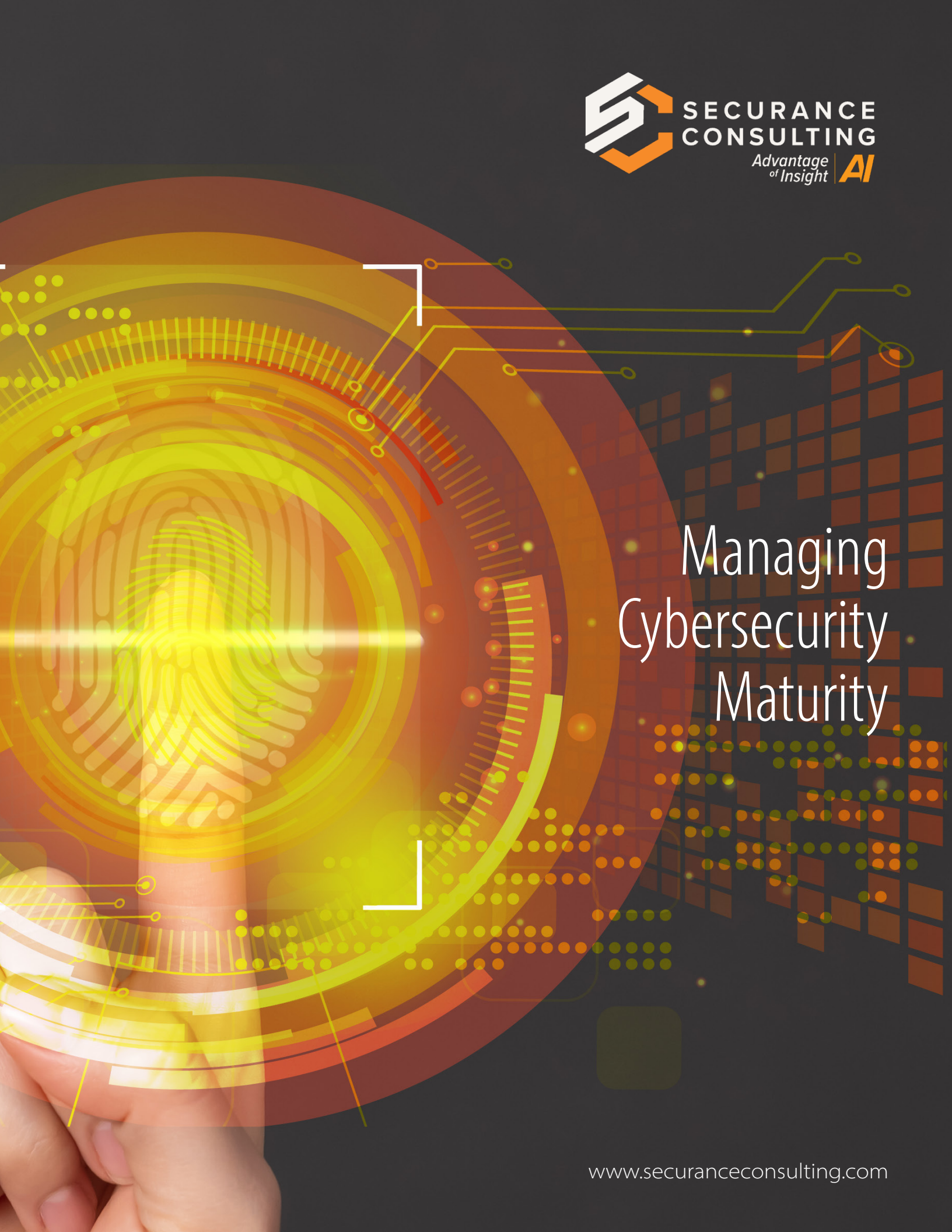
SECURANCE CONSULTING

Advantage of Insight | AI



Managing Cybersecurity Maturity

www.securanceconsulting.com

WHAT IS CYBERSECURITY MATURITY?

Not all people reach peak maturity— but security systems can get pretty close. Cybersecurity maturity refers to how effectively an organization supports its security defenses through all stages of business growth and operations. As an organization evolves, its needs change, as well. This means a mature cybersecurity program entails keeping a laser focus on continuous improvement.

Cybersecurity maturity is a model that ensures IT process and technology improvement is just as consistent and disciplined as other aspects of an organization's operations. It requires executive involvement, planning, and proactive improvement to ensure a high level of preparedness for thwarting cybersecurity threats.[1] The goal is to leave reactive security approaches behind and create an intelligence-driven approach to strengthening security posture.

While it seems that every company has its own maturity model, making it difficult to know where to begin, this paper will introduce some popular models and what elements make them effective gauges of an organization's security program maturity. It will also detail helpful steps organizations should consider before taking the plunge to assess cybersecurity maturity.

> "Cybersecurity is a discipline that needs consistent, repeatable, continuous action to be effective."[1]

WHY TRACK MATURITY?

First things first: What's in it for us?

Implementing new controls and technologies to beef up an existing system, while helpful and oftentimes necessary to respond to evolving cyberattacks, does not guarantee an optimal security posture— only a defensive one. Tracking maturity allows organizations to measure their cyber threat preparedness over time, in the context of their business, with a focus on repeatable outcomes, and with meaningful detail.[1]

The challenge with battling security threats with layers of defenses, such as firewalls, intrusion prevention and detection systems, anti-virus software, and physical access controls, is that each layer comes with its own data. The more data introduced into an IT environment, the more strain on resources— technological and human. On top of that, every layer added increases the complexity of the security infrastructure, introducing new threat vectors and creating the need for additional security policies, procedures, and controls.[2]

When maturity is tracked, the initial score can then be compared to subsequent scores, reflecting the progression of security, which can be used to secure larger budgets, plan future IT goals, and serve as tangible proof of the current state of control. Armed with this information, organizations can spend more time focusing on improving specific facets of security and less time in hour-long meetings arguing about which areas require the most attention.

Let's not forget the human element. Tracking maturity involves honing in on processes and people, who oil the proverbial machine. For example, if an organization discovers much of its cybersecurity success is thanks to only a handful of people, training procedures must be set in place to ensure future employees can handle the systems, technologies, and workloads of current staff without operational disruption.

When IT security processes' maturity is aligned with business goals as well as technology, organizations create a safety net, which allows them to pursue new opportunities, "such as adopting new technologies, expanding markets, and launching new products and services."[2]

Cybersecurity maturity is:

A score to measure an organization's preparedness against threats and gauge progression toward IT goals

A means of condensing the complexity of the current security posture

A measurement that takes into consideration government and industry compliance, the decision-making process, and the effectiveness of controls[1]

HOW DO WE MEASURE MATURITY?

There are a multitude of maturity models out there, so deciding where to begin can be overwhelming. On the other hand, this means organizations have a plethora of resources to review before finding the best fit for their business.

Before assessing cybersecurity maturity, the Chief Information Security Officer (CISO) or equivalent should put together a picture of the organization's IT security risk. This will help establish the organization's objectives as it undertakes the task of determining maturity. Such assessments might include:

- Ensuring security policies are aligned with regulatory and business requirements.
- Confirming threat and vulnerability management processes are agile enough to evolve and stay ahead of the growing threats.
- Verifying security operations are active and diligent in protecting assets, and swift to identify attacks against the organization.
- Ensuring security strategies are built to look beyond the immediate, or tactical, and bring innovative and cost-effective solutions to fruition.
- Confirming that security and compliance efforts ensure controls are designed properly and operating effectively.[2]

> Tracking maturity takes the focus off of random metrics, like number of incidents resolved, systems patched, or compliance boxes checked.[3]

MATURITY MODELS

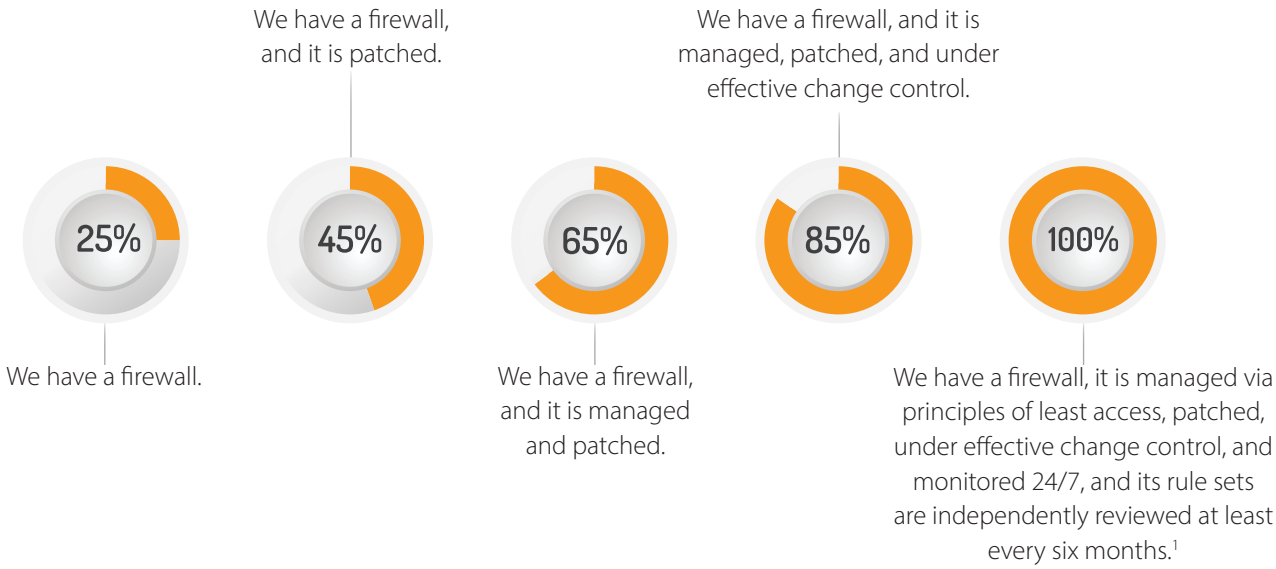
Maturity models provide clear-cut ranking systems to measure the effectiveness of an organization's risk management program. They're intended to help reduce risk by identifying more efficient processes for vulnerability management and responding to security threats and breaches. Honestly, security will never be perfect, and maturity models are not designed to get an organization to a definite end state. That being said, knowing that security is never finished is an important advantage.[5] It allows organizations to have the mindset of continuous improvement. If and when ground is lost in security maturity, the framework of a maturity model will help put things back on track.

We'll start with a model many organizations use to evaluate their information system maturity, though the model wasn't originally created for that purpose. The U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) lays out five Functions, which are further broken down into Categories and Subcategories of activities to be analyzed (see Table 1 below). The Functions are: Identify, Protect, Detect, Respond, and Recover. The following Tiers are used to score each Function's Categories:

As with maturity models, following NIST CSF is not a "one-and-done" exercise. The purpose of using the model is to take a snapshot of the organization's risk profile and determine if the current cybersecurity program is sufficient to deter threats and accomplish business goals. Similarly, it is up to the organization to determine which Tier is acceptable for each Category. It may not be necessary for all areas to reach Tier 4. It will be up to the organization to determine if reaching Tier 4 will have a significant impact on its risk profile, taking into consideration a cost-benefit analysis and other factors.

NIST's actual maturity model is PRISMA, or the Program Review for Information Security Assistance. It is comprised of five levels, including Policies, Procedures, Implementation, Test, and Integration. PRISMA goals are summarized here.

The progression of maturity for a firewall



The NIST Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

How to Measure Your Organization's Cybersecurity Maturity, IT World Canada, 2017

> Security maturity is a process with no defined finish line— and any ground gained can be lost.

A second maturity framework is Control Objectives for Information Technology (COBIT), a scale that challenges enterprises right from the start, as there is a large gap between the requirements for Level 0: Incomplete and Level 1: Performed. In order to attain a higher level, an organization must go from not having an IT process implemented to having that process implemented and its purpose entirely achieved.

A third model, the Project Management Maturity Model (P3M), helps organizations evaluate and compare their own practices to industry best practices and their competitors, its purpose is to map out a clear path for improvement and show businesses how well they manage projects, with the ultimate goal of improving enterprise efficiency by identifying, analyzing, and optimizing project management processes.[7]

Maturity Models for Information Security Management (2MISM) is a series of processes for systematically establishing, documenting, and continuously managing procedures to improve the safety and reliability of enterprise assets. It focuses on the confidentiality, integrity, and availability of sensitive information, as well as establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security management systems.[7]

Lastly, but certainly not least in popularity, is Gartner's ITScore model, developed to help organizations evaluate and improve their information security programs and process maturity across key security and risk management domains:

Business continuity management

Compliance

Identity and access management

Information security

Risk management

While the ITScore methodology is consistent across all roles and domains, the dimensions measured are specific to the respective requirements of each. The common theme of the maturity model will sound familiar— moving beyond traditional IT-centric approaches to security maturity and focusing on improving processes that reach (and benefit) the entire enterprise.

> "A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline."[4]

This model is broken up into five maturity levels:

Level 1: Initial. Existing processes are likely to be ad hoc, disconnected, disorganized, and IT-centric. No formal responsibilities have been assigned to pursue improvements, and no formal program is in place.

Level 2: Developing. Due the increasing recognition of the need for a formal program, management commitment has likely been secured, requirements are being assessed, responsibilities are being assigned, and an implementation plan is being developed to begin improvement efforts.

Level 3: Defined. The scope and objectives of an enterprise-wide program have been established, and processes and performance metrics have been defined. A formal program is now in place, with an identified leader and clear commitment from senior management and other key stakeholders.

Level 4: Managed. Most identified gaps have been closed. Decisions about program activities are based on input from stakeholders across the enterprise and are designed to address the clearly identified needs of the business and, particularly, risks associated with those activities.

Level 5: Optimizing. The program is now recognized as a strategic business imperative enterprise-wide. Accountability for associated risks rests with line-of-business owners, who explicitly accept ownership of residual risk.[8]

A thousand pages could be written about the maturity models available today, but the above models should provide a good idea of what functions maturity models serve and goals that drive them. Each organization hoping to mature its cybersecurity systems should select the model that fits the needs of the business best. Some organizations might find it prudent to even create a hybrid model of their own.

Positive indicators of security maturity include:

- **More automation;**
- **Fewer staff involved in critical processes; and**
- **Measurable progress.[5]**

CONSIDERATIONS

While maturity models provide clear benchmarks for assessing security, there are a few responsibilities organizations must address independently before quantifying the maturity of their information systems. As with any undertaking, organization, planning, and a thorough understanding of the business and its resources are integral to success.

Management commitment. Is everyone on board up top? Assessing cybersecurity maturity takes time and resources, like any project, and those performing the work require strong leadership throughout. Leaders should be prepared to give guidance and tangible goals to ensure the project remains focused, and staff remains committed.

> Controls are defined as any action taken by an organization to manage risk and increase the likelihood that established objectives and goals will be achieved.
>
> *Institute of Internal Auditors*

Performance and acceptable risk. What is the current state of security, and where is it going? Without establishing performance levels and acceptable risk, staff will not know the target state for the security program. Once determined, this information should be shared with the business, so everyone understands the risk involved.

Expectations and measurement. This should be nothing new for seasoned management— strategy should always be informed by clear guidelines and expectations. Communicating the criteria for success to the security team provides clarity and purpose for the project.

Stakeholder involvement. Those with a stake in the project should have their voices heard, so a consensus can be reached regarding which steps will be taken, the acceptable level of risk, and the importance of continuous improvement.

Budget and resources. The big issue: money. Is there enough in the budget to achieve the designated goals in the allotted time? Don't forget about sufficient staff resources, as well.[2]

Helpful hint

Many IT departments underestimate the value of properly inventorying devices— or, they think it's too much of a burden. Particularly in the age of "bring your own device" (BYOD), inventory is critical. Organizations might find asset management software to be particularly helpful when embarking upon the cybersecurity maturity journey. It helps to identify unauthorized cloud applications, Wi-Fi routers, and plug-in desktop storage. If an organization doesn't have enterprise- and employee-owned devices inventoried, the CISO can make the decision to continue the maturity assessment but limit the scope to IT-controlled devices.[3]

CONCLUSION

As with any cybersecurity initiative, the generic goal is to "improve security," but that means different things for different entities. It is up to individual organizations to determine which maturity model will suit their business needs and drive improvement in their security posture. First, a CISO or equivalent should compile the organization's risk profile. This includes evaluating security policies for regulatory compliance, assessing threat and vulnerability management processes, and confirming that security operations identify attacks and protect assets, security strategies yield innovative and cost-effective solutions, and security compliance efforts ensure controls are designed and operating effectively. Then, the organization should follow its cybersecurity maturity model of choice— the one whose grading scale makes the most sense for the IT environment and technologies in question. Decision-makers should ensure that key measures:

- Are sufficiently granular to produce meaningful results;
- Can be appropriately applied to processes and controls; and
- Are repeatable and consistent.[1]

Once an organization determines where on the chosen maturity scale it falls, it can begin the process of improvement, climbing the levels or tiers of the model in pursuit of more effective security procedures, processes, and controls. Each stage of the assessment can reveal additional capabilities, exposures, risks, and considerations regarding where and how the organization can take its cybersecurity maturity to the next level.

It's important to note that not all organizations have the resources, structure, or need to reach the highest level of maturity—and that's okay. Cybersecurity maturity is a journey. The goal isn't necessarily "Tier 4." Rather, it's continuous improvement.

Contact Securance to learn more about how your organization can improve the maturity of your information security program and reap benefits across the enterprise.

> "As with any undertaking, organization, planning, and a thorough understanding of the business and its resources are integral to success."

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

[1] Cyber Security Maturity: What is It?, CNS Group

[2] RSA Archer Maturity Model: IT Security Risk Management, RSA, 2015

[3] How to Measure Your Organization's Cyber Security Maturity, IT World Canada, 2017

[4] Evaluating the Maturity of Cybersecurity Programs for Building Control Systems, Pacific Northwest National Laboratory, 2016

[5] Behind the Curve? A Maturity Model for Endpoint Security, SANS Institute, 2017

[6] A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM), SANS Institute, 2015

[7] Towards a New Maturity Model for Information System, International Journal of Computer Science Issues, Volume 12, Issue 3, 2015

[8] ITScore Overview for Security and Risk Management, Gartner, 2014

Managing Cyber Security Maturity

SECURANCE CONSULTING
Advantage of Insight AI

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com