VIMRO
OUTCOME AS A SERVICE

The Demystification of Successful Cyber Security!

The financial and operational benefits of holistic customized cyber security solutions.

VIMRO's Cyber Security Enabling Methodology Overview

In order to avoid exposing your company, its clients, your employees (not to mention yourself!) to cybercrime, it is vital to invest in a good cyber security program. VIMRO's approach to an effective cyber security program involves a holistic security methodology. Our methodology maximizes value and effectiveness because we have combined the most efficient tactics to include frameworks, best practice guides, and work papers from reputable security organizations such as NIST, ISO2700/27002 and MITRE.

Combining vetted complementary frameworks yields a program that is effective and yet efficient; a program dynamic enough to anticipate new risks, yet iterative enough to become familiar. Equally important, a holistic methodology prevents oversights within your program. For example, while a cyber security framework alone equips you with the controls you must implement and manage, it leaves you without the metrics you need to validate those controls and the overall success of your cyber security system.

A successful methodology is dynamic, adapting to ever-changing threats; and that can only happen if you treat it as an evolving process. For any methodology to work, you must adopt it in a controlled, systematic manner. Implementing a cyber security program too quickly or without the adequate resources reduces its effectiveness and demotivates the team members involved.

12100 Sunrise Valley Dr. Suite 290-1 Reston, VA 20191

The Demystification of Successful Cyber Security!

The following is an overview of a VIMRO cyber security system:

- The foundation of our security system first aligns your organization's business needs with your IT security, allowing you to focus on the critical business applications, systems, and processes that need strong security controls. For example, when you implement a new application, include a security representative in the development of the budget and project plan. This is how you ensure that time and resources are allocated for security controls throughout the project; and for support throughout the new application's lifecycle. If you overlook security requirements in the beginning stages of a project, the application and associated systems may require rework for failure to meet your company's approved security standards. And rework, delays, or budget excesses invariably reduce your new application's ROI. (See VIMRO's paper: Omitting Static Code Security Analysis Can Cost You. BIG!)
- The second layer of our foundation includes implementing a security framework. Many of VIMRO's clients have adopted either the NIST Cybersecurity Framework(1) or ISO27001/ISO27002(2).
- Along with the framework, organizations have adopted a cyber security Capability Maturity Model (CMM) that involves a strategy to optimize critical security controls, mechanisms, and processes (Level 5 in the CMM). The cyber security CMM includes:
  - Level 1 – Initial: Processes are unpredictable, poorly controlled, and reactive
  - Level 2 – Managed: Processes are characterized for projects and are still often reactive
  - Level 3 – Defined: Processes are characterized for the organization and are proactive, taking their procedures from the organization's standards
  - Level 4 – Quantitatively Managed: Processes are measured and controlled
  - Level 5 – Optimizing: Focuses on process improvement
- To manage performance leading toward the optimal level (Level 5) in the security CMM, we recommend Key Performance Indicator (KPI) metrics. Many clients start with MITRE Cyber Resiliency Metrics(3).
- VIMRO policies, standards, and procedures include all of the verbiage necessary to raise your organization to the upper levels of the cyber security CMM. These are critical to success. Without these, your organization will not even surpass Level 2 in the security CMM.
- After writing your security policies, standards, and procedures, we implement technological mechanisms (these include IPS, DLP, SIEM, and so forth) to support your cyber security program, and train workforce members to apply the requirements of the formal documents to their practices
- VIMRO's risk management program includes continuous evaluation of your technological mechanisms and processes to validate them, and find areas, which need improvement, so that your company always maintains optimized security controls.

[1] NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/
[2] ISO 27001/27002: http://www.27000.org/
[3] MITRE Cyber Resiliency Metrics: https://register.mitre.org/sr/12_2226.pdf

(800) 272 0019
Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL

The Demystification of Successful Cyber Security!

VIMRO
OUTCOME AS A SERVICE

For any items that do not meet KPI, we implement a Corrective Action Plan, which sets expectations dates for the resolution of any issues cited.

Below is an example application of the VIMRO methodology to one specific security control item: a firewall. The NIST Cybersecurity Framework includes Configuration Management in the family of controls. Using the firewall as our example:

- An organization includes firewall configuration requirements in a policy; procedures are written for how the firewall will be implemented and managed.
- The procedure includes a baseline security assessment vulnerability report. The baseline is to be updated whenever a change is made on the firewall.
- The policy, procedure, and baseline reports define the controls (CMM Level 3) for the firewall.
- In order to determine if the company is maintaining controls for the firewall to meet CMM Level 4, the firewall is audited using KPIs (a common approach is to conduct firewall configuration audits every six months).
- Some examples of KPIs include:
  - There must be a change record for each change made to the firewall. The acceptable KPI for changes without corresponding records is 0.
  - A vulnerability assessment report must not result in high or medium scores. The acceptable KPI for high or medium findings in a vulnerability assessment is 0.
- If during firewall configuration audits, some findings do not meet the KPI requirements, it is an opportunity to determine why this is the case. Perhaps there are too few people to meet the KPI objectives; perhaps skillsets are lacking and training on maintaining the firewall is necessary. For any items that do not meet KPIs, we implement a Corrective Action Plan (CAP), which sets expectation dates for the resolution of any issues cited. We conduct an audit immediately after said date to ensure that the items have been improved based on the CAP. This is an example of an optimized process (Level 5) for firewall controls practices.

Authored by VIMRO's Cybersecurity Leaders

(800) 272 0019

Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL

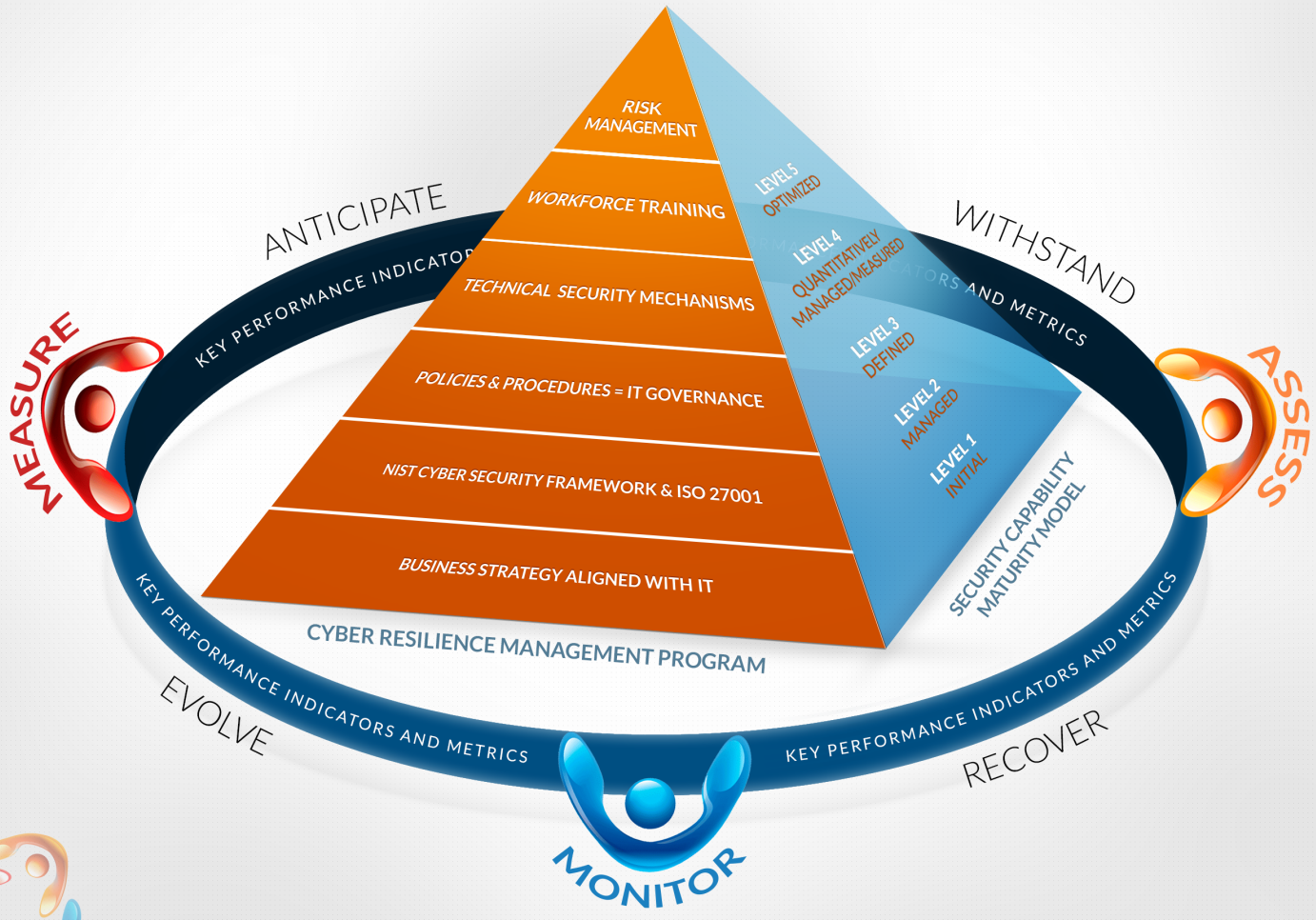
The Demystification of Successful Cyber Security!

VIMRO
OUTCOME AS A SERVICE

"The holistic approach arms your organization to prevent, detect, and respond to cybercriminal attacks....."

All layers of our Cyber Security Enabling Methodology are equally critical and require your steady dedication. Systematic attention to each level of the process yields a solid foundation today that is also dynamic enough to safeguard you going forward. VIMRO's holistic approach arms your organization to prevent, detect, and respond to cybercriminal attacks that threaten your business, clients, employees, or sensitive data.

The VIMRO Cyber Security Enabling Methodology



services@vimro.com

Contact VIMRO to learn more details about our approach and how we can help you build and maintain an Optimized Cybersecurity Risk Management Program.

Authored by VIMRO's Cybersecurity Leaders

(800) 272 0019

Ashburn, VA | Baltimore, MD | Boston, MA | Glendale, CA | Las Vegas, NV | Reston, VA | San Diego, CA | Tampa, FL