**GLOBAL FEDERAL, INC. (GFI)**

Global Federal, Inc. (GFI) is a Federal Government Component that manages thousands of accounts across the United States. A Government Agency, that specializes in financial management, loan application approval, and investment of money management for their government customers.

GFI employs over 1,600 employees and has been experiencing consistent growth for nearly six years. A well- honed management strategy built on scaling operational performance through automation and technological innovation has propelled the company into the big leagues;

The executive management team of GFI:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | CEO  John Thompson | |  | | | |
|  | | | | | |  | | | | |
|  | | | Deputy CIO  Trey Elway |  | |  | | Executive  Assistant Kim Johnson |  | |
|  | |  | |
|  | | | | | |  | | | | |
|  | | Executive  Assistant Julie Anderson | |  | |  | | Executive  Assistant Michelle Wang |  | |
|  | |  | |
|  | | | | | |  | | | | |
| CCO  Andy Murphy |  | | COO  Mike Willy |  | CFO  Ron Johnson | |  | Director of  Marketing John King |  | Director of HR Ted Young | |
|  | |  |  |  |

# Figure 1 GFI Management Organizational Chart BACKGROUND AND YOUR GROUPs ROLE

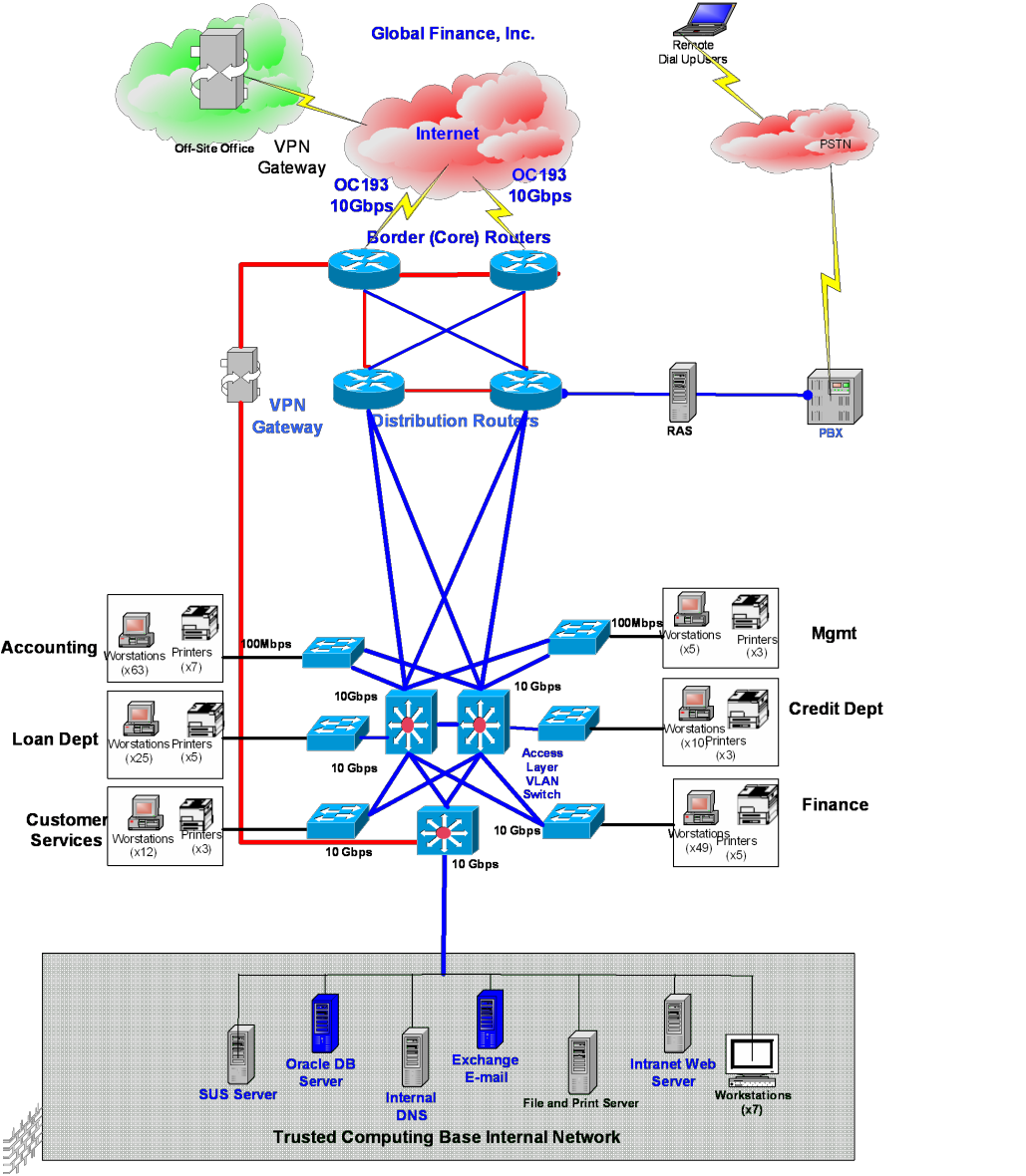
Your Security Company is educated, trained, and hired to protect the physical and operational security of GFI’s information system.

Your group was hired by COO Mike Willy and currently report to the COO. You are responsible for a $5.25m annual budget, a staff of 11, and a sprawling and expansive data center located on the 5th floor of the corporate tower.

GFI has experienced several cyber-attacks from outsiders over the past a few years. In 2012, the Oracle database server was attacked and its customer database lost its confidentiality, integrity, and availability for several days. Although the company restored the Oracle database server back online, its lost confidentiality damaged the agencies reputation. Another security attack was carried out by a malicious virus that infected the entire network for several days. While infected the Oracle and e-mail servers had to be shut down to quarantine these servers.

There’s no question that the agency’s CEO sees the strategic importance of technology in executing his business plan, and in this way, you share a common basis of principle with him: that IT is a competitive differentiator. Your team has been tasked to identify vulnerabilities in the network and provide a mitigation strategy for each identified vulnerability. Also, provide an overall risk determination before and after your recommended mitigations. This deliverable will help the agency determine the most critical vulnerabilities and their mitigations moving forward.

# CORPORATE OFFICE NETWORK TOPOLOGY



90

90

**Wireless Antenn**9**a**0

You are responsible for a corporate WAN spanning 10 remote facilities and interconnecting those facilities to the central data processing environment. Data is transmitted from a remote site through a VPN appliance situated in the border layer of the routing topology; the remote VPN connects to the internal Oracle database to update the customer data tables. Data transaction from the remote access to the corporate internal databases is not encrypted.

A bulk of the data processing for your company is handled by Oracle database on a high end super computer. The trusted computing based (TCB) internal network is situated in a physically separated subnet. This is where all corporate data processing is completed and internal support team has its own intranet web server, a SUS server, an internal DNS, an Exchange e-mail system, and other support personnel workstations. Each corporate department is segregated physically on a different subnet and shares the corporate data in the TCB network.

**ASSIGNMENTS**

* Create an Executive Summary for the deliverable.
* Create an inventory of the current assets and prioritize them in the order of mission criticality.
* Make a list of access points internal and external (remote).
* Evaluate current perimeter security protection and enterprise topology.
* Evaluate current remote access to enterprise.
* List identified vulnerabilities and correlate them to SP800-53 rev. 4 (AU, IA, SC and AC Control families) 4 per person in your group
* Assess probability of compromise and its impact on each system within the environment.
* Assess vulnerabilities on each asset and impacts if compromised.
* Recommended mitigation procedures commensurate with identified.
* Formulate a quantitative or qualitative risk assessment for current and then after mitigations have been identified.
* Conclusion

# Risk Assessment Paper Rubric

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Non-compliant** | **Minimal** | **Compliant** | **Advanced** |
| **List Vulnerabilities for IT System** | Did not list vulnerabilities(1) | Evaluated authentication protocols, methodologies but with insufficient data or inadequate description. (10) | Evaluated authentication protocols, methodologies with supporting data and description, but lacks mission objectives. (20) | Evaluated authentication protocols, methodologies with supporting data, description; and addressed mission objectives. (30) |
| **Assess risk based on probability of compromise and its impact on each asset.** | Did not assess risk based on probability of compromise and its impact discovered on each asset. (1) | Assessed risk based on probability and its impact discovered on each asset but incomplete. (6) | Assessed risk based on probability and its impact discovered on each asset but did not summarize them. (14) | Assessed risk based on probability and its impact discovered on each asset and summarized them. (20) |