**Vulnerability Assessment and Penetration Testing**

**A Minor Project Report Submitted to**



**Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal**

**Towards Partial Fulfillment for the Award of**

**Bachelor of Technology**

**(Computer Science and Engineering)**

**Submitted By:**

**Siddharth Jain(0827CS171211)**

**Shubham Malviya(0827CS171208)**

**Siddharth Choudhary (0827CS171210)**

**CS4 III YEAR**

**Supervised By: Guided by:**

**Mr. Ritesh Khedekar Mrs. Vandana Kate**

**Ms. Nupur Agrawal**

****

**Department of Computer Science and Engineering**

**Acropolis Institute of Technology and Research, Indore**

**July - Dec 2019**

**BUSINESS CASE**

Executive Summary

Information security is no longer an IT issue and is fast becoming a critical business issue. Recent high-profile hacking cases have shown that security vulnerabilities are not restricted to organisations of a particular size or a specific industry. Many IT systems are deployed with known and unknown security holes and bugs, and insecure default settings (such as blank passwords). New vulnerabilities may also occur as a result of mis-configurations and settings. Vulnerability assessment is the process of identifying such vulnerabilities in information systems. Penetration test, on the other hand, is the process of evaluating information security by simulating a malicious attack using vulnerabilities in information systems.

Businesses today have to address a vast array of regulatory compliance needs around data privacy & security, intellectual property management. With high cost of non –compliance (penalties, license cancellations, downtime, etc.), enterprises are under pressure to ensure timely and robust third-party audits. Looking beyond regulatory compliances, enterprises in any case need to address the increasing possibility of vulnerabilities within mission critical applications and data, due to a constantly changing IT environment.

This is where Netmagic’s Security Audit & Testing services make a big difference. Other than being a certified CERT – IN Empaneled Information Security Auditor, Netmagic brings to you a world-class service quality team dedicated to security, best-of-breed technology skills and leading partner tie-ups. What makes us stand out among normal Security Audit & Testing companies is our ability to not just recommend, but also execute the recommended changes to our customer’s IT environment.

Our Security Audit & Testing services are driven by decades of cumulative experience and a specialized team that combines cutting-edge technology tools and the vast power of human intelligence.

Numerous factors contribute to the true cost of a security breach such as:

* Damage to your reputation
* Regulatory fines for disclosed customer data
* Cost to repair the damage
* Lost Data
* Decrease in stock prices
* Employee wages while services are down
* Revenue lost while services are down

Depending on the size and industry of your company, you can see how any of these factors can exponentially increase the cost of a breach making it difficult to determine.

identifying vulnerabilities and risks in your network and IT infrastructure. Some of the benefits of our VAPT suite is as follows:

* Validates the effectiveness of current security safeguards
* Quantifies the risk to internal systems and confidential information
* Raises executive awareness of organisation’s exposure to information security threats
* Provides detailed remediation steps to prevent network and IT infrastructure compromise
* Protects the integrity of information assets exposed on Internet
* Helps to achieve and maintain compliance with various regulatory requirements.
* Our VAPT suite includes use of both open source as well as commercial tools to analyse both network traffic and information systems to identify any exposures that increase vulnerability to attacks. We simulate an attack and test the network and systems’ resistance as part of Penetration Testing.
* **Vulnerability Assessment** deals with potential risks, whereas **Penetration Testing** is actual proof of concept.
* **Application Testing** evaluates controls in web applications to prevent compromise of security of the application or the underlying system through flaws in the design, development, deployment, or configuration.
* **Host Review** is a white box (or full disclosure) test to evaluate the system security configuration settings.
* Together, these services test various layers of security controls and provide a holistic perspective.

## Issue

As the world becomes increasingly interconnected, [your business is only as secure as its weakest link](https://go.recordedfuture.com/risk-report) — and it’s estimated that more than half of all organizations have suffered data breaches through vulnerable third parties. Make informed decisions and reduce your overall risk with real-time security intelligence about the companies in your ecosystem.

Continuously Monitor Third-Parties

Organizations lack visibility into new third-party risks that may be introduced after they conduct a vendor security assessment. Recorded Future Company Intelligence Cards™ deliver on-demand access to complete, real-time information about the ever-evolving risk landscapes for more than 150,000 companies. Security intelligence enables deeper analysis and faster action by reducing time spent reviewing vendor questionnaires, and driving risk-prioritized [alerts in real time](https://www.recordedfuture.com/solutions/threat-alerting/) throughout the lifecycle of the relationship.

Improve Due Diligence for Procurement

All too often, vendor questionnaires provide a biased view of a potential vendor’s current and historic cyber risk profile. Recorded Future provides procurement teams with access to more than 100,000 sources, all centralized in Company Intelligence Cards featuring Risk Scores that enable rapid and deep analysis. This helps organizations understand and mitigate the objective risks of doing business with a provider, while dramatically accelerating the onboarding process.

## 

## Anticipated Outcomes

## VAPT decreases the chance that an attack will occur. Data security—VAPT creates more secure applications, increasing data security and protecting your intellectual property.

### **1 To Identify Gaps Between Security Tools**

This may sound like a weird reason but if you perform pentest using different tools for the same web app, there are higher chances that you would get varied results, sometimes contradicting each other. So if you know the security posture of your web app, you can and you should use it to compare tools. In my experience, keeping tools constant and doubting your own application is not correct. Ideally you should perform manual penetration testing, gather results and then compare tools to see which of those are capable of capturing the same set of results. Remember - there is a great difference between manual and automated penetration testing, my personal choice is manual.

### **2. To Prioritize Risk**

It is found that usually vulnerabilities are found and collected, but the risk prioritization is not carried out. With all the security risks to contend with these days, it's crucial for IT decision makers to determine how to prioritize risks in order of importance. Usually if risks are not prioritized, I have seen many organizations spend lot of time on trivial problem fixing and tend to delay or ignore or forget fixing the most critical ones.

### **3. To discover loopholes & Misconfigurations**

This reason is obvious as it sounds. Web apps, mobile apps and IT networks are prone to human errors and that's exactly what a hacker exploits. Most of the hacking attempts are due to incorrect coding practices and mis-configurations, than the vulnerabilities emerging from the platforms. Ideally letting a third party services firm run a penetration test is the right thing to do, to avoid conflict of interest situations, and get a completely unbiased outcome. This outcome can result into a skill matrix, so that you can deploy right people at the right job. Remember there cannot be any compromise in terms of skill-set when it comes to cyber security.

### **4. To Improve Your Product SDLC Process**

QA teams find functional bugs, while pentesters find security bugs. Periodic penetration testing aligned with SDLC process is an ideal approach to ensure lock-tight security. This way, the product code and changes go through multiple iteration of security checks, thus reducing the vulnerabilities drastically.

### **5. To Ensure Best Out Of Your Cyber Security ROI**

Organizations tend to invest huge amount of money, but they do not know what is happening with that money. This is especially true for IT product companies who develop a great cloud based software, deploy people, deploy infrastructure, have processes, but simply don't possess a habit of continuous security improvement using VAPT. This eventually results into some type of attack and/or data leakage, and pretty much renders the entire investment useless.

## Recommendation

Various options and alternatives were analyzed to improve the business processes and reduce the overhead costs. The approach described herein allows us to meet our corporate objectives of continuously improving efficiency, reducing costs, and capitalizing on technology. The web-based platform is compatible with all other current IT systems and will improve the security of your application. Vapt decreases the chances of being attacked by hackers by improving the security and simulating the vulnerabilities of your application. This project will somehow help in reducing the costs and allow us to perform vapt at lower costs. This project will help in getting rid of data breaches and also helps in identifying vulnerabilities and risks in your network and IT infrastructure as it validates the effectiveness of current security safeguards, quantifies the risk to internal systems and confidential information, raises executive awareness of organisation’s exposure to information security threats, provides detailed remediation steps to prevent network and IT infrastructure compromise, protects the integrity of information assets exposed on Internet and also helps to achieve and maintain compliance with various regulatory requirements.

## Justification

This project should be implemented because it provides the organization a detailed view of potential threats faced by an application which helps to stimulate the threats. Vulnerability assessment and penetration testing helps the organization in identifying programming errors that leads to cyber attacks. Apart from that Vulnerability assessment and penetration testing helps in providing risk management to the organisation, safeguards the business from loss of reputation and money which is very important for effective business outcomes.

Vulnerability assessment and penetration testing plays a major role in security as it secures applications from internal and external attacks. Vulnerability assessment and penetration testing is very effective in protecting the organizations data from malicious attacks. To keep the financial data secure while transferring it between systems or over networks we need vulnerability assessment and penetration testing. It protects user data and helps to identify security vulnerabilities within an application. The most important reason to perform vulnerability assessment and penetration testing is to find out loopholes within the system, to assess the tolerance of business in cyber attacks and also to implement effective security strategy in the organization.

# PROBLEM DEFINITION

PROBLEM STATEMENT

Today, most of the software applications are written using web technologies that can be accessed anywhere and anytime using the Internet. Things have evolved over the years; especially security of browser-based applications as compared to conventional client based architecture is not the same. There is a huge gap between codes that run on a computer as compared to websites that run inside a browser. Therefore, [security testing](http://www.360logica.com/blog/2014/12/role-security-testing-play-release-products.html) holds immense importance for web based applications. This has resulted in a huge demand for testers. If we talk about testers having the expertise in this area, web application security has proven to be a daunting task.

How is Security related to your Testing?

Security Testing is a technique to ensure whether a system protects data and maintains functionality as expected. Security testing covers a larger test space as compared to functional testing. While testing security aspects, you can try automating most of the part that is possible and work smartly with the rest. Developers have a comparatively tougher job, as they are required to write algorithms to resolve an NP-complete problem (complete path traversal) efficiently.  The key is to precisely select the speed of traversal, as there is a lot to do.

1. High-priority vulnerability

You can make trade-offs in resources and coverage while performing functional testing. In addition, you can analyze and narrow the scope of testing by focusing on the critical aspects from a business perspective and considering those that are mostly used. However, it is always better to test the entire application with certain non-critical bugs identified, but not fixed.  The scenario is just vice-versa in the case of security testing. Here, even a non-critical issue can cause similar damage as one on the application’s login page.

2. Test hidden parts of the application

A functional tester is concerned with testing an application’s front-end and back-end interface. A performance tester is primarily concerned with the load levels that a back-end can handle. The test target is defined by the application in all other cases. However, in security testing you must defend against a variety of unspecified attacks:

* An SQL injection attack through textboxes, radio-buttons, drop-downs, and other UI controls.
* A hidden POST parameter
* A GET parameter
* A cookie value

3. Protect application from damage

Testers must consider the behavior of the application under test if the user were to perform normal or at worse random actions. However, if a user modifies the value of a cookie, they should not validate or verify the application’s behavior in the functional testing phase. In case of security testing, testers are expected to consider the entire ways that a user might willfully damage the application under test. This would increase the number of areas to be considered while performing security testing.

## 

## Organizational Impact

Vulnerability Assessment is all about analyzing the organization’s network with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately. With the same area in focus, we perform different mechanism tasks. Using different tools and techniques, we perform diverse testing’s and find out the risk, check how they impact in real scenario & fix all types of risks that could be a cause of the attack.The goal of penetration testing completely relies on the type of activities performed for a particular engagement with its primary goal focusing on finding vulnerabilities that some heinous identity could use to destroy and inform the client about all the risks with the recommended strategic approach. There are additionally various programming structures that are utilized to expose vulnerabilities. Internal and External infrastructure pen testing performed by security experts against exploitable loopholes and also review the components within an organization.

## Technology Migration

|  |  |  |
| --- | --- | --- |
| Category | Tool | Description |
| Host Based | STAT | Scan multiple systems in the network. |
|  | TARA | Tiger Analytical Research Assistant. |
|  | Cain & Abel | Recover password by sniffing network, cracking HTTP password. |
|  | Metasploit | Open source platform for developing, testing and exploit code. |
| Network-Based | Cisco Secure Scanner | Diagnose and Repair Security Problems. |
|  | Wireshark | Open Source Network Protocol Analyzer for Linux and Windows. |
|  | Nmap | Free Open Source utility for security auditing. |
|  | Nessus | Agentless auditing, Reporting and patch management integration. |
| Database-Based | SQL diet | Dictionary Attack tool door for SQL server. |
|  | Secure Auditor | Enable user to perform enumeration, scanning, auditing, and penetration testing and forensic on OS. |
|  | DB-scan | Detection of Trojan of a database, detecting hidden Trojan by baseline scanning. |

### 1) Nessus Pro:

Nessus pro is a de facto industry standard for vulnerability assessment. Nessus Professional automates point-in-time assessments to help quickly identify and fix vulnerabilities,including software flaws, missing patches, malware, and misconfigurations, across a variety of operating systems and applications.

### Importance**of Nessus:**

* No limit to the number of IPs or assessments.
* Easily customize reports with client name and logo. Email directly to the client after every assessment.
* Intelligent vulnerability assessment with Live Results.

### Features:

### Identify flaws before attackers exploit them.

* Quickly prioritize high-risk areas for action.
* best-in-class penetration testing tools.
* Make testing easier, quicker and more reliable.
* Perform comprehensive scans for numerous types of security flaws.
* Quickly identify non-compliant applications and functions.
* Fix vulnerabilities easily with custom remediation advice.

### 2) BurpSuite:

Burp Suite, software that continually pushes the boundaries of web security. It is an integrated platform for performing vulnerability & penetration testing of web applications. Its work seamlessly to support the entire testing process, from initial stage of mapping to the analysis of an application’s attack surface, through to finding and exploiting security vulnerabilities.

### **How BurpSuite can meet the web security requirements:**

* Help prevent security breaches of your organization’s applications
* Develop a more robust and secure applications
* Achieve compliance with industry requirements

### **Features:**

1. Full-featured web vulnerability scanner
2. Powerful manual testing tools
3. Professional reporting
4. Numerous community extensions
5. Frequent product updates
6. Easy to use by novices and experts
7. Mature scanning engine
8. Detailed remediation advice
9. Fast and excellent support
10. Affordable and flexible licensing mode

### 3) Metasploit:

Metasploit is the most impactful penetration testing solution. It increases penetration testers’ productivity, validates vulnerabilities, and manages phishing awareness. Metasploit helps you carry out penetration testing engagements that take a comprehensive approach, using exploits, leveraging passwords, attacking web applications, and sending phishing emails.

# PROJECT OVERVIEW

## Project Description

[Vulnerability Assessment](https://www.veracode.com/security/vulnerability-assessment-software) and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. [Vulnerability scanners](https://www.veracode.com/node/607) alert companies to the preexisting flaws in their code and where they are located. [Penetration tests](https://www.veracode.com/node/605) attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws. In this project we will perform [Vulnerability Assessment](https://www.veracode.com/security/vulnerability-assessment-software) and Penetration Testing to find threats in web sites and web applications in order to make them more secure from attackers.

## Goals and Objectives

The objective of VAPT Vulnerability Assessment and Penetration Testing (VAPT) is to identify all potential loopholes within your network security system and show the potential impact of those threats and loopholes by exploiting them.

Penetration testing is the process of discovering possible vulnerabilities within a system, application, website, etc. It aims to protect the system from unauthorised access and possible weaknesses within the network infrastructure and helps to improve the configuration of an application. When a company isn't sufficiently protected, it leaves a coding vulnerability which could lead to sensitive data being accidentally damaged or exposed to the public.

Vapt decreases the chances of being attacked by hackers by improving the security and simulating the vulnerabilities of your application. This project will somehow help in reducing the costs and allow us to perform vapt at lower costs. This project will help in getting rid of data breaches and also helps in

identifying vulnerabilities and risks in your network and IT infrastructure as it validates the effectiveness of current security safeguards, quantifies the risk to internal systems and confidential information, raises executive awareness of organisation’s exposure to information security threats, provides detailed remediation steps to prevent network and IT infrastructure compromise, protects the integrity of information assets exposed on Internet and also helps to achieve and maintain compliance with various regulatory requirements.

## Project Performance

This project will ensure the security of web applications and websites and provides developers a list of threats that can be used to train many developers. Vulnerability assessment and penetration testing provides us with threats so that we can stimulate them in order to have a more secure website or web application. In this project we tried to reduce the cost of performing Vulnerability assessment and penetration testing. Vulnerability assessment and penetration testing ensures security by revealing the threats so that organisations can improve their security by getting rid of these threats. Vulnerability assessment and penetration testing protects the web applications and websites by improving the security issues.

## Major Project Milestones

This section lists the major project milestones and their target completion dates. Since this is the business case, these milestones and target dates are general and in no way final. It is important to note that as the project planning moves forward, a base-lined schedule including all milestones will be completed.

Example: The following are the major project milestones identified at this time. As the project planning moves forward and the schedule is developed, the milestones and their target completion dates will be modified, adjusted, and finalized as necessary to establish the baseline schedule.

|  |  |
| --- | --- |
| Milestones / Deliverables | Target Date |
| Project Charter | 01/01/20xx |
| Project Plan Review and Completion | 03/01/20xx |
| Project Kickoff | 03/10/20xx |
| Phase I Complete | 04/15/20xx |
| Phase II Complete | 06/15/20xx |
| Phase III Complete | 08/15/20xx |
| Phase IV Complete | 10/15/20xx |
| Phase V Complete | 12/15/20xx |
| Closeout/Project Completion | 12/31/20xx |

# STRATEGIC ALIGNMENT

This project can benefit our universities and organisations by revealing the threats and helps them to improve their security as a result them can protect data and their applications from hackers. Vulnerability Assessment and Penetration Testing (VAPT) is to identify all potential loopholes within your network security system and show the potential impact of those threats and loopholes by exploiting them.

Penetration testing is the process of discovering possible vulnerabilities within a system, application, website, etc. It aims to protect the system from unauthorised access and possible weaknesses within the network infrastructure and helps to improve the configuration of an application. When a company isn't sufficiently protected, it leaves a coding vulnerability which could lead to sensitive data being accidentally damaged or exposed to the public.

identifying vulnerabilities and risks in your network and IT infrastructure as it validates the effectiveness of current security safeguards, quantifies the risk to internal systems and confidential information, raises executive awareness of organisation’s exposure to information security threats, provides detailed remediation steps to prevent network and IT infrastructure compromise, protects the integrity of information assets exposed on Internet and also helps to achieve and maintain compliance with various regulatory requirements.

# 

# GLOBAL ENGAGEMENT

Vulnerability assessment and penetration testing plays a major role in global engagement as it can help in imoroving the security of any organisation or institute. This project can benefit our universities and organisations by revealing the threats and helps them to improve their security as a result them can protect data and their applications from hackers.

# COST BENEFIT ANALYSIS

 It is often times difficult to justify the budget and [quantify the return on investment for a penetration test](https://www.triaxiomsecurity.com/2019/02/15/what-is-the-roi-of-a-penetration-test/). While we always recommend ensuring your firm is conducting a reasonable amount of testing with a sufficient scope to maintain a stable security posture, we recognize that sometimes the budget and required level of testing just don’t always align. Today, we’ll detail strategies to reduce the overall cost of a penetration test while still achieving some of the key benefits of testing.

In conducting a thorough test of every single asset, as the name implies, sampling is selecting a subset of your assets for testing. This limits the scope of the penetration test which, in turn, can reduce the cost of testing. There are a number of concerns with this approach, so it’s important to carefully consider what assets you pick. It’s a great idea to work with your penetration testing firm to vet the list of assets to be tested and provide feedback on potential concerns. Some of the key considerations when using a sampling approach are:

* Vulnerabilities may be missed because not all assets are being tested.
* Chained exploits utilizing vulnerabilities across multiple assets may be missed.
* Sampling will not satisfy most compliance requirements for penetration testing.
* You will be able to see weaknesses in certain classes of assets if you have a standardized configuration process (e.g. all your network devices are shipped with SNMPv1 enabled with the default community string).
* You will be better off doing some level of testing to start quantifying your risk than no testing at all.

**Vulnerability Scanning:** While 10 times out of 10 we will recommend a full blown [penetration test over a vulnerability scan](https://www.triaxiomsecurity.com/2018/03/09/what-is-the-difference-between-a-penetration-test-and-a-vulnerability-scan/), there are scenarios where a vulnerability scan makes sense. For example, if you already complete annual penetration testing, but you want a more robust security program and you need a third-party to help with vulnerability management. In this scenario, you’ll be able to identify and remediate known vulnerabilities identified by the scans to help improve the results of your annual penetration test, as well as your security as a whole. In this approach, you’re actively managing vulnerabilities and your risk landscape throughout the year, rather than during a one-time assessment. If you want to get started with a security program but aren’t sure where, maybe a quarterly vulnerability scan is a nice way to start fixing some issues prior to conducting an [annual penetration test.](https://www.triaxiomsecurity.com/2018/10/12/how-often-should-my-company-get-a-penetration-test/)

**Multi-Year Contracts**: At Triaxiom, we offer multi-year discounts for any security assessment. When you know you will be conducting annual testing, why not go ahead and lock into a multi-year contract and achieve some cost savings? By having a long term engagement in place, you can strategically plan releases/upgrades/architectural changes while still planning your security assessment well in advance. It also helps you to know that your project has already been budgeted for and you won’t see any year-over-year price increases.

**Multi-Assessment Discount (Bundling):** Although it seems counter intuitive to add additional scope when you are looking to reduce your budget, it may make for an easier conversation with your decision makers or executive management.  At Triaxiom, we offer a discount when 3 or more assessments/services are purchased together. For example, the conversation may start with: “We can get an external penetration test, internal penetration test, and a social engineering assessment for the same cost as just the external penetration test and internal penetration test, and we’ll get a better view of our risk by doing all three at the same time.”

**Be Honest and Just Ask:**Be honest when having initial conversations with a penetration testing firm. Let them know what your budget is and what your expectations are. Not only does this streamline the overall process but it can help not to waste your time, if the services you are looking for are way out of line with your proposed budget. It always helps the penetration testing firm understand where you are at budget wise and if they will be able to meet your testing requirements within that budget.

At the end of the day, our goal at Triaxiom is to help build a more secure world by helping each of our clients improve their security posture. We will try every way possible to achieve your requirements within your budget!

# IMPACT ANALYSIS

## Systems Impacted

Select the option that reflects the level of integration required with other university systems (i.e. Directory, Treasurer’s System, Workday, etc.).

* Low – 1 Internal System
* Med / Low – 1 External System
* Medium – 1 Internal System
* Med / High – 1 External System
* High – Significant % of Systems

**Selected**

**High**

## 

## Campuses Impacted

### 

* Low – 1 Campus
* Medium – Multiple Campuses
* High – Enterprise Wide

**Selected**

**High**

## 

## Compliance

* Low – Not Required
* Medium – Company Policy
* High – Regulatory

**Selected**

**High**

## Conformity to Standards

### (Select one)

* Low – Conforms to Current Standards
* Med – Conforms w/ Exceptions
* High – Requires New Standards

**Selected**

**Medium**

## Cost Savings

* Low – Less than <$100,000
* Med / Low – $101K - $250K
* Medium – $251K - $500K
* Med / High – $500K - $1M
* High – More than $1,000,000

**Selected**

Low – Less than <$100,000

## Cost of Project

* Low – Less than $50,000
* Med / Low – $51K - $100K
* Medium – $101K - $250K
* Med / High – $251K - $1M
* High – More than $1,000,000

**Selected**

Low – Less than $50,000

## Duration

* Low – 15 – 30 Days
* Med / Low – 31 – 60 Days
* Medium – 61 – 90 Days
* Med / High – 91 – 120 Days
* High – More than 120 Days

**Selected**

**High - More than 120 days.**

## 

## Resource Hours Needed for Project

* Low – Less than 160 Hours
* Med / Low – 161 – 500 Hours
* Medium – 500 – 1,000 Hours
* Med / High – 1,001 – 5,000 Hours
* High – More than 5,000 Hours

**Selected**

Med / Low – 161 – 500 Hours

## 

## Internal Experience on Similar Project(s)

* High – Multiple Prior Projects
* Med – Limited Experience
* Low – Never Done This Before

**Selected**

**Med - Limited Experiences**

## Alignment Score

* No Objectives
* 1 Objective
* 2-3 Objectives
* More than 3 Objectives

**Selected**

**1 Objective**

# 