SECURITY ASSESSMENT

iV4's Security Assessment empowers you to take a proactive, head-on approach to eliminating risk. Gain unprecedented insight into your current security stance, as well as strategies for strengthening any weak areas. The ultimate benefit of an iV4 Security Assessment is that security becomes measurable, and therefore manageable, for your organization.

Led by iV4's Security Red Team, we identify risks and compliance issues specific to your industry and the technology you use, addressing problem areas before they disrupt your business. Additionally, iV4 prepares our regulated clients for audit and mitigate compromised scenarios.

The Security Assessment

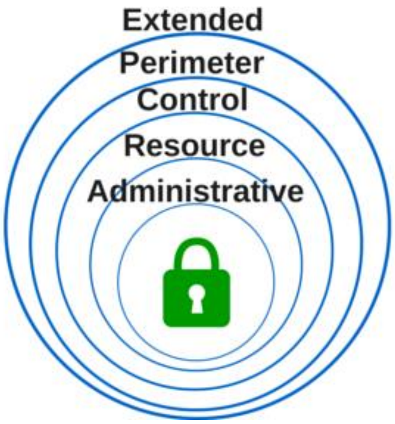
To assess your security posture and provide security metrics, iV4 analyzes the following layer of defenses that your organization currently deploys:

1. **Physical** – how access to facilities, systems and information is controlled
2. **Technical** – testing security configuration of network systems
3. **Administrative** – review current policies, procedures, and standards

Next, iV4 delivers a detailed report, assigning a security rating for each component reviewed based on Common Vulnerability Security Scores (CVSS) and business data dependency and sensitivity. Recommendations for full remediation of existing vulnerabilities, system hardening, and security architecture redesign are included.

Evaluation Areas

iV4 takes an outside-in approach analyzing each layer to provide a complete view of organizational risk.



The following five layers are analyzed:

1. **Extended Layer** – Public Information Controls (Google Hacking) Assessment
2. **Perimeter Layer** – Web vulnerability and penetration testing (Public facing systems), Infrastructure (Routers, Firewalls, Core Switches, Wireless), Physical Security Assessment
3. **Control Layer** – Review of authentication and authorization mechanisms, password audit, and hardening appraisal for Core Directory Services
4. **Resource Layer** – Assessment of key internal assets (servers, workstations, applications)
5. **Administrative Layer** – A review of client's required and addressable security policies and procedures and organization's current security program (Change Management, Incident Response, Standards, etc.)

SECURITY ASSESSMENT

Compliance Solutions

Every organization must follow regulations and policies – especially those enterprises operating in heavily regulated industries. iV4 is experienced with industry-specific regulatory compliance requirements from:

- FISMA
- FERPA
- DFARS
- NY DFS
- PCI/DSS
- FFEIC
- HIPAA

Benefits of a Security Assessment

Predict security threats: Proactively identify exposures throughout your environment and understand how they impact your organization

Validate critical vulnerabilities: Increase efficiency, pinpointing critical threats through penetration testing

Assess security controls: Test defense efficacy and make informed spending decisions based on risk to individual units within your organization

Analyze web application vulnerabilities: Reduce risk and minimize development spending by identifying exposures before go-live

Communicate risk clearly and effectively: Present risk analytics in the context of key assets, operational areas, compliance mandates, and business objectives

Scale security assessments: Expand scope, reach, and frequency without adding internal headcount

Retain a competitive edge: Understand what your investment in security "buys" you and how that compares with what your competitors spend

Plan for the future: Gain insight into meeting compliance requirements and long-term security management

iV4's Investment in Your Security

To ensure you're protected from the latest threats to your digital assets, iV4 continually researches, and then acquires, the latest security analysis systems. From advanced vulnerability assessment and security software to hacker-emulating penetration testing tools, iV4 is constantly investing in its security infrastructure.