# ARM YOUR BUSINESS

## ASSESS, REMEDIATE, MANAGE

12 Step Managed
**Cybersecurity Program**

START WITH A
**SECURITY MATURITY LEVEL ASSESSMENT**

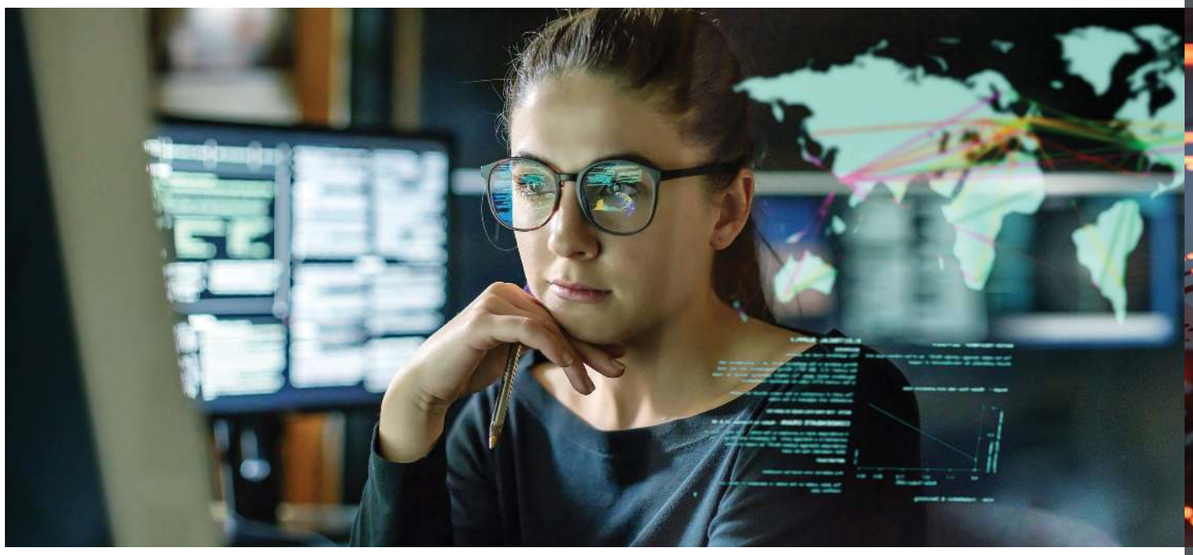
Our unique 12 step Managed Cybersecurity Program starts with a comprehensive assessment that lays the foundations to secure your business.

Inovo **InfoSec**
THREE DIMENSIONAL CYBERSECURITY

# ARM YOUR BUSINESS
# ASSESS, REMEDIATE, MANAGE

## 01 CONDUCT
## SECURITY MATURITY LEVEL ASSESSMENT (SMLA)

After completion of the SMLA, your business will have a documented map of sensitive information and assets as well as a full understanding of your technology landscape. The SMLA includes a full Risk Assessment that will identify risks to business systems. Information will have been identified and assessed, and senior management will be aware of where and how they might get breached.



## 02 CREATE
## vCISO-LEAD INFORMATION SECURITY COMMITTEE

An InfoSec committee is in place and any conflicting duties and responsibility are segregated. Every quarter, senior management continue to assess and measure risk reduction, report on incidents and threats, easure the performance of controls, review policy violations and security plan implementation progress. The business understands where the risks are and the plan to remediate them.



ARM YOUR BUSINESS
ASSESS, REMEDIATE, MANAGE

## 03 CREATE
## INFORMATION SECURITY POLICY AND PROCEDURES

The rules for business technology systems have been determined and agreed upon by the relevant parties. Policy and control requirements have been tailored by senior management. The business has identified where sensitive information can be stored, how it can be shared, and who owns it. Accountability for all confidential and sensitive information has been assigned to a sole owner.


## 04 UNDERTAKE
## SECURITY POLICY AND EMPLOYEE AWARENESS TRAINING

Each business unit has been trained on security policies, the acceptable use of assets, where sensitive information is allowed to be stored, how it can be shared, and who owns it. Users understand the common causes of unintentional data exposure such as emailing confidential documents to the wrong person due to auto complete, as well as common email phishing tactics, phone and impersonation scams, how to identify them, and how to report them.

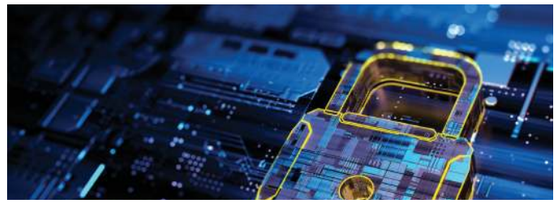
## 05 24/7/365 SECURITY OPERATIONS CENTER (SOC) **ONGOING ALERT MONITORING, INVESTIGATION AND ESCALATION**

A team of Security Analysts (the SOC) reviews logs for indications of compromise around the clock and follows a written Incident Response Plan to investigate and evaluate potential incidents.

## 06 **INTRUSION DETECTION AND DATA LOSS PREVENTION** SOFTWARE IMPLEMENTED

Intrusion detection software scans for threats. At least 90 days of detailed forensic audit logs are retained that show who logged into systems both on-site and remotely, what they did with their access, any changes to system permissions and access, any indicators of attack and compromise, and intrusion attempts.

## 07 IMPLEMENT, AUTOMATE, AND REPORT ON THE **CRITICAL SECURITY CONTROLS**



The business is now operating at an acceptable level of risk. Each security control in the Business System Security Plan has been implemented, automated, measured, and reported to the senior management team on a monthly, quarterly and annual basis. A continuous cycle of audit and control testing is in place.



ARM YOUR BUSINESS
**ASSESS, REMEDIATE, MANAGE**

## 08 CREATE **INCIDENT RESPONSE PLAN**

A written Incident Response Plan is in place: this will be tested on a minimum annual basis. Using this plan, the business is properly prepared to respond to and recover from real data breach incidents.

## 09 REVIEW **CYBERSECURITY INSURANCE POLICY**

Cybersecurity insurance requirements have been reviewed and the correct policy put in place. The business can recover some financial losses if any controls are breached.

## 10 COMPLIANCE PORTAL **GOES LIVE**

The Compliance Portal acts as a central repository for all Security Policies, Risk Assessments, System Security Plan, Quarterly Security Committee actions, and evidence of compliance with control frameworks and regulations.

# ARM YOUR BUSINESS
# ASSESS, REMEDIATE, MANAGE

## 11 ONGOING RISK AND VULNERABILITY MANAGEMENT

Vulnerability scans are undertaken weekly ensuring that the business is always aware where vulnerabilities are and if they're being actively attacked. As part of the plan for continuous improvement, the relevant business units meet at least monthly to identify and review new and ongoing vulnerabilities that a threat actor could exploit.

## 12 PENETRATION TESTING

An annual Penetration Test enables the business to understand if the Security Controls are effective in a real-world scenario. A Pen Test is undertaken by a Certified Ethical Hacker who is sanctioned to attack the organization using a blend of real threat actor tactics.