Unit 42 Cyber Risk Management

Implementing a cyber risk program can be a daunting task. The experts from Unit 42 can deliver tailored cyber risk management solutions appropriate for the size of your organization, your industry, and your current risk management operations maturity level.

Where Are You?

Consider the following characteristics of each "maturity tier" to determine the relative cybersecurity maturity level of your organization.

Table 1: Cybersecurity Maturity Bands and Characteristics

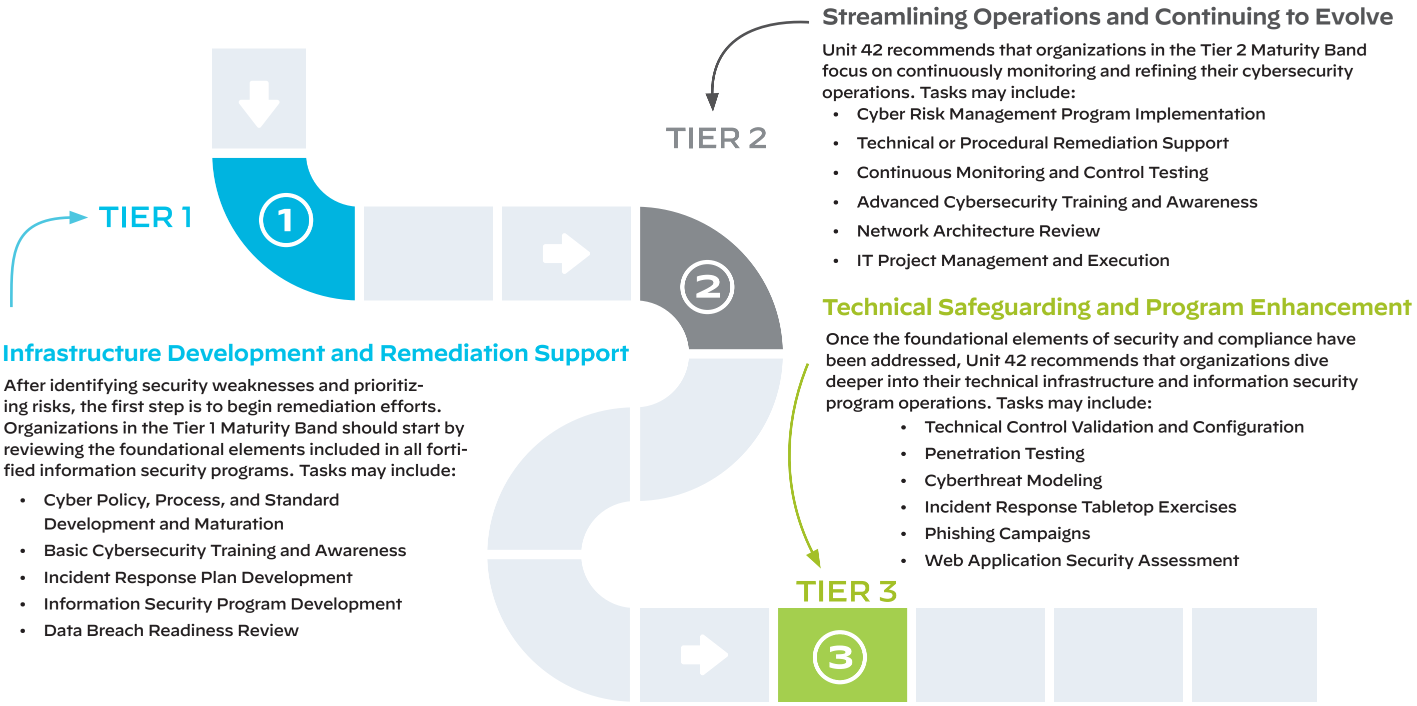
TIER 1	TIER 2	TIER 3
□ Minimal or no documented cybersecurity policies, processes, or standards exist	□ Cybersecurity documentation exists and is aligned to a recognized framework, but does not provide specific action-oriented details	□ Cyber risks have been identified, and remediation efforts are prioritized based on criticality
□ Rapidly expanding or newer company is subject to regulations within the near future	□ Client has recently merged with or acquired organizations	□ Personnel have demonstrated a security-first mindset and do not fall victim to common phishing emails, etc.
□ Limited security training and awareness exists among personnel	□ Cyber risks have been identified, but remediation efforts are not streamlined or prioritized based on criticality	□ Cyber Risk Assessments and Technical Testing is conducted on a predetermined, ongoing timeline
□ Cyber Risk Assessment has never been conducted or has not been conducted within the previous 18 months	□ Technical controls are in place, but the network infrastructure has not been tested with Offensive Security exercises	□ Cybersecurity documentation exists, is aligned to a selected framework, and clearly defines the security expectations and operations of the organization

Establishing which maturity tier your organization fits into is the first step in strengthening your overall security posture. The next step is to conduct an assessment based on where you're starting, and then develop a plan against which to execute.

Where Are You Going?

Cyber Risk Assessment

A Cyber Risk Assessment aids in identifying organizational strengths, weaknesses, and opportunities. Unit 42 recommends a Cyber Risk Assessment to clients looking to gain a better understanding of their cybersecurity landscape and the risks associated with their current security posture. Figure 1 shows the tasks that correlate to the maturity tier of your organization.



Streamlining Operations and Continuing to Evolve

Unit 42 recommends that organizations in the Tier 2 Maturity Band focus on continuously monitoring and refining their cybersecurity operations. Tasks may include:

- Cyber Risk Management Program Implementation
- Technical or Procedural Remediation Support
- Continuous Monitoring and Control Testing
- Advanced Cybersecurity Training and Awareness
- Network Architecture Review
- IT Project Management and Execution

Technical Safeguarding and Program Enhancement

Once the foundational elements of security and compliance have been addressed, Unit 42 recommends that organizations dive deeper into their technical infrastructure and information security program operations. Tasks may include:

- Technical Control Validation and Configuration
- Penetration Testing
- Cyberthreat Modeling
- Incident Response Tabletop Exercises
- Phishing Campaigns
- Web Application Security Assessment

Infrastructure Development and Remediation Support

After identifying security weaknesses and prioritizing risks, the first step is to begin remediation efforts. Organizations in the Tier 1 Maturity Band should start by reviewing the foundational elements included in all fortified information security programs. Tasks may include:

- Cyber Policy, Process, and Standard Development and Maturation
- Basic Cybersecurity Training and Awareness
- Incident Response Plan Development
- Information Security Program Development
- Data Breach Readiness Review

Figure 1: Priorities by organizational maturity level

Unit 42 Can Help Stop Attacks Before They Start

Unit 42 offers CRRM services to assist organizations in achieving their unique security goals. Our team of elite professionals is dedicated to proactively identifying and assessing cybersecurity risks across people, processes, and technology.

Our experts will create a personalized mitigation roadmap detailing the requirements to reach your organization's security goals as well as assist with remediation activities to mature your information security programs.

Information Governance and Compliance

Unit 42 risk management experts work with your organization to determine its level of sophistication related to information governance and to ensure compliance with necessary standards applicable to your industry.

Unit 42 Information Governance and Compliance Services

- **Cybersecurity Framework Assessment:** This assessment establishes your organization's cyber resilience according to frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and Center of Internet Security (CIS) Top 20. Our team identifies the current risks facing your organization's cybersecurity infrastructure and works with you to develop a strategic plan and maturity roadmap for an enhanced information security program.
- **Regulated and Contract-Based Cybersecurity Assessments:** This assessment maps to the control requirements of contractual, state, and regulatory frameworks (e.g., CCPA, GDPR, HIPAA, NYDFS). Our team evaluates control requirements, finds and remediates gaps, and demonstrates compliance.
- **Governance, Risk, and Compliance (GRC) Solution Assessment and Deployment:** As part of the GRC assessment, our team performs an in-depth assessment to determine the most appropriate GRC tool for your organization. We deploy the selected solution throughout your organization, including the transfer of legacy GRC records into the new GRC environment. We also provide training for your personnel to ensure the solution is leveraged in a streamlined fashion.

Technical Testing and Offensive Security

Unit 42's technical assessment team tests your people, processes, and technology to evaluate your organization's cybersecurity posture and overall cyber resilience.

Unit 42 Technical Testing and Assessment Services

- **Penetration Testing:** Our technical experts will simulate a real-world cyberattack to assess the strength of your countermeasures and identify hidden security vulnerabilities.
- **Vulnerability Assessments:** Unit 42 conducts a technical assessment to identify vulnerabilities and security weaknesses throughout your environment. Our team identifies known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation actions.
- **Compromise Assessments:** Our compromise assessment, based upon your organization's data, logs, and existing telemetry, identifies whether there are any indicators of compromise or threat actors present in the environment.
- **Web Application Security Assessment:** The Unit 42 team evaluates web applications for vulnerabilities, including flaws in development, configuration, deployment, upgrade process, maintenance, or third-party add-ons.
- **Cyberthreat Modeling:** Unit 42 experts identify and prioritize threats, determining likely attack vectors and the information assets threat actors are most likely to target.

Information Security Program Development

The Unit 42 advisory team helps your organization mature its information security program.

Unit 42 InfoSec Development Services

- **Virtual Chief Information Security Officer (vCISO):** A Unit 42 vCISO can aid your organization in developing and implementing a cybersecurity strategy, evaluating risk and providing risk mitigation steps, and serving in an executive-level capacity to oversee risk management and security communications with your C-suite and board.
- **Staff Augmentation and Interim Roles:** Your organization can enlist the help of Unit 42 technical experts as needed. Our team can assist on projects related to overall security architecture design, systems and application hardening and implementation, and tuning of new technical controls.
- **Cyber Program, Policy, and Standard Development and Maturation:** Our experts work with you to develop or improve policies to meet the demands of your organization while keeping in mind industry-specific standards, current business objectives, and future goals.
- **Cybersecurity Training and Awareness:** Unit 42 works with your leadership to create a cyber-aware culture and train your employees to better recognize cyberthreats. Unit 42 provides remote or on-site training modules for groups ranging from 5 to more than 5,000.

Incident Response and Awareness

Unit 42 has significant experience in responding to cybersecurity data breaches. We apply the knowledge gained from these incidents to our incident response assessments, leveraging our expertise to help your organization be better prepared in the event of an incident.

Unit 42 IR Readiness Services

- **Breach Readiness Review:** Unit 42 experts perform targeted cybersecurity risk assessments focused on detective controls and the people, processes, and technologies necessary to effectively respond to cyberthreats.
- **Incident Response Plan Development:** We work with your team to develop or enhance your organization's Incident Response Plan and supporting documentation, ensuring it aligns with industry standards and best practices.
- **Incident Response Tabletop Exercises:** Unit 42 builds customized scenarios based on industry-specific threats, allowing your team to simulate its response to a severe data security incident with key stakeholders.

Third-Party Cyber Risk Management

Our team works with your organization to assure smooth assimilation of third parties into your network, whether as vendors, partners, or due to corporate development activities.

Unit 42 Third-Party Risk Management Services

- **Cybersecurity Due Diligence Reviews:** We perform a targeted assessment of pending merger and acquisition activity. Focused and tactical, this assessment provides transparency to deal participants, identifies potential red flags, and highlights hidden cybersecurity risks. Our experts provide an independent appraisal of the overall information security program maturity.
- **Vendor Cybersecurity Risk Assessment:** Our team evaluates vendor-based cybersecurity risk so that your organization may improve information security-related contract requirements.

About Unit 42

Unit 42 brings together an elite group of cyber researchers and incident responders to protect our digital way of life. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art incident response and cyber risk management services. Our consultants will serve as trusted partners to rapidly respond to and contain threats so you can focus on your business. Visit paloaltonetworks.com/unit42.

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com