, forums etc.)

- Corporate
  - ✓ Physical
  - ✓ Logical

- ✓ Org Chart
- ✓ Electronic
- ✓ Infrastructure Assets
- ✓ Financial

- Individuals and interviews
- Covert Gathering
- Foot printing
- Identify Protection Mechanisms
- External Foot printing
- Internal Foot print

Threat Modelling

- ❖ Business Process Analysis
- ❖ Business Assets Analysis
- ❖ Threat Agents/Community analysis

Vulnerability Analysis

- ❖ Active Scanning
- ❖ Passive Scanning
- ❖ Validation

Exploitation

We exploit the vulnerable manually using exploitation tool to figure out the technical and business impact.

Post Exploitation

We perform the post exploitation in order to pivot form one network to another to assess the network segmentation security.

Reporting

The purpose of the reporting and documentation is to assist your organization in its efforts to improve its security posture by identifying areas of potential risk that may need to be

remediated. The report will be structured in a way to clearly communicate what was tested, how it was tested, and the results of the testing.

We will provide two types of report.

- Executive Report: Report for Executive explaining about security findings and risk metrics
- Technical Report: This report will contain detailed technical findings, tool used etc.

Report Outline

- Executive Summary
- Statement of Scope
- Statement of Methodology
- Statement of Limitations
- Testing Narratives
- Segmentation Test Results
- Findings
- Tool used

7.2 Web Application Penetration Testing

Penetration testing of web application is done through vulnerability assessment, process review and penetration testing using OWASP testing guide. This involves evaluating the applications security by simulating an attack on the system from external and internal threats. The process starts with an active analysis of the system for any potential vulnerability that could have resulted from poor or improper system configuration, insecure coding practices or other known or unknown software flaws, or operational weaknesses in process or technical countermeasures.

Technuf limited will perform Web application testing that simulates real-world attacks against your applications designed to identify security and compliance issues. Technuf limited uses various tools and manual verification, review, and crawling techniques to perform an in-depth and comprehensive vulnerability assessment and penetration testing of your application.

Our Approach

- ❑ Blackbox Testing
  - ❑ Our Penetration Tester tries to break the system with no internal knowledge of the target system.
- ❑ Gray-box Testing
  - ❑ Our Penetration Tester tries to break the system which has the access and knowledge levels of a user, potentially with elevated privileges on a system.

Objective:

- Highlight weaknesses in Application Logic
- Identify the strength of Application Authentication
- Highlight weaknesses in Privilege Management
- Identify the weaknesses in Communication Channel
- Highlight the weaknesses in Data Management

The Web Application penetration testing include the following test cases:

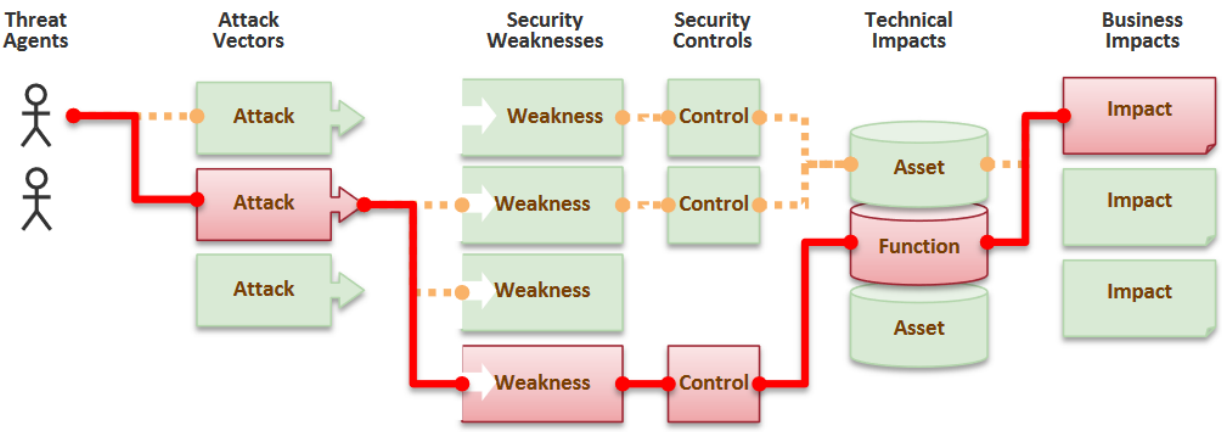
- Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards
- XML External Entities (XXE)
- Insecure Deserialization
- Insufficient logging and monitoring

Web Application Penetration Testing Workflow

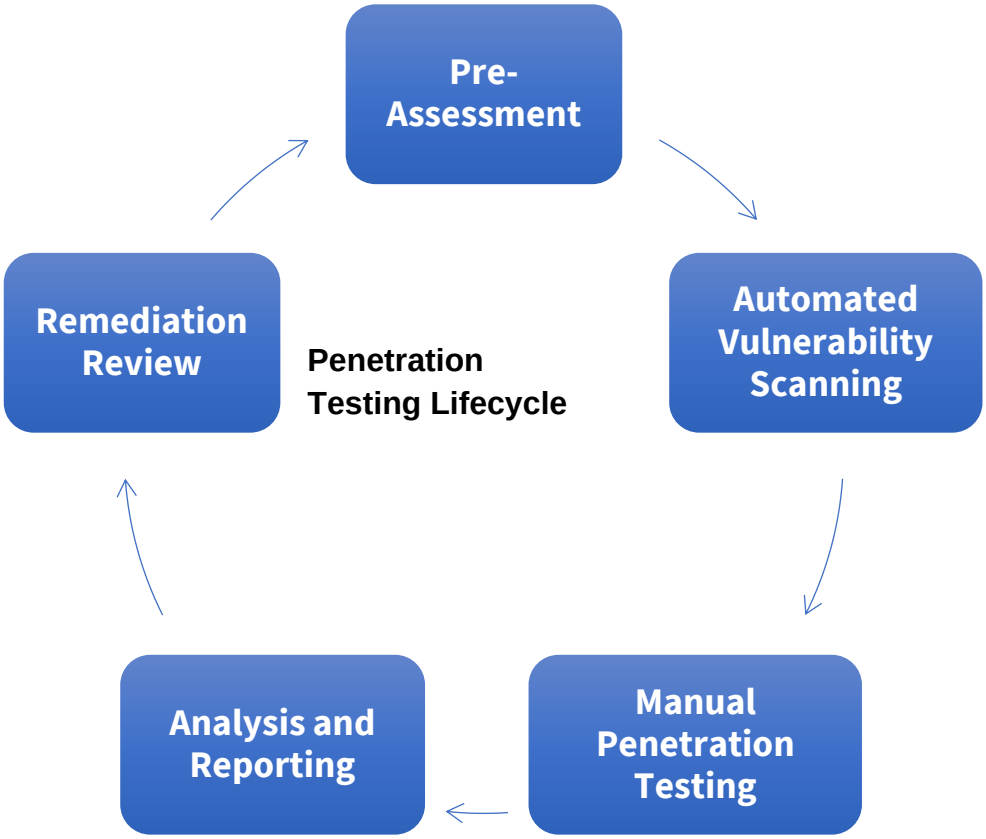
Penetration Testing is the process of attempting to gain access to resources with/without any prior knowledge of the requirements, in order to identify vulnerabilities that exist in a system or network. Penetration Testing must be performed annually and after any significant infrastructure or application changes to the environment with pre-defined standards. Technuf limited Technology strictly follows two different standards while carrying out penetration test:

- NIST Special Publication 800 – 115 "Technical Guide to Information Security Testing and Assessment" and
- Open Web Application Security Project "Top Ten"

Penetration Testing Workflow



Web Application Penetration Testing Methodology



Pre-assessment

During the first phase of penetration testing, we will have the:

- Team Introduction Session
- Web Application Knowledge Sharing Session
- Escalation Procedure session
- Test requirement gathering session

Automated Vulnerability Scanning

During the second phase, we will perform the vulnerability assessment and information gathering for the identification of the vulnerable endpoints.

Manual Penetration Testing

We will perform the manual penetration in the identified vulnerable end points using exploitation and web proxy tools.

Analysis and Reporting

We will prepare the report and will deliver in the following way:

- First Draft Report
- Final Executive Report
- Final Technical Report

Remediation Review

In the last phase, we will provide the consultation regarding the remediation process and, we will perform the reverification testing in the patched applied.

Guideline of Application Penetration Testing

Map the Application content

- Spidering
- Discovering Hidden Content
- Discovering Hidden Parameters

Analyze the Application

- Identifying data entry points
- Identifying Server Technology
- Used Mapping the Attack surface

Testing Authentication Mechanism

- Testing Login Brute Force
- Testing for User Enumeration
- Testing for Account Recovery function
- Testing Password Quality
- Testing any “Remember me” function
- Testing any impersonation function
- Testing username uniqueness
- Testing for predictable username and password

- Testing for any fail-open conditions
- Analyzing insecure storage of credentials

Testing Session Handling

- Testing tokens for meaning
- Testing tokens for predictability
- Testing for insecure transmission of tokens
- Testing for disclosure if tokens in logs Mapping of token to sessions
- Testing for session termination
- Testing for session fixation
- Testing for cross site request forgery
- Analyzing cookie scope

Testing Input Based Vulnerabilities

- Fuzzing all request parameters
- Testing for SQL injection
- Testing for Cross Site Scripting
- Testing for HTTP head injection
- Testing for OS command injection
- Testing for path traversal Testing for file inclusion
- Testing for other injection (if possible—SOAP injection, LDAP injection, XPATH injection)

Testing for Application Logic

- Identifying the logic attack surface
- Test transmission of data via the client
- Test for reliance on client-side input validation
- Test handling of incomplete input
- Test trust boundaries
- Test transaction logic
- API Testing

Assess Server Hosting

- Test for Web server/ Application server vulnerabilities
- Default credentials
- Default content
- Dangerous HTTP methods
- Virtual hosting misconfiguration
- Test for Web services

Miscellaneous Tests

- Check for DOM-based attacks
- Check for iFrame injection
- Caching Sensitive data in URL Parameters
- Check for weak SSL ciphers

7.3 API Penetration Testing

API penetration testing service for web applications simulates a realistic (but well-controlled) attack on your applications and their back-end infrastructure executed by an in-house ethical hacker, with an aim to:

- Identify the weaknesses.
- Demonstrate how these weaknesses could be exploited.
- Find solutions to effectively remediate the vulnerabilities.

API penetration testing focuses on the security of APIs that your business exposes externally with supporting documentation. These are not APIs that are private or used internally in your own applications – we can cover those interfaces with a web application test – these are instead interfaces that you publish for users to implement in their own applications. We'll take the same documentation you provide to users; construct API calls like they would, and then use them to discover security issues.

7.3.1 API Penetration Testing Methodology

7.3.1.1 Pre-engagement interactions

Through a pre-engagement process, we identify your core-competencies and analyses your documentation.

7.3.1.2 MAP the API & Threat Modelling

Modelling security assessments based on real-time threats; we map your API accurately using ASMX/Helpdocs etc.

7.3.1.3 Dynamic Analysis

We then perform a vulnerability test based on REST OWASP API Security project and evaluate the extent to which the identified bugs could cause losses and recommend steps to reproduce the bugs.

7.3.1.4 Business Logic Flaw testing

Every business is different and so are its vulnerabilities. We run comprehensive tests to locate logic flaws in your IT processes that could potentially affect your security.

7.3.1.5 Reporting

We complete the cycle with the delivery of a comprehensive API security assessment report and work with your development team to fix vulnerabilities.

7.3.2 API Penetration Testing Guideline

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user.

7.3.2.1 Broken User Authentication

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising system's ability to identify the client/user, compromises API security overall.

7.3.2.2 Excessive Data Exposure

Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

7.3.2.3 Lack of Resources & Rate Limiting

Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.

7.3.2.4 Broken Function Level Authorization

Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

7.3.2.5 Mass Assignment

Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on a whitelist, usually lead to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.

7.3.2.6 Security Misconfiguration

Security misconfiguration is commonly a result of unsecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

7.3.2.7 Injection

Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

7.3.2.8 Improper Assets Management

APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

7.3.2.9 Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Reporting Format

The purpose of the reporting and documentation is to assist your organization in its efforts to improve its security posture by identifying areas of potential risk that may need to be remediated. The report will be structured in a way to clearly communicate what was tested, how it was tested, and the results of the testing.

Technuf limited will provide two types of report.

- Executive Report: Report for Executive explaining about security findings and risk metrics
- Technical Report: This report will contain detailed technical findings, tool used etc.

Report Outline

- Executive Summary
- Statement of Scope
- Statement of Methodology
- Statement of Limitations
- Testing Narratives
- Segmentation Test Results
- Findings

- Tool used
- Clean up the environment

7.4 Mobile Application Penetration Testing

Mobile Applications have become an essential part of our lives as our dependence on smart phones has grown. But many users are unaware of the security of their devices. A recent study on the state of application security that "84 percent of mobile app users believe that their mobile health and finance apps are adequately secure."

Security can often be a false perception if we do not know how our applications were developed and penetration tested. The reality is that downloading and using these applications can represent a potential risk to both you and your organization, given that untested apps may contain security bugs that can make your data vulnerable.

One way to avoid this risk is to make sure that mobile apps have been properly pen tested against security vulnerabilities. Penetration testing can provide us with a certain level of confidence but hacking into mobile applications demands a different approach and setup than with web applications.

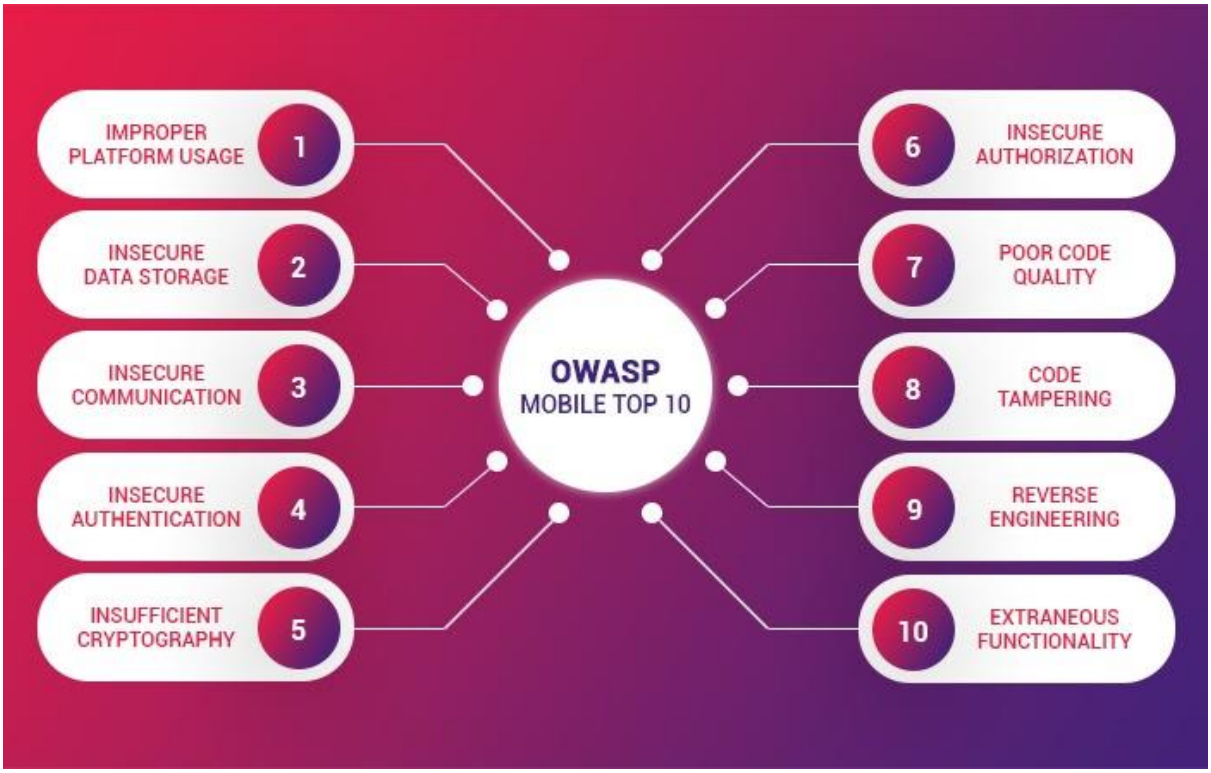
Our comprehensive mobile application penetration testing approach and methodology have been developed after performing several mobile app security assessments across various clients in different sectors such as banking, finance, healthcare etc.

What to Expect in our Mobile Application Penetration Service?

Deep Support for both iOS and Android Platforms Each mobile security assessment simulates multiple attack vectors and risks, including insecure storage, stolen device risk, mobile malware attacks, and both authenticated/unauthenticated app users. Apps residing on in-house mobile devices. We provide custom scenarios to map enterprise conditions as well.	**Static, Dynamic, and Source Code Analysis** Integrating both static and dynamic analysis, our security experts test each mobile app at-rest and during runtime to identify all vulnerabilities. This deep-dive methodology also targets local vulnerabilities as well, such as insecure storage of credentials, Android backups including sensitive app data, etc.

Mobile Application Penetration Testing Coverage Area

- Android Application
- IOS Application



Technuf has created a research-driven mobile penetration testing methodology that incorporates guidance from the OWASP Application Security Verification Standard. Using a combination of manual and dynamic analyses along with custom harnesses for automated fuzzing, Technuf mobile application penetration testing provides verification and validation across all major control categories, including authentication, session management, access control, malicious input handling, cryptography at rest, and much more.

Mobile Application Penetration Testing…

- Provides a complete picture of the risks in your mobile applications and helps you mitigate them through remediation guidance.
- Finds the risks related to mobile applications regardless of where those risks exist: client-side code, server-side code, third-party libraries, or underlying mobile platforms.
- Finds the security vulnerabilities that endanger your users, or their data being managed by your application as well as risky or unintended behaviours.

- Delivers assessments and mitigation advice tailored to the various types of mobile applications including internal and external applications as well as applications developed using native APIs and cross-platform development frameworks.

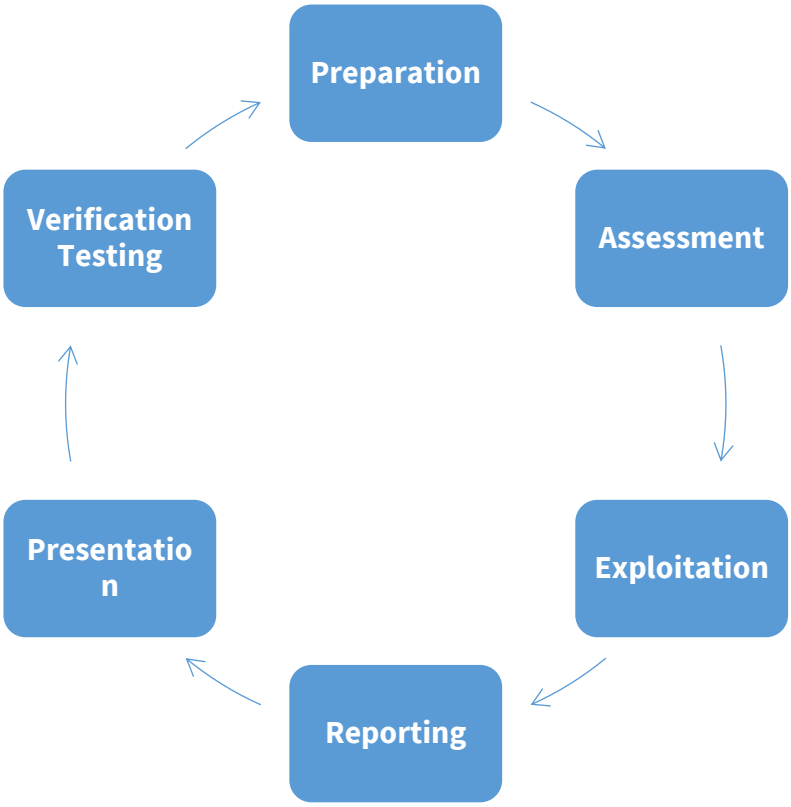
Mobile Application Penetration Testing Methodology

For mobile application penetration testing, we utilize the same tools and techniques as malicious hackers, providing detailed visibility into security vulnerabilities - without the associated business risk.

Mobile Application Penetration Testing Objective

- ❑ Highlight weaknesses in Application Logic
- ❑ Identify the strength of Application Authentication
- ❑ Highlight weaknesses in Privilege Management
- ❑ Identify the weaknesses in Communication Channel
- ❑ Highlight the weaknesses in Data Management

The Mobile Application Penetration Testing is divides into four stages:



7.4.1 Preparation

Information gathering is the most significant step in a penetration test. The ability to find hidden cues that might shed light on the occurrence of vulnerability can be the difference within a successful and unsuccessful penetration testing.

7.4.2 Assessment

The process of mobile assessment applications is different because it challenges the penetration tester to compare the apps before and after installation. The assessment techniques that encountered within the mobile security include:

- File system analysis
- Package analysis
- Reverse engineering
- Static analysis
- Dynamic analysis
- Inter-Process Communication Endpoint Analysis

7.4.3 Exploitation

Penetrations testing engineer operates upon the information determined from the information-gathering step to attack the mobile application. Entirely performed intelligence gathering ensures a high possibility of a successful project.

This phase includes exercising all potential vulnerabilities recognized in the previous stages of the assessment and trying to exploit them as an attacker would. Not only automatically recognize vulnerabilities that exploited, but issues requiring hand-operated classification and exploitation evaluated, as well. That involves business logic flaws, authentication/authorization bypasses, direct object references, parameter tampering, and session management. Pentester tries to exploit the vulnerability to gain sensitive information or perform malicious actions. Then finally delivers privilege escalation to rise to the most privileged user (root) to not face any restrictions on any actions that completed.

7.4.4 Reporting

The purpose of the reporting and documentation is to assist your organization in its efforts to improve its security posture by identifying areas of potential risk that may need to be

remediated. The report will be structured in a way to clearly communicate what was tested, how it was tested, and the results of the testing.

Technuf will provide two types of report.

- Executive Report: Report for Executive explaining about security findings and risk metrics
- Technical Report: This report will contain detailed technical findings, tool used etc.

7.4.5 Report Outline

- Executive Summary
- Statement of Scope
- Statement of Methodology
- Statement of Limitations
- Testing Narratives
- Segmentation Test Results
- Findings
- Tool used
- Clean up the environment

7.4.6 Presentation

The final activity of the penetration testing will be a presentation of all documentation to the client. We walk the client within the information provided, make any updates needed, and address questions regarding the assessment output. Following this activity, we'll give new revisions of documentation and schedule any formal retesting, if it is applicable.

7.4.7 Verification Testing

When client patches all vulnerabilities, Technuf penetration tester will verify, validate and approve it.

7.4.8 Configuration Security Audit

One of the most certain ways to avoid hosts being compromised is to secure them by reducing their surface of vulnerabilities. That process is commonly known as hardening, and the

configuration assessment is the most effective way to determine where the hosts may have their hardening improved.

Configuration Audit is done based on the industry standard such as NIST and CIS benchmark. Our Configuration Audit consist of the two methods.

7.4.8.1 Automated Configuration Assessment

We will use the open source and licensed Security Configuration Assessment tool identify gaps and vulnerabilities.

7.4.8.2 Manual Configuration Assessment

Our Security Configuration auditors will manually verify the configuration of the system to avoid machine error.

8 Project Timeline

8.1 Work Schedule and Planning for deliverables

S. No.	Deliverable (D)	7	12	14	15	15	8	45	8	3	Total
1	Scoping										
2	Information Gathering										
3	Discovering and Scanning										
4	Vulnerability Assessment and False Positive Analysis										
5	Exploitation										
6	Reporting and Presentation										
7	Remediation Period										
8	Reverification Testing										
9	Release of Final Report										

9 Detailed Work Plan

Based on information provided by the BRAC, we are prepared to start the Vulnerability assessment and penetration testing at a mutually agreeable date. Depending on the schedules of the BRAC, we expect the project to end in February 2023 with detailed time below.
We have broken down the work plan as per the deliverable's objectives.

9.1 Scoping

Main Activities

- Preliminary Meeting
- Rules of engagement and Timescales
- Establish Lines of Communication
- Understanding the service, architecture, and assets details
- Methodology of assessment (Black Box, Gray Box, White Box)

Duration: 7 Days.

9.2 Information Gathering

Main Activities

- Prioritize scope and timescales (production and staging environment)
- Automated information gathering
- Passive Reconnaissance
- Active Reconnaissance
- Identify Protection Mechanisms

Duration: 12 Days

9.3 Discovery and scanning

Main Activities

- Enumeration: Finding Attack Vectors
- Web application scanning and content discovery
- Network Scanning
- Automated and custom discovery and scanning

Duration: 14 Days

9.4 Vulnerability Assessment and False Positive Analysis

Main Activities

- Automated & Manual Web Vulnerability Assessment
- Network Vulnerability Assessment
- Classify Vulnerability found through industry standard guideline
- Validation & Correlation using compliance framework
- Public Research (Vulnerability Databases, Vendor Advisories)
- Private Research (Testing Configurations, Fuzzing, potential avenues/vectors creations)

Duration: 15 Days

9.5 Exploitation (Penetration Testing)

Main Activities

- Exploiting found vulnerabilities
- Tailored Exploits
- Post Exploitation
- Privilege escalation
- Remove all executable, scripts and temporary files from a compromised system.
- Remove any user accounts created for connecting back to compromise systems.

Duration: 15 Days

9.6 Reporting

Main Activities

- Executive Report
- Technical Report
- Report Presentation

Duration: 8 Days

Milestone: Within 3 Days of Penetration Testing report

Final Output: Draft Report

9.7 Remediate Period

Main Activities

- Prioritizing Vulnerabilities
- Vulnerability remediation Plan

- Remediation Consultation

Duration: 45 Days

9.8 Reverification Testing

Main Activities

- Revalidation testing of the patched vulnerabilities
- Reporting of unpatched vulnerabilities

Duration: 8 Days

Final Output:

Reverification Testing report

9.9 Final Report

Main Activities: Release of Final Report

Duration: 3 Days

9.10 Reporting Format Details

Throughout the engagement, we will provide draft deliverables to the BRAC Program Manager for review and comment. This will provide opportunities to review the deliverables and obtain the BRAC's feedback on their content and quality.

final report deliverable to consist of:

• Executive Summary Report

• Detailed Findings Report

9.10.1 Executive Summary Report

The target audience for this report is the BRAC's executive management. This report will comprise the assessment scope, objectives, and approach of each of the assessments. The report will also summarize the urgent and high-risk security vulnerabilities identified by the scanning tool in clear terms, as well as provide potential remediation strategies.

9.10.2 Detailed Findings Technical Report

The target audience for this report is the BRAC's security management, operations teams, and application development teams. This report will outline the scope of the assessment activity, procedures used to perform the activity, and summary of identified vulnerabilities. This data will

be structured to include a severity rating for Vulnerability Risk Classification based on industry standards. Items that are deemed a critical risk will be escalated to you at the time of discovery, and will also be reported in this document.

At the conclusion of the engagement, deliverable reports, supporting evidence, related documentation, raw output from tools and assessments, and other beneficial data will be presented to the Brac Program Manager on email for distribution to the appropriate Brac teams. In addition, two printed copies of the final report will also be delivered.

The advice, recommendations, work product, and deliverables provided as part of this engagement will be developed for BRAC management, and are not intended for use by any other party or for any other purpose, and may only be relied upon by BRAC management and will be so marked.

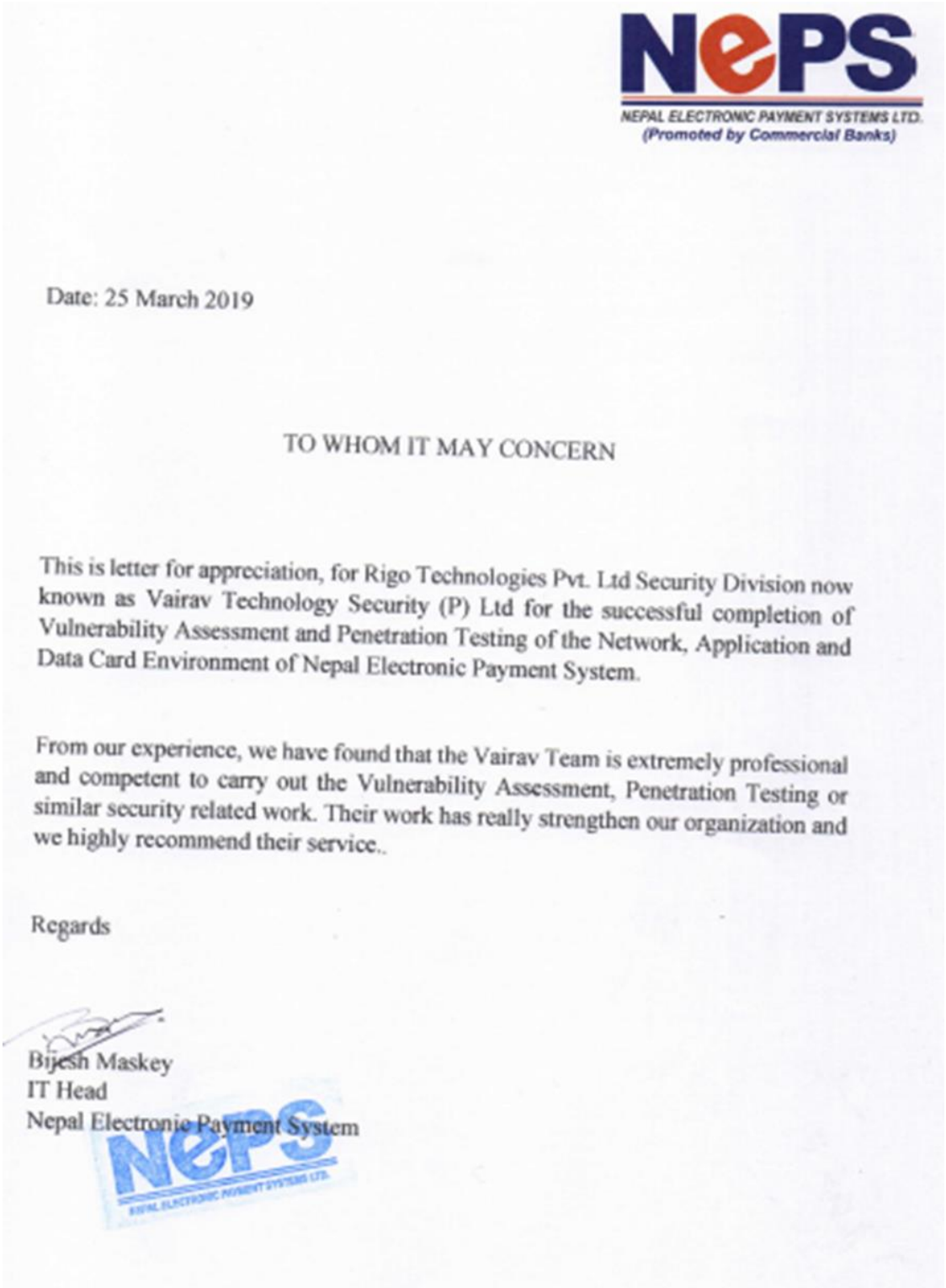
10 Relevant Work Experience of Technuf and Associates

Project Name EAC Program – Cybersecurity Operations Support Services (COSS) ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**
Project Name Department of Defense, Defense Human Resources Activity (DOD – DHRA) - SharePoint Software Development & Administrative Support Services for Cloud Based IS Project ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**
Project Name State of Vermont -For Information Technology Professional Services ❑ Relevant Document attached below.

[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]
Project Name Information Technology Professional Services: IPICS Software Development Service; Network & Server Infrastructure Support; IoT Documentation Support, Cisco Collaborative Knowledge (CCK) Project ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**
Project Name Cybersecurity Infrastructure Support for Yoga Alliance ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**
Project Name HIDS-EDR (Host based Intrusion Detection System – Endpoint Detection and Response) ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**
Project Name RSA Archer Cybersecurity Project ❑ Relevant Document attached below. **[This is govt project. due to confidentiality and privacy clause we are unable to disclose much details of the project]**

Project Name

Vulnerability Assessment and Penetration Testing of the Network, Application and Data Card Environment of Nepal Electronic Payment System



NEPAL ELECTRONIC PAYMENT SYSTEMS LTD.
(Promoted by Commercial Banks)

Date: 25 March 2019

TO WHOM IT MAY CONCERN

This is letter for appreciation, for Rigo Technologies Pvt. Ltd Security Division now known as Vairav Technology Security (P) Ltd for the successful completion of Vulnerability Assessment and Penetration Testing of the Network, Application and Data Card Environment of Nepal Electronic Payment System.

From our experience, we have found that the Vairav Team is extremely professional and competent to carry out the Vulnerability Assessment, Penetration Testing or similar security related work. Their work has really strengthen our organization and we highly recommend their service..

Regards

Bijesh Maskey
IT Head
Nepal Electronic Payment System

Project Name

Vulnerability Assessment and Penetration Testing of the We Applications Developed by AMNIL Technologies

Project Name

AMNIL
Technologies Pvt. Ltd.

Telephone
977 1 5537084

E-mail
info@amniltech.com

Location
Mahabauan, Lalitpur, Nepal

Website
www.amniltech.com

Date: 25 March 2019

TO WHOM IT MAY CONCERN

This is letter for appreciation, for Vairav Technology Security (P) Ltd for the successful completion of Vulnerability Assessment and Penetration Testing of the web application developed by AMNIL Technologies Pvt. Ltd. and the excellence work done by the organization.

From our experience, we have found that the Vairav Team is extremely professional and competent to carry out the Vulnerability Assessment, Penetration Testing or similar security related work. Their work has really strengthened our organization and we highly recommend their service.

Regards

For: AMNIL Technologies Pvt. Ltd

Amit Joshi

(CEO)

Information System Audit

NABIL BANK®

Nabil Bank
P.O. Box 3729, Teendhara, Durbarmarg
Kathmandu, Nepal
Email : info@nabilbank.com
Tel : (977-1) 4227181, 4221718
Fax : (977-1) 4226905
SWIFT : NABBNPKA
Website : www.nabilbank.com

HO/Admin/ 088/076/77

01 September 2019

Vairav Technology Security P. Ltd.
Baluwatar,Kathmandu
Nepal.

Subject: Information System Audit

Dear Sir,

We are pleased to inform you that your quotation for Information System Audit (IS Audit) has been accepted by the bank as per the specification in your quotation dated 30 July 2019.

S.No.	Description	Amount
1	System (IT/IS) Audit	[redacted]
2	Value Added Tax(VAT)	
	Total Cost	

Terms and Conditions:

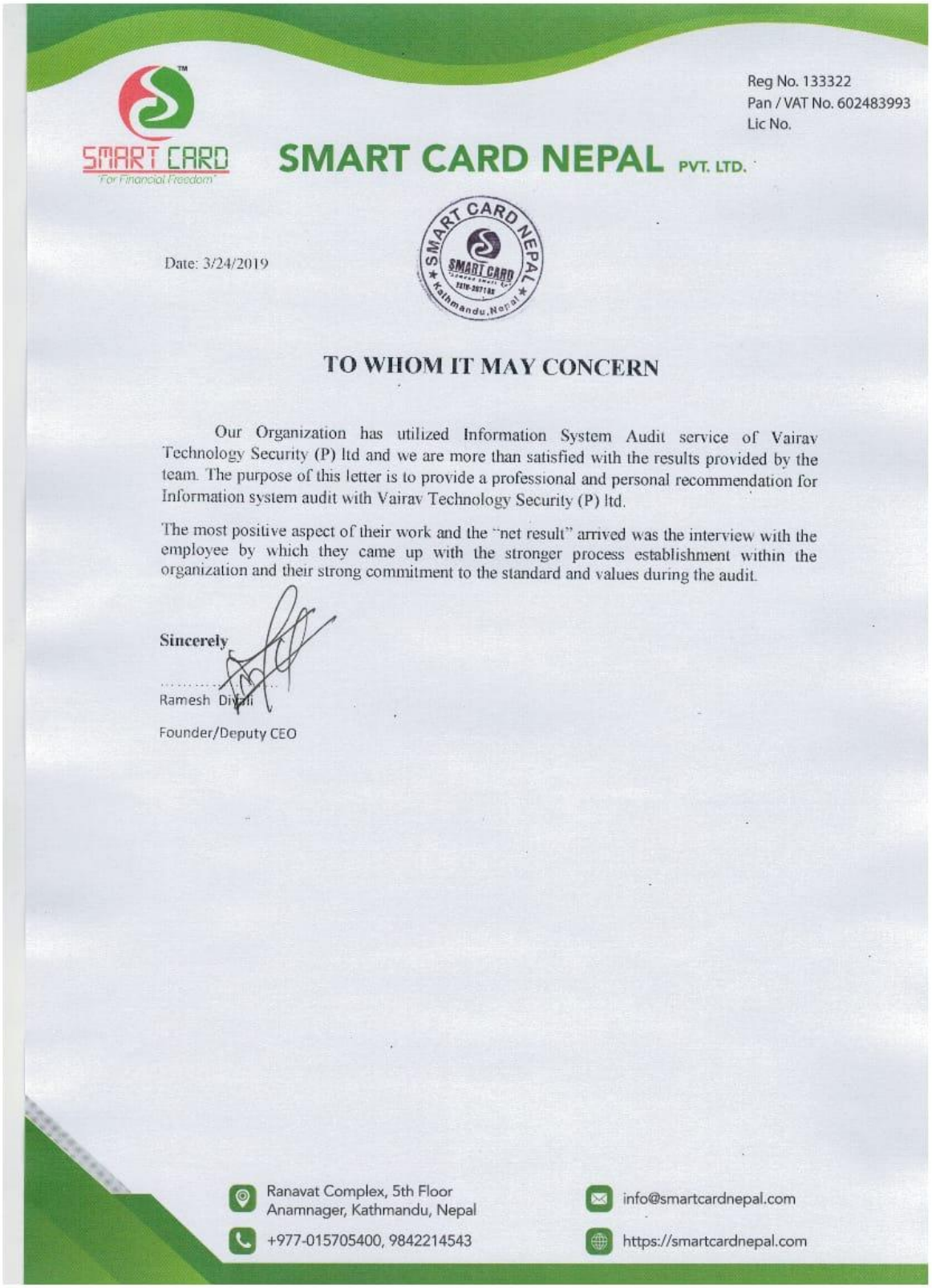
1. Please complete the above mentioned scope of work at in coordination with the Mr. Sushil Bhattarai, Head IT.
2. Out of pocket expense will be provided for travel outside valley.

Yours truly,

Authorized Signatory
Nabil Bank Ltd.

Project Name

Information System Audit



SMART CARD
"For Financial Freedom"

SMART CARD NEPAL PVT. LTD.

Reg No. 133322
Pan / VAT No. 602483993
Lic No.

Date: 3/24/2019

SMART CARD NEPAL
SMART CARD
Kathmandu, Nepal

TO WHOM IT MAY CONCERN

Our Organization has utilized Information System Audit service of Vairav Technology Security (P) ltd and we are more than satisfied with the results provided by the team. The purpose of this letter is to provide a professional and personal recommendation for Information system audit with Vairav Technology Security (P) ltd.

The most positive aspect of their work and the "net result" arrived was the interview with the employee by which they came up with the stronger process establishment within the organization and their strong commitment to the standard and values during the audit.

Sincerely

.....
Ramesh Divali
Founder/Deputy CEO

Ranavat Complex, 5th Floor
Anamnager, Kathmandu, Nepal
+977-015705400, 9842214543
info@smartcardnepal.com
https://smartcardnepal.com

11 Company Documents

List of legal Documents	
Trade License	

ঢাকা উত্তর সিটি কর্পোরেশন
www.dncc.gov.bd
(রাজস্ব বিভাগ)

R

লাইসেন্স ইস্যুর বিবরণ		
ওয়ার্ড নম্বর	ইস্যুর ক্রমিক নম্বর	ইস্যুর তারিখ
২০	১৮৭০	১৫/১/২০২০

ট্রেড লাইসেন্স
(TRADE LICENCE)
No : 184190

স্থানীয় সরকার (সিটি কর্পোরেশন) আইন ২০০৯-এর ধারা ৮৪-এর প্রদত্ত ক্ষমতাবলে সরকার প্রণীত আদর্শ কর তফসিল ২০১৬ এর ১০ নং অনুচ্ছেদ অনুযায়ী ব্যবসা, বৃত্তি, পেশা বা শিল্প প্রতিষ্ঠানের উপর আরোপিত কর আদায়ের লক্ষে নিম্ন বর্ণিত ব্যক্তি/প্রতিষ্ঠানের অনুকূলে এ ট্রেড লাইসেন্স ইস্যু করা হলো। যার কার্যকারিতার মেয়াদ .....

১। মালিকের নাম : ফারহিদা লায়লা কাদের (ব্যবস্থাপনা পরিচালক)
২। পিতার নাম :
৩। মাতার নাম : বেগম আছিয়া আকতার
৪। স্বামী / ~~স্ত্রীর নাম~~ : ফয়সাল কাদের
৫। মালিকের ঠিকানা

বর্তমান বসবাসের ঠিকানা
হোল্ডিং নং : ১১
রোড নং : ২১২ বনানী
থানা :
ঢাকা ১২১৩ (পোস্ট কোড)

স্থায়ী/ রেজিস্টার্ড ঠিকানা
হোল্ডিং নং / গ্রাম :
রোড নং / পোস্ট অফিস : -২-
থানা :
জেলা :

৬। ব্যবসা প্রতিষ্ঠানের নাম : টেকনাফ লিমিটেড
৭। পরিশোধিত মূলধন (লিঃ কোম্পানীর ক্ষেত্রে)ঃ টাকা ১,১৪,৫০০/-
৮। ব্যবসা প্রতিষ্ঠানের ঠিকানা : ২১২ টাওয়ার (১০ম তলা) ও বীর উত্তম এ কে খন্দকার
ফোন ____ ই-মেইল ____ মোবাইল নম্বর ____
৯। ব্যবসার ধরণ : ইনফরমেশন কমিউনিকেশন, টেলিকমিউনিকেশন, হার্ডওয়্যার, সফটওয়্যার, আমদানী, রপ্তানী, সার্ভিসিং
১০। আদর্শ কর তফসিল ২০১৬ এর ক্রমিক নং ঃ ৭৮
১১। ট্রেড লাইসেন্স/ নবায়ন ফি (বার্ষিক) ঃ টাকা (অংকে) ২০০০/-
(কথায়) (দুই হাজার) টাকা।
১২। সাইনবোর্ড কর (বার্ষিক) ঃ টাকা (অংকে) ৪৮০/-
(কথায়) (চার শত আশি) টাকা।
১৩। ইস্যুকৃত চালান ঃ বই নম্বর ১৮৪১১০

লাইসেন্সধারীর নিকট হতে সকল বকেয়া পাওনা বিবিধ রশিদ নম্বর ____, তাং ____ এর মাধ্যমে আদায় করা হয়েছে।
লাইসেন্সটি ২০/১ নম্বর ডি.সি.আর. ____ বইয়ের ২৭২ নং পৃষ্ঠায় লিপিবদ্ধ করা হয়েছে।

১৫/১/২০২০
লাইসেন্স ও বিজ্ঞাপন সুপারভাইজার
(নাম ও পদবীসহ সীল)
মোঃ সাইদুল ইসলাম চৌধুরী
লাইসেন্স ও বিজ্ঞাপন সুপারভাইজার
অঞ্চল-৩ (মহাখালী)
ঢাকা উত্তর সিটি কর্পোরেশন, ঢাকা।

১৫/১/২০২০
কর কর্মকর্তা
(নাম ও পদবীসহ সীল)
মোঃ তহলিল উদ্দীন
কর কর্মকর্তা
অঞ্চল-৩
ঢাকা উত্তর সিটি কর্পোরেশন, ঢাকা।

ঢাকা উত্তর সিটি কর্পোরেশন
(রাজস্ব বিভাগ)

(নবায়ন পাতা)

ট্রেড লাইসেন্স
(TRADE LICENCE)
No : 184190

লাইসেন্স গ্রহীতা কর্তৃক চালানের সাথে হাল মাসের ভাড়ার রশিদ/ রশিদের ফটোকপি, দাখিলক্রমে ফি/ কর নির্ধারিত চালানে ব্যাংকে জমা প্রদান এবং ব্যাংক কর্তৃপক্ষের সীল মোহরযুক্ত স্বাক্ষর থাকতে হবে।

নবায়ন কার্যকারিতার মেয়াদ ২০১৮-২০১৯ খ্রিঃ

১। জমার তারিখ ঃ
২। লাইসেন্স বই নম্বর ঃ চালান বই নম্বর
৩। টাকার পরিমাণ ঃ লাইসেন্স/ নবায়ন ফি = 2000/-
সাইনবোর্ড কর = 860/-
সারচার্জ = 2800/-
মোট টাকা (অংকে) = 8660/-
মোট টাকা (কথায়) =
স্ক্রল নম্বর তারিখ

..................ইং অর্থ বছরের ট্রেড লাইসেন্স বকেয়া ফি ও সাইন বোর্ড কর কর্পোরেশন কর্তৃক নগদে আদায় করা হইল। আদায়কৃত রশিদ নং........ তাং........ টাকার পরিমান........।

মোঃ সাইদুল ইসলাম চৌধুরী
লাইসেন্স ও বিজ্ঞাপন সুপারভাইজার
অঞ্চল-৩
ঢাকা উত্তর সিটি কর্পোরেশন, ঢাকা।

ব্যাংক ক্যাশিয়ারের স্বাক্ষর ও সীল (ব্যাংকের সীল) ব্যাংক কর্মকর্তার স্বাক্ষর ও সীল

নবায়ন কার্যকারিতার মেয়াদ ২০১৯-২০২০ খ্রিঃ

১। জমার তারিখ ঃ
২। লাইসেন্স বই নম্বর ঃ চালান বই নম্বর 02
৩। টাকার পরিমাণ ঃ লাইসেন্স/ নবায়ন ফি = 2000/-
সাইনবোর্ড কর =
সারচার্জ =
মোট টাকা (অংকে) =
মোট টাকা (কথায়) =
স্ক্রল নম্বর তারিখ

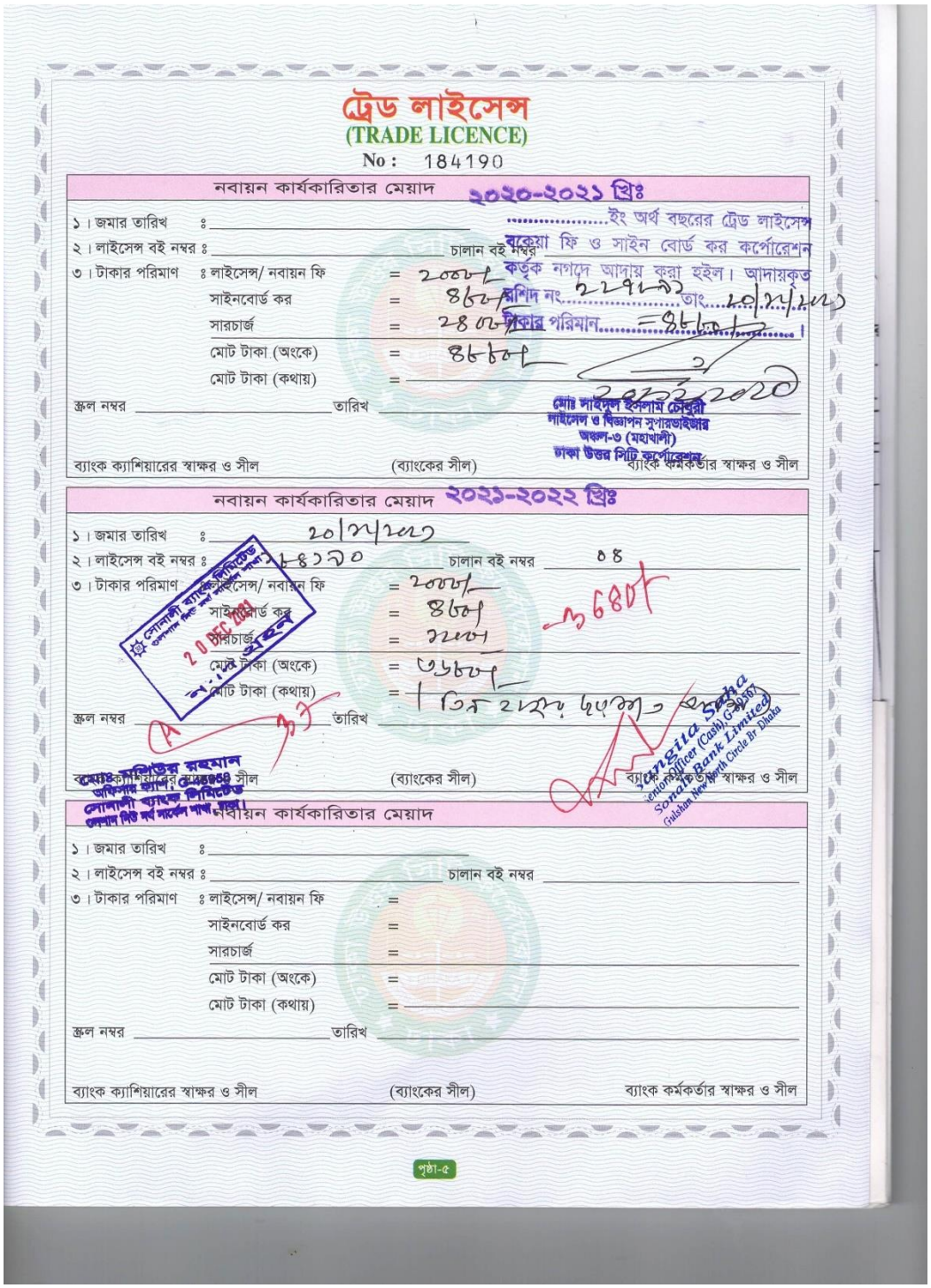
16 JAN 2020

Kaniz Fatema
Senior Officer (Cash)

Md. ... Uddin
Senior Officer (Cash)
Joint Custodian (C)
Sonali Bank Limited
Mohakhali Br. Dhaka

ব্যাংক ক্যাশিয়ারের স্বাক্ষর ও সীল (ব্যাংকের সীল) ব্যাংক কর্মকর্তার স্বাক্ষর ও সীল

পৃষ্ঠা-৪



ট্রেড লাইসেন্স
(TRADE LICENCE)
No : 184190

নবায়ন কার্যকারিতার মেয়াদ ২০২০-২০২১ খ্রিঃ

১। জমার তারিখ ঃ .....ইং অর্থ বছরের ট্রেড লাইসেন্স
২। লাইসেন্স বই নম্বর ঃ চালান বই নম্বর বকেয়া ফি ও সাইন বোর্ড কর কর্পোরেশন
৩। টাকার পরিমাণ ঃ লাইসেন্স/ নবায়ন ফি = ২০০০/- কর্তৃক নগদে আদায় করা হইল। আদায়কৃত
সাইনবোর্ড কর = ৪৬০/- রশিদ নং ২২৭১৯২ তাং ২০/২/২০২১
সারচার্জ = ২৪০/- টাকার পরিমান = ৪৬৮০/-
মোট টাকা (অংকে) = ৪৬৮০/-
মোট টাকা (কথায়) =
স্ক্রল নম্বর তারিখ ২৩/২/২০২০

মোঃ লাইসুল ইসলাম চৌধুরী
লাইসেন্স ও বিজ্ঞাপন সুপারভাইজার
অঞ্চল-৩ (মহাখালী)
ঢাকা উত্তর সিটি কর্পোরেশন

ব্যাংক ক্যাশিয়ারের স্বাক্ষর ও সীল (ব্যাংকের সীল) ব্যাংক কর্মকর্তার স্বাক্ষর ও সীল

নবায়ন কার্যকারিতার মেয়াদ ২০২১-২০২২ খ্রিঃ

১। জমার তারিখ ঃ ২০/২/২০২১
২। লাইসেন্স বই নম্বর ঃ ২১৪১২০ চালান বই নম্বর ০৪
৩। টাকার পরিমাণ ঃ লাইসেন্স/ নবায়ন ফি = ২০০০/-
সাইনবোর্ড কর = ৪৬০/-
সারচার্জ = ২২০/-
মোট টাকা (অংকে) = ৩৬৮০/-
মোট টাকা (কথায়) = ৩৬৮০/-
স্ক্রল নম্বর তারিখ

সোনালী ব্যাংক লিমিটেড ২০ FEB ২০২১

Sangita Sarna
Senior Officer (Cash) (G-2)
Sonali Bank Limited
Gulshan New North Circle Br Dhaka

ব্যাংক ক্যাশিয়ারের স্বাক্ষর ও সীল (ব্যাংকের সীল) ব্যাংক কর্মকর্তার স্বাক্ষর ও সীল

নবায়ন কার্যকারিতার মেয়াদ
১। জমার তারিখ ঃ
২। লাইসেন্স বই নম্বর ঃ চালান বই নম্বর
৩। টাকার পরিমাণ ঃ লাইসেন্স/ নবায়ন ফি =
সাইনবোর্ড কর =
সারচার্জ =
মোট টাকা (অংকে) =
মোট টাকা (কথায়) =
স্ক্রল নম্বর তারিখ

ব্যাংক ক্যাশিয়ারের স্বাক্ষর ও সীল (ব্যাংকের সীল) ব্যাংক কর্মকর্তার স্বাক্ষর ও সীল

পৃষ্ঠা-৫

E-TIN	

Government of the People's Republic of Bangladesh

National Board of Revenue

Taxpayer's Identification Number (TIN) Certificate

TIN : 419998293269

This is to Certify that **Technuf Limited** is a Registered Taxpayer of National Board of Revenue under the jurisdiction of **Taxes Circle-311 (Company)** , Taxes Zone **15, Dhaka**.

Taxpayer's Particulars :

1) Name : **Technuf Limited**

2) Registered Address/Permanent Address : **High Tower (9th Floor), 9 Mohakhali, Gulshan, Dhaka**

3) Current Address : **High Tower (9th Floor), 9 Mohakhali, Gulshan, Dhaka**

4) Previous TIN : **Not Applicable**

5) Status : **Company**

Date : August 17, 2013

Please Note:

1. A Taxpayer is liable to file the Return of Income under section 75 of the Income Tax Ordinance, 1984.
2. Failure to file Return of Income under section 75 is liable to-
   (a) Penalty under section 124; and
   (b) Prosecution under section 164 of the Income Tax Ordinance, 1984.

Deputy Commissioner of Taxes
Taxes Circle-311 (Company)
Taxes Zone 15, Dhaka
Address : Razzak Plaza (5th Floo), 383, Tongi Diversion Road, Mogbazar, Dhaka Phone : 8318573

N. B: This is a system generated certificate and requires no manual signature.

VAT Registration	

Government of the People's Republic of Bangladesh
National Board of Revenue

Mushak-2.3

Customs, Excise and VAT Commissionerate, Dhaka (North)

Value Added Tax Registration Certificate

This is to certify that the person whose details are given below is carrying on Taxable business and registered under Value Added Tax and Supplementary Duty Act, 2012 (Act No. 47 of 2012)

Business Identification Number (BIN) Details

BIN : 000402427

Name of the person	: Technuf Limited
Registration	: Registered for VAT
Registration Type	: Central
Date of Effect	: 06/2017
Date of Issue	: 18/06/2017

This is a system generated certificate and doesn't require any signature

12 Technical Experts for Performing the Assignment

S. N	Name	Position	Highest Qualification	Work Experience (in year)	Specific work Experience (in year)	Total Time Input (days)
1	Saroj Lamichhane	Team Leader	• **ISACA- 2021** Certified Information System Auditor (CISA) • **Islington College (London Metropolitan University, London)** MSc. Hons in Networking and IT Security	15+	12+	15

❑ Relevant Certifications

Certificate of Achievement

Short Course: CISSP Security

This is to certify that

Saroj Lamichhane

has completed the Short Course: CISSP Security

Grade: Pass (55/100)

13/09/2013

Dr Craig Wright
Lecturer

IT Masters
itmasters.edu.au

Charles Sturt University

CISA Certified Information Systems Auditor.
An ISACA® Certification

ISACA hereby certifies that

Saroj Lamichhane

has successfully met all requirements and is qualified as a Certified Information Systems Auditor;
in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

21174626	29 April 2021	31 January 2025
Certificate Number	Date of Certification	Expiration Date

ISACA

ISACA Chief Executive Officer

2	Bijay Limbu Senihang (Web, Network, Security)	Security Engineer	• **Islington College (London Metropolitan University, London)** BSc. Hons in Networking and IT Security- 2013 • **Certified Ethical Hacker, CEH**	9+	9+	10
	❑ Relevant Certification					

3	Somael Kabir	CTO	• **East West Universtity** BSc in CSE • **Certified Ethical Hacker: CEH, C|CISCO, RHCVA, RHCv5**	16+	16+	92

❑ Relevant Certification

4	Tayeb Khan	Head of IT Infrastructure	• **Jahangirnagar University –** Masters in CS • **State University of Bangladesh -**BSc in CSE • **CCNSP** (Cyberoam Certified Network & Security Professional) • CNSS Certified Network Security Specialist • Red hat Linux System and Network Administrating • Microsoft Certified Professional (MCP) • Professional Cloud Architect • Professional Cloud Network Engineer	11+	11+	92

❑ Relevant Certification

5	Ashish GC	Pentester	• **Islington College (London Metropolitan University, London)** BSc. Hons in Networking and IT Security	9+	9+	92
	❑ Relevant Certification					
6	Prem Basnet (Web, Network, Security)	Pentester	• **Tribhuvan University** BSc. CSIT	5+	4+	92
	❑ Relevant Certification					

7	Akash Kanu (Web, Network, Security)	Pentester	• **Islington College(London Metropolitan University, London)** • Bsc (Hons) Computer Networking and IT Security **Certified Ethical Hacker, CEH**	4+	4+	92

❑ Relevant Certification

CEH ETHICAL HACKER PRACTICAL

THIS IS TO ACKNOWLEDGE THAT

Aakash Kanu

IS AWARDED THE "CERTIFIED ETHICAL HACKER (PRACTICAL)" CERTIFICATION
FOR COMPLETING THE RIGOROUS CHALLENGES GIVEN IN THE STIPULATED TIME.

ISSUE DATE: **25 June, 2021** EXPIRY DATE: **24 June, 2024**

CERTIFICATION NUMBER
ECC1849035267

EC-Council

Sanjay Bavisi, President

12.1 Resources information

S. N	Name	Position	Highest Qualification/ Certifications/Research /Training	Work Experience (in year)	Specific work Experience (in year)
1	**Eric Miller**	**System Administrator**	**BS in Computer Science**, University of Maryland Baltimore County, May 2018 Computer Gaming and Simulation programming, Montgomery College, Jan 2011 **Security Clearance** • IRS Cleared, Public Trust, MBI (Active) • CJIS Clearance **Certifications and Training** **Certificates** • Splunk Core Certified User • CMMI Appraisal Team Member	**11+**	**8+**
2	**Abhishek Jha**	**Project Manager**	**Computer Engineering**, Colorado, Colorado State University	**11+**	**3+**
3	**Eric R Smith**	**Security Analyst**	**Bachelor of Science**, Computer Science Minor: Computer Information System James Madison University, Harrisonburg, VA **Security Clearance** IRS Cleared, public trust, MBI **Certifications and Training** Certificates	**4+**	**2+**

			• NSA approved "Information Systems Security Professionals", NSTISSI No. 4011 certification • CISSP Tools/Frameworks • FireEye Security Products, IDA Pro, Kali, Splunk, Docker, VMWare, Wireshark, Elasticsearch, MS O365, SharePoint, OneDrive		
4	**Fasial Qader**	**Program Manager**	**Doctor of Philosophy (PhD)**, Information Systems, concentration in Cybersecurity under the School of Engineering, University of Maryland, Baltimore County, Maryland, USA **Master's Degree**, Computer Science and Engineering Johns Hopkins University, Baltimore, Maryland, USA **Bachelor's Degree**, Computer Science, minor Mathematics, University of Wisconsin, Oshkosh, Wisconsin, USA **Security Clearance** • Clearance Level, Certifying Agency • Example, Top Secret/SSBI, Department of Homeland Security, 2008 **Certifications and Training** • Service Oriented Architecture • CS 800 Computer Science Colloquium	**28+**	**11+**

			• INFS 614 Database Management
			• ISA 562 Information Security Theory/Practice
			• IS 698 Advanced Data Analytics for Cybersecurity
			• IS 733 Advanced Data Mining and Data Analytics
			• IS 805 – Advanced Field Research Methods
			• IS 809 Computational Modeling
			• Authored Research papers on
			  • Computational Models to Capture Human Behavior in Cybersecurity Attacks
			  • Persistent Threat Pattern Detection through Network Traffic Mining
			  • Stress Detection and Analysis: Affective Computing and Cognitive Factors Research
			• Telecommunication Boot Camp
			• Oracle & Sybase Training:
			  • Database Administration
			  • Writing Effective Stored Procedures
			  • Performance and Tuning Replication Server		

5	**Sarwar Hasan**	**Sr. Software Engineer**	• **B.Sc., Electrical Engineering and Computer Science**, Massachusetts Institute of Technology (M.I.T.), Cambridge, MA	**11+**	**10+**

6	**Shah Ahmed**	**MD, Principle Engineer,**	• Bachelor, Computer Science and Chemistry, University of Saskatchewan, Saskatoon, Saskatchewan, Canada, 1983 **Certifications and Training** • Unified Modeling Language (UML), Rational Software Architect (RSA), Rational Rose, Rational Unified Process (RUP), Service Oriented Modeling and Architecture (SOMA) • Design Patterns • Configuration Management, Change Management, Rational ClearCase, Rational ClearQuest • Quality Control, Principle of Testing, Advanced Performance Testing • Enterprise Architecture, Zachman Framework, Gap Analysis • Project Management Principles • JAVA and Enterprise JAVA • CORBA, XML • E-Commerce Components and Architecture • Object Oriented Analysis and Design	**28+**	**15+**
7	**Md Shamsul Arefin**	**Software Engineer**	**Master's Degree**, Computer Science and Engineering University of Texas at Dallas, USA **Bachelor's Degree**, Computer Engineering North South University, Dhaka,	**10+**	**8+**