CONCAVE FORT

The Protective FORT Your Cyberspace Needs!

VAPT

Concave FORT's Vulnerability Assessment & Penetration Testing in partnership with Immuniweb aims to detect security vulnerabilities and verify the security, integrity, and availability by conducting internal / external types of VAPT for :

Mobile Application | Web Application | Network | Systems

Immuniweb's Award-winning AI technology for intelligent automation and acceleration:

1. Saving as much as 90% of the human time compared to traditional human services.
2. Risk-based and threat-aware testing.
3. Full DevSecOps & CI/CD Integration.
4. It covers the major Compliances around the globe including:

UKGDPR & EUGDPR, HIPAA, NIST, FISMA, CERTIFICATION, SANS, PCI DSS COMPLIANT, ISO 27001

Zero False Positives SLA

Money-Back Guarantee for a single false-positive

In-Depth Testing

Business logic testing, SANS Top 25, PCI DSS & OWASP coverage

Actionable Reporting

Tailored remediation guidelines and 24/7 access to analysts

Rapid Delivery SLA

Guaranteed execution schedule and report delivery

DevSecOps Native

SDLC and CI/CD tools integration, WAF for mobile backend flaws

SOPHOS | Barracuda | COMMVAULT | ImmuniWeb AI for Application Security

Software Quality testing

Independent Auditing

Independent auditing of software engineering practices, quality assurance and testing practices for conformance to relevant international standards such as ISO/IEC 9126, ISO/IEC 25000:2005 and applicable security standards for Fintech domain, such as ISO 27001.

Extended Testing Team Model

Extended testing team model offers the client teams to work in close coordination with our testing teams. The model is ideally suited for companies that are rapidly expanding and allows experts of our company to augment the existing technical resources of client organizations.

Consultancy

Consultancy on integrating state of art software engineering and automated testing strategies in organizations, improvements to software development and quality assurance processes, information, and data security for critical application.

Capacity Building

Capacity building on Automated Testing, Quality control, Standards for Software Systems, Software Testing Certifications, penetration testing and information security practices and standards.

Assessment and Analysis of the Existing Software

Assessment and analysis of the existing software of the existing software engineering, quality assurance and testing practices of the organizations, assessment of information security threats to the organizations and evaluation of their existing information security processes and infrastructure and applications.

Independent Software Testing

Independent Software Testing or in Testing as a Service (TaaS) model, our teams provide independent, third-party validation and verification services to the client organizations. The services range from manual and automated testing at system, integration, or unit levels to automated load and stress testing for web applications, mobile applications, desktop applications, and embedded systems.

Security Testing:

Security Testing: of critical applications for security threats, functional correctness, and scalability. The services include, automated penetration testing to assess network and application vulnerabilities, testing against known security vulnerabilities, e.g., OWASP vulnerabilities for web applications, and static analysis to identify source code vulnerabilities.

Secure Architecture

Concave FORT Secure Architecture Reviews are a collection of services based on industry best practices designed to evaluate the effectiveness of technical and operational security controls deployed in an organization. The reviews focus on People, Processes & Technology to improve the resilience of the organization's security posture in consideration of Business Requirements, Best Practices referred to CIS Benchmarks, NIST CSF.

Network Security Architecture Review

We begin by understanding the organizations business goals and control objectives and then review the network design, key components, protocols and data flow to and from the network, core technologies that the network is reliant upon to meet its security objectives and assess them against relevant standards.

Infrastructure Security Architecture Review

Review of Infrastructure Security capabilities, Server and Application hardening, Common Service Security (wireless, VOIP, Email), Boundary protection (VPNs, BYOD, Airgaps), Secure device management and Integrated cryptographic systems.

Network Device Audit and Configuration Review

Review of Device management environment, Minimum Security Baseline Configuration, Access control, Change Management, Patch Management, configuration hardening, Segmentation controls, Mapping of device rule base with organization security policy and audit and configuration review of the device against standards.

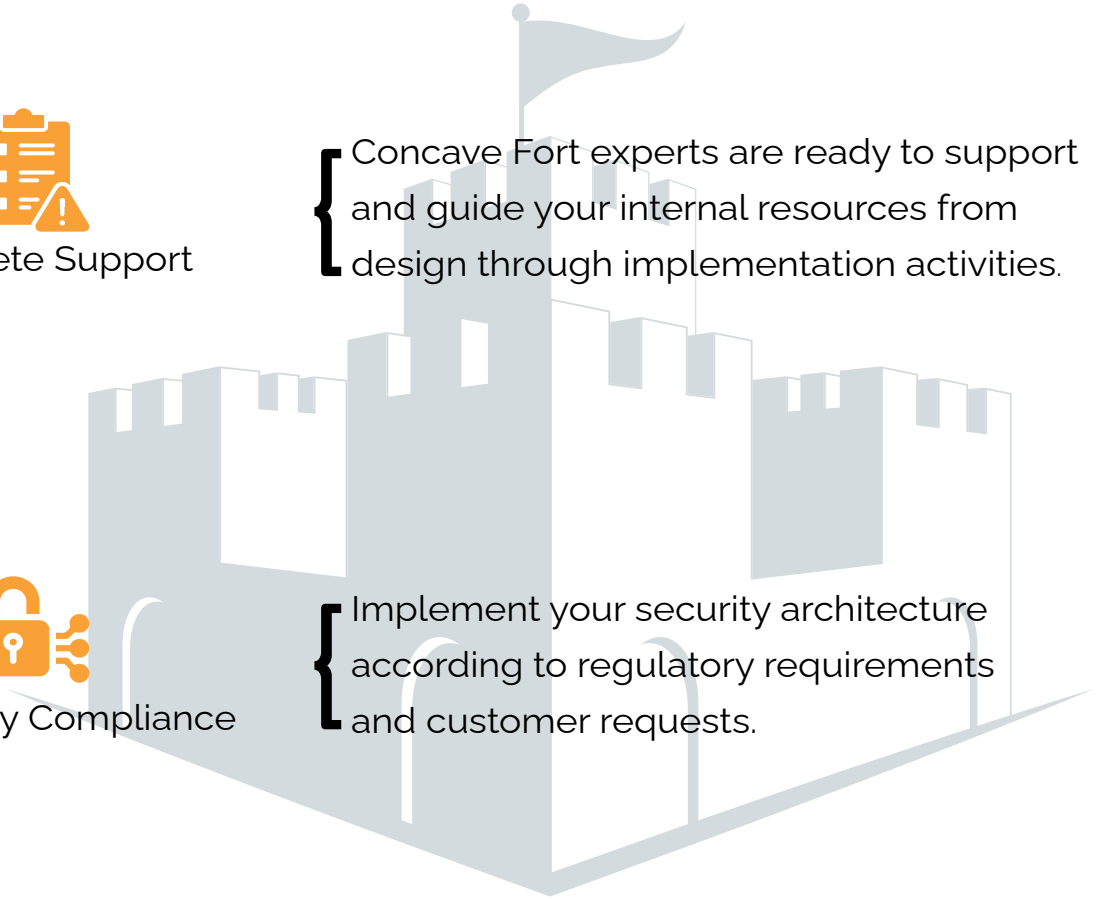
Why Concave Fort for Secure Architecture?

Tailored Architecture

Concave Fort utilizes a combination of people, processes & technology to optimize and customize your security architecture.

Complete Support

Concave Fort experts are ready to support and guide your internal resources from design through implementation activities.



Regulatory Compliance

Implement your security architecture according to regulatory requirements and customer requests.

Focus on Progress

Build a security architecture that's ready to make progress with you as your organization continues to grow and change.

SOPHOS Barracuda COMMVAULT ImmuniWeb® AI for Application Security

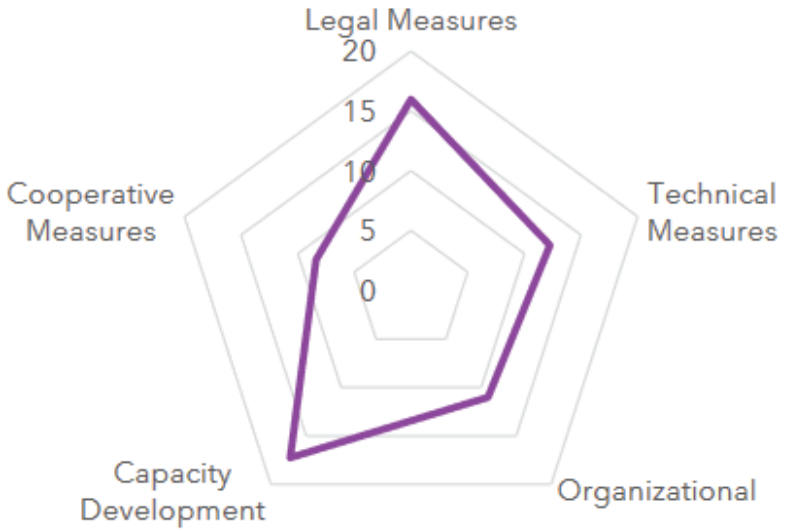
GRC

Concave FORT's in Partnership with Immuniweb and Commvault to offer corporate governance & risk management and compliance to your organization.

1. Differentiate yourself from your customers by getting in a certified security system to be put in place.
2. Consultancy in specialized areas such as information technology can assist to manage your organizational risks.
3. Environment's security and compliance with international standards address the People, Processes and Technology which improves organizational strategy.
4. Reducing costs on additional compliance efforts. Common processes, procedures and controls implemented as part of ISO 27001 conformance can be leveraged for other compliance efforts such as PCI, HIPAA and more.
5. The PCI compliance elevates the overall security posture of an organization in terms of infrastructure and environment.

Companies We have Worked With

Cybersecurity Index of Pakistan



Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development Measures

Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: ITU Global Cybersecurity Index v4, 2020