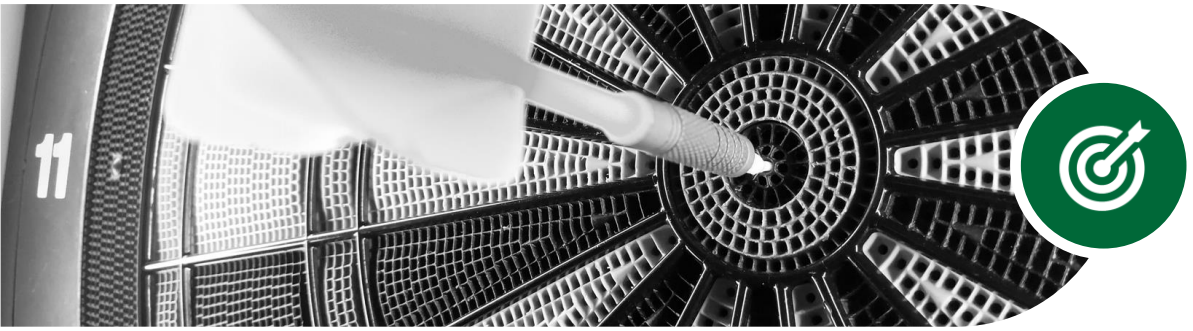
BIM Cybersecurity

Vulnerability Assessment and Penetration Testing Services | 2021

VISION

Transforming Myanmar by **solving business problems** through **innovative digital technologies and solutions**



MISSION

Become the **Trusted** long-term Business and Technology Partner to provide transformation into digital while managing the technology challenges ahead.

CORE VALUES

Commitment to Customer

We are obsessed with our customer's Success

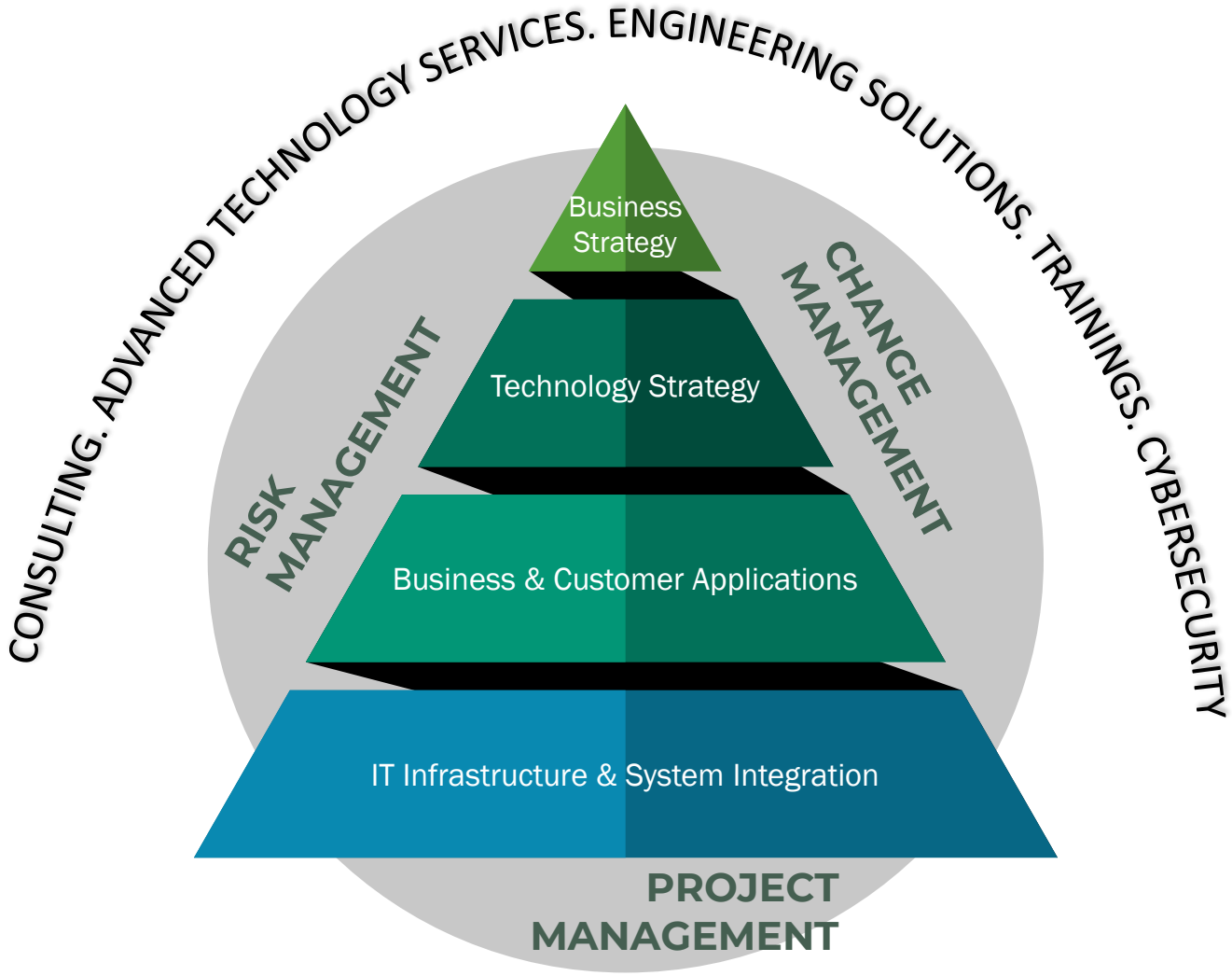
Commitment to Partners

We strive to be the value partner for our suppliers and win together

Be humble

We learn to take nothing for granted

BIM Group's Strategy



BIM Group's Capabilities

PEOPLE

Trainings

TECHNOLOGY SOLUTIONS

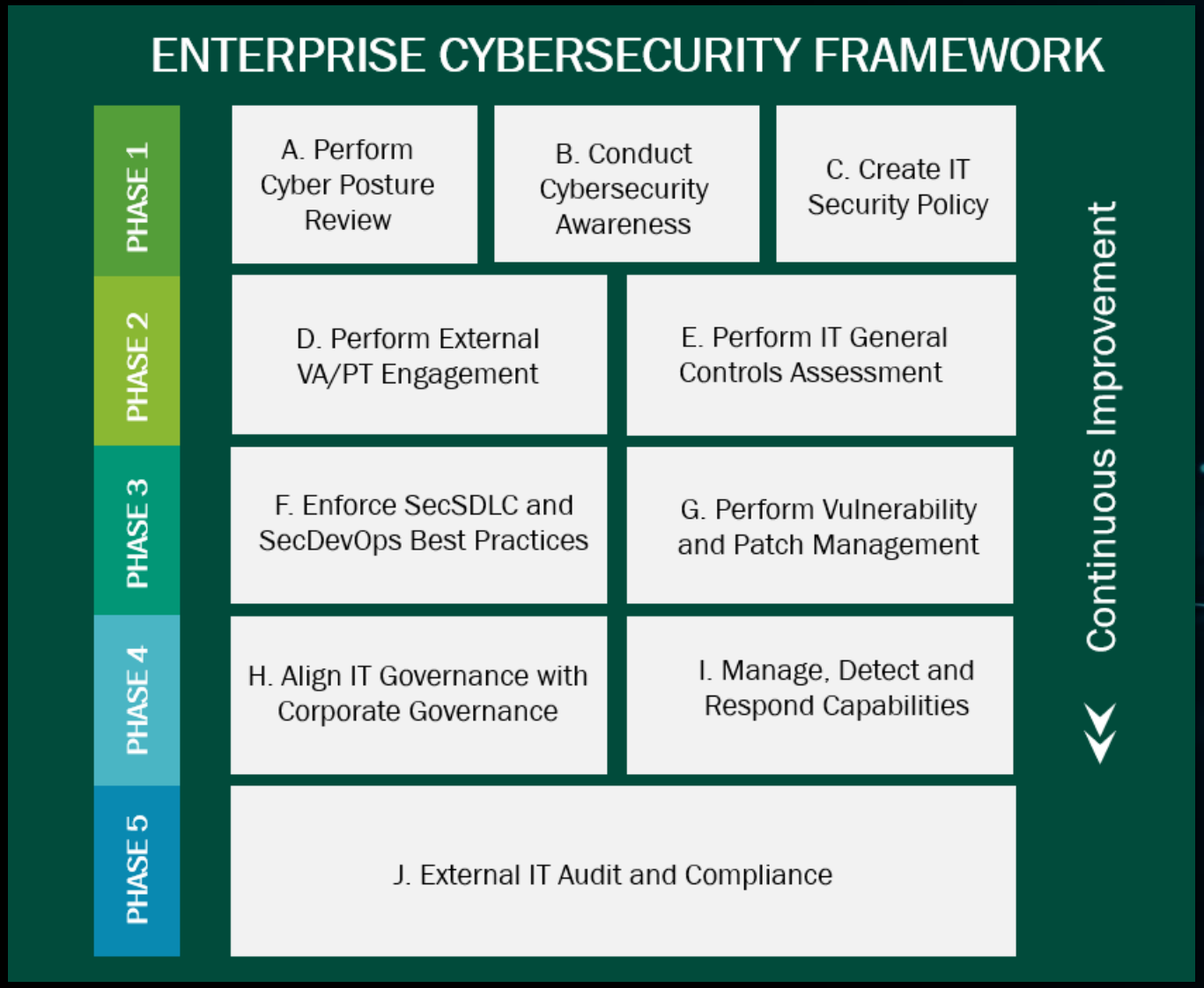
- Business Applications (ERP, CRM, CORE Banking)
- Business & Data Analytics
- Enterprise Mobility and Modernize Communication Services
- Technology Risk and Cybersecurity Services
- Cloud & Infrastructure Solutions
- Smart Engineering Solutions

INDUSTRY EXPERTISE

Financial Services	★ Banking ★ Insurance ★ Microfinance
Retail	★ Textile & Garment Factory ★ Wireless Communications ★ Telecoms ★ Grocery
Healthcare	★ Hospitals
Hospitality	★ Hotels ★ Resorts
Manufacturing	★ FMCG

IT GOVERNANCE & MANAGES SERVICES

- IT Services Management & Governance
- IT Infrastructure Management
- End-Users IT Services
- Managed Security Services



Guide to Managing Your Cybersecurity

Our approach to VAPT in the Digital Cloud

Penetration Testing of the Public Internet Facing Digital Applications and Infrastructure

The public internet facing digital applications and infrastructure can be of the starting reconnaissance point of entry for many cyber criminals and frequently used as the first vector of attack. From the Risk Management perspective, it is crucial to detect and eliminate potential vulnerabilities on the internet facing infrastructure, as it will create an opportunity for attackers to gain an entry point into your Enterprise. Performing regular vulnerability scans and penetration tests can greatly decrease the risk of a security breach and can help better understand the overall security posture of the applications and infrastructure

Our approach

- Black-box and grey-box testing
- Fuzzing and identifying potential attack vectors
- Manual verification of identified vulnerabilities

Penetration Testing of an internal cloud or hybrid infrastructure

This part of test assumes the presence of an attacker within the internal network of the company in the "trusted zone" and to find out whether the infrastructure is virtualized, or a hybrid configuration is in place. The goal and aim for this test is identify vulnerabilities within the internal network and assess the possibility and impact of a potential, successful exploitation which can result in multiple risk areas such as loss of confidential information, breach of privacy laws for compliance and regulatory reasons and loss of trust from employees, partners and shareholders through the reputation damage caused by the breach.

Our approach

- Penetration testing within the internal network
- Identification of key business systems and security mechanisms
- Assessing the possibility of identified vulnerabilities to get unauthorized access to restricted resources.

Manual review of cloud configuration and key, selected hosts

During this part of the assessment, we verify the security configurations of the cloud subscription, as well as the configuration of selection of hosts that is critical from the business and risk perspective. We verify the controls against the industry's cloud best practices and standards. The manual review of access controls, implementing logging and monitoring mechanisms and encryption is a great way not only to defend against a remote attacker, but also to protect against an insider threat and possibly the early detection to ensure that the proper controls and risk management practices are in place.

Our approach

- Verify security mechanisms in place and cloud configuration against industry's best practices and guidelines / standards i.e. CSA's Security Guidelines
- Thorough inspection of critical systems, key digital assets, applications and hosts

Identify your Risks

- **Where are you most vulnerable?**

Finding out which business applications, systems, cloud infrastructure or mobile devices could have weaknesses.

- **Do you have appropriate controls in place?**

It is very likely that the vulnerabilities exists without proper defenses are in place and even if you do, how effective are they?

- **What can you do about it?**

The investments and decisions need to be made to either to mitigate or accept the risks but understanding the potential impact would be crucial.

- **Next steps**

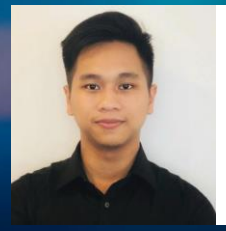
Talk to BIM Cybersecurity to learn more about how we can assist you with your Cybersecurity Journey.

Contact us

and learn more

Mike Phone Myint

Managing Director
BIM Cybersecurity
mikemyint@bimgoc.com
LinkedIn



Nay Myat Min

Manager
BIM Cybersecurity
naymyatmin@bimgoc.com
LinkedIn

BIM CYBERSECURITY

OCP ES HACKATHON Microsoft WINNER

Winner Microsoft Partner 2020 Partner of the Year Myanmar Microsoft

Winner Microsoft Partner 2021 Partner of the Year Myanmar Microsoft

© 2021 BIM Cybersecurity. All rights reserved. BIM Cybersecurity is part of BIM Group and refers to the Business Unit which has its own legal an separate entity. This content is for generation information purposes only and should not be used as a substitute for consultation with professional advisers and consultants. At BIM, our purpose is to solve important business problems using innovative digital technology solutions and to build trusted long term business technology partner relationship with our clients. Find out more about us at www.bimgoc.com.