The idea is to provide an overview of the current state of enterprise key management for Superior Health Care.

1. Provide a high-level, top-layer network view (diagram) of the systems in Superior Health Care. To do this, start by reading these resources on data at rest, data in use, and data in motion. The diagram can be a bubble chart or Visio drawing of a simple network diagram with servers. Independent research may be used to find one to use.
2. Identify data at rest, data in use, and data in motion as it could apply to your company. Focus on where data is stored and how it’s accessed is a good place to start. Finally, review these resources on insecure handling, and identify areas where insecure handling may be a concern for your organization.

Use this information in your implementation plan.

In the next step, you will consider key management capabilities.

\*\*\*\*\*Now you must begin your research into CrypTool, to better understand enterprise key management.

1. Conduct independent research to identify the gaps in key management that are in existing corporations. Any factual information should be cited using APA format. If data is lacking, use fictitious information.
2. Identify the posed risks to the cryptographic systems as a result of these gaps, including but not limited to crypto attacks. Read these resources to brush up on your understanding of crypto attacks.
3. Propose solutions that the companies could have used to address these gaps. Be sure to identify what is needed to implement these solutions.
4. Identify challenges other companies have faced in implementing a key management system. Include any proposed remedies to these challenges.
5. Explain the uses of encryption and the benefits of securing communications by hash functions and other types of encryption. When discussing encryption, be sure to evaluate and assess whether or not to incorporate file encryption, full disc encryption, and partition encryption. Discuss the benefits to using DES, triple DES, or other encryption technologies. To complete these tasks, review the resources provided to you. You’ll need to understand the following topics:

A.uses of encryption

B.hash functions

C.types of encryption

D.DES

E.triple DES

1. Describe the use and purpose of hashes and digital signatures in providing message authentication and integrity. Check out these resources on authentication to further your understanding. Focus on resources pertaining to message authentication.

2. Review the resources related to cryptanalysis, then explain the use of cryptography and cryptanalysis in data confidentiality. Cryptanalysts are a very technical and specialized workforce. Your organization already has a workforce of SEs. Conduct research on the need, cost, and benefits to adding cryptanalysts to the corporation’s workforce. This is to support part of the operation and maintenance function of the enterprise key management system. You are determining if it's more effective to develop the SEs to perform these tasks. If the corporation does not develop this new skilled community, what are other means for obtaining results of cryptanalysis?

3. Research and explain the concepts, in practice, that are commonly used for data confidentiality: the private and public key protocol for authentication, public key infrastructure (PKI), the x.509 cryptography standard, and PKI security. Take time to read about the following cryptography and identity management concepts: public key infrastructure and the x.509 cryptography standard.

Provide the CISO with information on different cryptographic systems either in use by other companies or systems that the company should consider procuring. You will need to independently research what key system products are available. You may research a company you have worked for or know about regarding the use of an enterprise key management system. The idea is for you to get acquainted with different systems that could be used by Superior Health Care.

1. Describe the cryptographic system, its effectiveness and efficiencies. Provide analysis of the trade-offs of different cryptographic systems. Review and include information learned from conducting independent research on the following:

•security index rating

•level of complexity

•availability or utilization of system resources

1. Also include information on expenses as pertains to various cryptographic ciphers.

Use this information in your implementation plan.

1. Finalize enterprise key management plan.

Identify the key components, the possible solutions, the risks and benefits comparisons of each solution, and proposed mitigations to the risks. These, too, should be considered as a separate section or could be integrated within the implementation, operation and maintenance sections.

The length of this report should be a 8-10 page double spaced Word document with citations in APA format with in text citations. The page count does not include figures or tables. There is no penalty for using additional pages if you need them. Include a minimum of three (3) references. Include a reference list with the report.

A possible outline could be:

•introduction

•purpose

•key components

•implementation

•operation

•maintenance

•benefits and risks

•Then turn your attention to the enterprise key management policy, which is the final step

•summary/conclusion