# Application Security Assessment

# Statement of Capabilities


**Tampa, FL**
1936 Bruce B. Downs Blvd, Suite 430
Wesley Chapel, FL 33543

**Washington, D.C / Virginia**
5810 Kingstowne Center Dr, Suite 120-156
Alexandria, VA 22315
support@alakoa.com
☎ 888 746 1458
813 354 2732

# 1 CONTENTS

# 2 FOREWORD

Alakoa Corporation provides timely, reliable, high quality Information Technology consulting services and custom application development. Offering project management, project staffing, contract programming and technology consulting for information technology and software development organizations. Alakoa Corporation strives for excellence in fulfilling our promise of quality and value.

This document outlines skills and experience and is provided as an introduction. Alakoa Corporation is experienced in participating in teaming and strategic alliances, which enhance our ability to create advanced IT systems and solutions at reduced cost and risk.

The company has a consistent record of meeting contracted performance and financial targets. The majority of development contracts are undertaken on a time and material basis.

## 2.1 About Our Name

Alakoa Corporation takes its name from the Hawaiian language translated as **The Bold Path**.

# 3 COMPANY PROFILE

## 3.1 Overview

Alakoa Corporation has successfully partnered with technology companies where software is the back bone of the business, to assist them in benefiting financially and technically by taking on their development, testing and maintenance needs.

## 3.2 Mission Statement

In all the dimensions of work that we perform for our clients, our firm lives by the creed to approach each engagement with an utmost attention to quality and respect to people, products, and those constituents we serve on a day-to-day basis. Simply stated, we believe in these guiding principles:

### 3.2.1 Serve Our Clients as Advisory Counselors for Their Success

- Adhere to the highest professional standards
- Play an integral role in problem solving, implementation, and knowledge building
- Build enduring, trust-based relationships
- Strive for superior quality and distinctive impact

### 3.2.2 Deliver the Best of The Firm to Every Client

- Go into all client projects with the “Whatever it takes” attitude.

### 3.2.3 Create an Unrivaled Environment for Superior Talent

- Develop and excite our people through active apprenticeship and stretching, entrepreneurial opportunities
- Foster an inclusive and nonhierarchical working atmosphere
- Foster an environment in which people can voice their opposing opinions
- Respect the individual’s responsibility for balancing personal and professional life

## 3.3 Core Values

### 3.3.1 Integrity and Trust

We maintain high ethical standards in our interactions with clients and business partners, and make decisions that factor in our principles first and foremost.

### 3.3.2 Meeting the Needs of Our Clients

We treat each client's business as our own. We care how they perform over the long term. Their success is our success.

### 3.3.3 Teamwork and Sharing

By aligning our client's processes and systems, we help our clients access the right information.

## 3.4 Vision

To provide world-class consulting and software development services that delivers:

- Greater Visibility
- Greater Accountability and Control
- Greater Time/Resource Optimization.

## 3.5 Company Facts

- Founded in 2007, Privately Held Corporation
- 10+ employees/contractors

## 3.6 Services Offered

### 3.6.1 Management Consulting

- Project Management
- Software Architecture Design
- Technical Writing
- Quality Assurance Services
- Strategic Staffing

### 3.6.2 Information Technology Consulting

- Product Development
- Application Development
- Portal and Collaboration Solutions
- Business Process Automation
- Business Intelligence (BI)
- Enterprise Application Integration (EAI)
- Product Maintenance
- Feature Enhancement
- Demo Engineering
- Platform Migration
- Vulnerability Assessments
- Enterprise Hosting Solutions

### 3.6.3 Domain Expertise

- Healthcare
- Transportation & Logistics
- Education
- Financial Services
- Public Utilities

- Federal, State and Local Government

# 4 APPLICATION SECURITY ASSESSMENT

Alakoa Corporation offers a complete suite of security consulting services – Design Validation, Threat Modeling, Penetration Testing, Code Review, and Policy Compliance. The entire suite of services is generally termed a *Security Assessment*, though some of the individual offerings may be considered optional (Design Validation, Code Review, Policy Compliance) – Threat Modeling and Penetration Testing are typically considered key aspects of a Security Assessment.

## 4.1 Design Validation

When engaged at the beginning of a project, Alakoa Corporation consultants can review the project with your team and provide valuable feedback on the design and architecture that has been proposed.

Alakoa will ensure that:

- A Threat Model has been developed (see Threat Model section below).
- The design addresses the concerns of the Threat Model.
- Security Best Practices are followed.
- Software Architecture Best Practices are followed.

Alakoa will work with the project team to find and mitigate any defects in the design.

If you don't have written documentation, Alakoa will work with your team to understand the *notional* design and architecture, and assist in creating the documentation.

## 4.2 Threat Modeling & Risk Assessment

Threat Modeling is a fundamental, though often overlooked, engineering exercise that can have an incredible effect on improving the security posture of an IT system. Threat Modeling enables your team to see the system through the eyes of an attacker, and then design security countermeasures that protect the system from attack.

Alakoa will guide your team through the Threat Modeling exercise:

- Identify Key Security Objectives
- Define Usage Scenarios
- Identify Security Mechanisms and Countermeasures
- Identify Trust Boundaries & Entry Points
- Identify Threat Agents & Attacks (Threat Profile)
- Identify Vulnerabilities

A Risk Assessment builds on the Threat Model and takes it one step further to:

- Establish the Risk of each Vulnerability – the likelihood and impact of exploitation
- Determination if the Risk can be Accepted or Mitigated

In addition to being a fundamental exercise to undertake during the design phase, the Threat Model also serves to guide Penetration Testing so that the Key Security Objectives are verified by empirical testing.

It is important that when identifying Key Security Objectives that it is known in advance what policies or laws the system must comply with (see Policy Compliance section below).

## 4.3 Penetration Testing

Penetration Testing is the exercise of simulating an attack on the system by a malicious user. It is the empirical verification of the implementation of your Design and Threat Model. There are three types of penetration testing, which differ in how internal information about the system is used to inform the attack of the system.

| Description | Strength | Weakness |
|---|---|---|
| **White Box Testing**<br>All information about the internal structure and configuration of the system is known. This includes system documentation and source code.<br><br>Testing is tailored to the internal design of the system. Input test cases are developed to comprehensively exercise all relevant code paths. Outputs are observed and compared to expected results. | • Very effective in discovering implementation defects.<br>• Possible to guarantee all relevant code paths are evaluated. | • Can result in an overwhelming amount of tests if discretion is not used to determine what is relevant to the goals of the test.<br>• Requires advanced skills to be able to understand the internal complexities of the system. |
| **Black Box Testing**<br>Only publicly available information about the system is known.<br><br>Testing focuses on manipulating inputs and observing outputs. Testing may also include various attempts to probe the system to discover unknown or obfuscated components, and infer internal implementation details via information leakage. | • Effective in discovering undocumented features (and defects in those features).<br>• For very complex systems, this approach can be used to simplify testing. | • Cannot guarantee that all code paths are evaluated. |
| **Gray Box Testing**<br>Gray box testing is a hybrid of White and Black box testing. Internal information is known (primarily from system documentation). Source code is not necessarily utilized for test plan development.<br><br>Testing is primarily black box oriented (manipulating inputs and observing outputs) but is guided by the internal information that is known.<br><br>Once a vulnerability has been identified, source code may be used to further investigate successful exploitation. | • Very effective in discovering implementation defects.<br>• Generally takes less time than either white or black box testing.<br>• Simplified, yet comprehensive coverage of vulnerabilities. | • Does not guarantee that all code paths are evaluated (just those identified as being key).<br>• Requires advanced skills to be able to understand the internal complexities of the system. |

Testing is guided by the Threat Model & Risk Assessment, but typically focuses on the following classes of vulnerability (this list is not exhaustive):

- **Availability**: Denial of Service
- **Authentication**: Bypassing authentication, non-repudiation, spoofing, password recovery abuse, weak credentials, brute force attacks
- **Authorization**: Bypassing access controls, privilege escalation
- **Session Management**: Session hijacking, session fixation
- **Input Validation**: Injection Flaws (SQL Injection, etc), Cross-site scripting (XSS) attacks, non-validated input, buffer overflows, manipulation of client-side code (validation performed in client)
- **Exception Handling**: Information leak, non-secure defaults
- **Logging**: Not enough logging, log injection, log forging
- **Cryptography**: Insecure algorithm, insecure key management
- **Configuration**: Insecure configuration

The result of a Penetration Test is a report that identifies what was tested, what potential vulnerabilities were found, and if any vulnerabilities were successfully exploited. The report will also include steps to mitigate the vulnerabilities.

## 4.4 Code Review

Alakoa can perform a review of the source code for the system – identifying places where security best practices are both followed and not followed. Reviews are typically limited to areas of the code that are directly concerned with security, but a complete code review can also be performed, where more general software engineering best practices will also be evaluated.

Platforms, Languages and Frameworks Supported:

- Microsoft .NET Platform: C# & VB.NET – Windows Forms, ASP.NET, ASP.NET MVC, ASP.NET Web Services (ASMX), WCF Services
- Classic ASP: VBScript and JScript
- Cold Fusion: Fusebox
- PHP4/5: Zend, Cake, CodeIgnitor
- SQL Server 2000/2005/2008
- Oracle 8i, 9i, 10g, 11g
- MySQL
- PostgreSQL

## 4.5 Policy Compliance

Many systems are required to comply with some kind of standard or policy – whether it is industry established policies such as PCI/DSS, requirements to comply with laws such as HIPAA, Sarbanes-Oxley, and GLBA/FSMA, government required processes like DIACAP and FISMA, or IT policies established internally by your organization.

While the specifics differ with each set of policies, procedures, and laws – they generally include a similar set of high-level requirements:

- Documentation of system design, configuration, and inventory of hardware/software.
- Documentation of policies, procedures and processes that are in place to address a variety of security concerns such as: Authentication, Access Control, Auditing, Data Integrity, Transmission Security, and Privacy Breach Notification.
- Documented Security Assessment / Risk Assessment

Alakoa can work with your team to develop security policies, procedures and processes as well as prepare supporting documentation required for compliance.

Customers that are HIPAA covered entities should note that the documentation created as a part of Design Validation, Threat Modeling, Penetration Testing and Code Review represents roughly 80-90% of the requirements for the Technical Safeguards section of the HIPAA Security Rule.

# 5 VALUE PROPOSITION

**Partnership with Clients**
Alakoa establishes strong and lasting relationships with our clients. A majority of our business comes through established relationships and recurring engagements. Our goal is to help our clients build and maintain an outstanding security program that will protect their environment now and for the future. We offer full life-cycle support for your applications – we can quickly re-assess a system when it is changed – building upon previous assessments rather than starting from scratch each time.

**Experience**
Alakoa has a proven methodology that has been tested and refined over years of performance. Alakoa consultants are unique in that they are both experienced security experts and accomplished senior level developers. This gives them the unique capability to evaluate from both security and software development points of view.

**Product Neutral**
Alakoa is not a product vendor or a VAR. We do not use commercial scanning products in our assessments. Therefore you can be assured that our recommendations will be based solely on what is best for your environment and do not contain any hidden product or managed service sales agenda.

**Validated Results**
Your design and threat model are validated, and your implementation is verified. Defects are enumerated, and mitigation strategies are provided. Every vulnerability is manually verified to eliminate false positives. This is in stark contrast to most companies, which leave you with a report that contains a huge list of potential vulnerabilities - from which you must chase down the false positives and figure out how to fix the remaining vulnerabilities on your own.

**Deep Analysis**
Our reports provide a customized roadmap for securing your particular environment, not just a list of vulnerabilities. Every report provides an informative and thorough analysis of the security posture of your application and provides recommendations for fixing all issues. Every report also contains an executive summary targeted to management as well as specific prioritized technical remediation steps for administrators.

**Confidence**
A professional security assessment will give you confidence in the security posture of your system, and satisfy both management and auditors that you have taken necessary steps to safeguard your systems and data.

# 5.1 Automated Vulnerability Scanners

It is a commonly held belief that automated vulnerability scanners, such as IBM Rational AppScan, McAfee Secure, and Comodo HackerProof have made the traditional professional Application Security Assessment obsolete.

This belief can lead to misleading and potentially dangerous evaluation of the security of a system. These tools are not designed to be stand alone “audit in a box” solutions, and though they can be very useful for initial discovery, compliance checking, and finding the low hanging fruit – they are not replacements for a professional assessment.

Automated scanners and professional assessments are not competitors, but compliment each other - they are both components of a well rounded and multi-faceted security strategy.

## 5.1.1 Why Automated Vulnerability Scanners Alone are Insufficient

### 5.1.1.1 Overwhelming Output

Automated tools test for every apparent vulnerability, regardless of its applicability or prioritization. This leaves the end user in a position where they must wade through an overwhelming list of possible vulnerabilities, false positives, and false negatives.

### 5.1.1.2 Limited Test Cases

Scanning tools must be continually updated to be effective. They resemble virus scanners, in that both must constantly strive to incorporate the newest threat into their recognition software. Unfortunately, unlike viruses, the newest attack is often the most widely used, and therefore one of the biggest threats to consider.

Professional security experts stay up to date and are able to adapt much faster than engineers are able to develop attack plug-ins/signatures.

Professional security experts are able to employ very complex attacks, which cross application boundaries or otherwise require finesse and human adaptability. Automated scanners can never match this human adaptability.

### 5.1.1.3 Inability to Verify Exploitation

Many automated scanners will simply do a surface check, and utilize a signature database to determine if a vulnerability exists. Professional security analysts will actually attempt exploitation of the presumed vulnerability, and either verify it, indicate it is likely to be exploited with more time, or determine that even though a vulnerability is apparent that exploitation is not possible.

### 5.1.1.4 Inability to Create Vulnerabilities

Professional security analysts find new vulnerabilities and exploit techniques regularly during audits. An automated scanner will never be able to do this.

### 5.1.1.5 Impossible to Detect Certain Classes of Vulnerability

Automated scanners are simply unable to detect certain kinds of vulnerabilities, let alone attempt to exploit them. This can include detecting weak cryptography, information leakage, and dynamic content (JS, Ajax, Flash).

## 5.1.2 Automated Vulnerability Scanners Strengths

Automated vulnerability scanners do have strengths when compared to professional audits. They are and extremely economical and efficient way to comply with security policies that require regular security testing (i.e. PCI DSS quarterly scanning). They are also useful in detecting configuration changes and vulnerabilities at the operating system, web server, proxy and web application server layers (i.e. detecting missing patches, etc).

## 5.1.3 Trust Marks

### 5.1.3.1 What is A Trust Mark

A Trust Mark is a seal/badge that you can display on your web site that provides assurance to the end user that your site has verified or enhanced security/privacy measures in place. This can include badges that show when your site was last scanned by an AVS, that your SSL certificate is valid and provided by a well known vendor who also vouches for the veracity of your business, or that you have a verified privacy policy.

The benefit of a Trust Mark is entirely psychological. In April of 2005 an independent research firm conducted a test about trust marks:

- 78 percent of online shoppers say that a seal indicates that their information is secure.
- Only one in five shoppers did not know what purpose trust marks served.
- The overwhelming majority of consumers feel it is important for sites to include a trust mark.
- 88 percent of U.S. online shoppers say it is important for an e-commerce site to include a trust mark of some kind on its site.
- 79 percent of online shoppers expect to see a trust mark displayed on a Web site's home page. The majority of shoppers also expect to see trust marks displayed on the page where personal information is entered and where the final transaction is completed.
- 71 percent of online consumers shop only at sites they know and trust, while 38 percent of online shoppers will only make purchases through sites that include a trust mark.
- Shoppers not only recognize and value third-party trust marks, but the presence of a trust mark can also persuade them to complete the purchase.
- Nearly 70 percent of online shoppers have terminated an online order because they did not "trust" the transaction. In those cases, 53 percent indicated that the presence of a seal would have likely prevented the termination.

Clearly the presence of a trust mark can have a positive effect on the end user’s perception of the security of your web site.

### 5.1.3.2 AVS Trust Mark versus SSL Trust Mark

What is not clear is if the end user is discerning enough to perceive a difference between a badge certifying that the site is secure due to automated vulnerability scanning, versus one certifying the site is secure because it uses a well known brand of SSL certificate.

### 5.1.3.3 Getting the Most Out of A Trust Mark

Regardless of the type of Trust Mark you choose to utilize (AVS, Privacy, Enhanced SSL) you will get the most out of your TM by placing it in a prominent place on your website, especially on key parts of the site where a user would be most conscious of security and privacy. Do not just place the Trust Mark at the bottom of your page, or in some “About Our Site Security” page.

# 6 PRICING ESTIMATES

| Task | Small | Medium | Large |
|---|---|---|---|
| Design Validation | 8-12 hours | 14-20 hours | Contact for Details |
| Threat Modeling & Risk Assessment | 8-12 hours | 14-20 hours | |
| Penetration Testing | 20-28 hours | 28-36 hours | |
| Code Review | 8-12 hours | 14-20 hours | |
| Policy Compliance | Contact for details | Contact for Details | |

The most basic vulnerability assessment will consist of just Threat Modeling and Penetration Testing. More thorough assessments will also include Design Validation and Code Review. Policy Compliance is only needed if you must comply with a specific policy (i.e. HIPAA, GLBA, SOX, etc) and is dependent on the requirements of the policy to determine an estimate.

Our hourly rate is $125/hr.