**Residency Research Makeup Project**

**Acme Enterprise Scenario Residency Week**

Acme Enterprise is a private company that is gearing up for an initial public offering (IPO). Prior to going public Acme must be in compliance with: GDPR, PCI DSS, and SOX. Acme is in the water purification business with new technologies that purify water in any form whether it is sewage, ocean, lake etc.

Part of its IPO process is to show due diligence and due care. Acme has identified your team to conduct a risk assessment and analysis of its information technology infrastructure to uncover any threats and exposures and provide mitigations and controls to reduce those uncovered threat/exposures, so it can have a successful IPO.

Using the Network Infrastructure design of the Acme Enterprise you are to assess risk of Acme’s:

1. Perimeter Security
2. Network Security
3. Endpoint Security
4. Application Security
5. Data Security
6. Operations
7. Policy Management

**Acme Perimeter Security**

Acme is currently protected by two dual Dynamic Stateful Inspection Firewalls that are configured in active and stand by mode. Acme is also configured to use PAT (port address translation) where 200.200.200.1 represents Acme on the public Internet. Acme translates this public IP through its clustered firewall to the internal IP space of 10.100.0.0/16 giving Acme 65334 useable IP addresses.

As part of Acme’s infrastructure, it also accesses cloud services for its business office tools through Office 365 and uses Dropbox for end user’s storage. Acme uses a web hosting service for its web front end and ecommerce which is connected to a back-end Oracle Database using enterprise MySQL. The database administrators have full access to all database information, but they lack oversight from anyone else.

There are two DMZ’s, but they are not utilized.

**Network Security**

Acme has a collapsed core design which means all internal LAN routing and Internet access occurs on its distribution level devices. This means, wireless access, web proxy access, access control lists and entries are located at this layer of the infrastructure. Currently Acme is using WPA 2 (wireless protected access 2) for is wireless security. The web proxy is configured with the following: General, Limited, and Exclusive Internet access. Each of these categories dictates what type of Internet access an end user will experience if belongs to one of these groups.

The Local area network uses the IP block in the following way: 10.100.1.0/24 User VLAN, 10.100.2.0/24 Research and Development VLAN.

Current access control lists are permit 10.100.2.0 0.0.0.255, permit 10.100.1.0 0.0.0.255. All other devices use the rest of the unallocated IP block of 10.100.0.0/16.

Also, all IP space is statically assigned. There is one default route to Internet but users of complain about access to internal services.

**Endpoint Security**

There is a mixture of MAC and Windows systems, XP, 7, and 10. JAMF is used to control and monitor MAC systems, the Windows devices rely on its end users to patch and update systems. The current endpoint security is signature-based MacAfee with no centralized control.

**Application Security**

DevOps is responsible for secure coding and development of applications, but it has no formal oversight. Policy for application monitoring tracking is adhoc there are no formalized procedures. The server farm houses all applications, the operating systems range from Server 2003 to 2016. Mobile device management, media server, content management, file server, directory services, database, are all the services being offered from the server farm. This server architecture is all hardware based there are no hypervisor systems in place.

**Data Security**

Data has not been classified, identity access management relies on one factor authentication; encryption, digital signatures, PKI rely on self-signed certificates, protection in the cloud is also missing and there is a lack of DLP (data loss prevention). Acme does store financial information in its data center as well as personal identifiable information.

**Operations**

Information technology is responsible for security however there is a security team under the IT department. The Chief Information Security Officer reports to the Chief Information Officer.

**Policy Management**

Acme has one Information Security Policy that addresses its information security architecture and program. It is not based on any of the existing information security management frameworks such as: IS0 27002, NIST CSF, or COBIT 5.

**You are going to conduct a risk assessment on Acme Enterprise using the risk assessment concepts we have learned about thus far. Each of the areas of the infrastructure mentioned above is where you will concentrate your assessments. After you have completed your risk assessment, you will then provide recommendations for each area that you assessed to reduce risk, exposure, and threat. Also, as part of your final submission demonstrate through a redesign where your mitigations will take place within the architecture. You can use the image below as guide for your risk analysis of each area.**



