Artemis Financial aims to deploy the best practices for encrypting long-term archive files. To determine these practices, they need to understand the available methods and their purposes, such as:

* AES (bit block cipher supporting keys of 128, 192, & 256): provides fast, strong encryption for securing sensitive data
* RSA: enable secure communication by encrypting data or keys with a public/private key pair.

AES with 256-bit strength is ideal for defending against security attacks. It uses strong encryption and avoids outdated algorithms susceptible to modern threats like brute-force attacks, cryptographic weaknesses, and data tampering. This essentially means using strong and modern encryption algorithms. Another best practice is to use encryption modes with built-in authentication to ensure data integrity. A defense against data tampering and unauthorized modifications. We can add ACL restrictions on access to encryption keys and sensitive files based on user roles. Complex passwords are harder for unauthorized users to guess. Log file access and encryption activities should be monitored and audited.   
With government regulations, you want to consider general data protection regulations. This applies to organizations that handle personal data of EU users. Requiring that data must be encrypted to protect personal data /information, encryption keys need to be managed properly. You will need to look at the normal HIPAA (Health Insurance Portability and Accountability Act) and ensure that this has encryption for both at rest and in transit to safeguard PHI (Personal Health Information). Other regulations that will be on the main check list will be:

* PCI DSS (Payment Card Industry Data Security Standard)- encrypt cardholder data using strong algorithms and protect encryption keys.
* GDPR (General Data Protection Regulation)- data must be encrypted to protect personal information and encryption key must be managed.

This risk assessment behind the recommendation is the key complexity with improper handling, storage, or rotation of encryption keys can lead to compromised data security, regardless of how strong the cipher is. To mitigate this, it is important to implement centralized key management to securely generate, store, and rotate keys. Again, implementing ACLs as well. Another risk will be errors occurring during implementation, such as failing to generate secure random numbers for IV’s (initialization vectors), which can weaken encryption. To mitigate this, usage of well- tested cryptographic libraries like Java built-in crypto package. Avoid constructing custom encryption code from scratch to minimize errors. Another risk will be failure to meet specific requirements, which may result in penalties or non-compliance flags. To mitigate as well, we would need to maintain sure backups in a key management system. Emphasizing multi-authentication factors to secure access to the key backups.   
A Hash function is defined as “a one-way function that takes input and produces output that is had to replicate and extremely difficult to reverse” (Kim & Solomon, 2023, p. 516). The purpose of hash function is to generate a unique, fixed- length representation of data. Ensuring data integrity by allowing verification that data hasn’t been tampered with.  
Bit levels indicate the size of the key used in encryption. Higher bit levels provide better security but require more computational power.   
The use of random numbers is to enhance encryption by adding unpredictable circumstances. Symmetric keys are faster and efficient for large scale encryption but a challenge when sharing the key between parties. With non-symmetric it eliminates the need to share a secret key securely but slower than symmetric encryption and is not practical for encrypting large amounts of data directly.  
The history and current state of encryption algorithms can start with early algorithms such as Caesar cipher. This is one of the earliest ciphers, using basic letter shifting techniques. Modern algorithms such as AES, which support 128-, 192-, and 256-bit key lengths and are highly secure against brute force attacks. Symmetrical AES remains a popular encryption standard for its security and efficiency. Asymmetric RSA and ECC are widely used for secure key exchanges and authentication. Advancements in computing raise potential risks to RSA and other factor-based algorithms regarding post-Quantum concerns.

[Strong Encryption Explained: 6 Encryption Best Practices](https://www.esecurityplanet.com/networks/strong-encryption/) (2024) Kime, Chad   
Kim, D., & Solomon, M. G. (2023). *Fundamentals of Information System Security* (4th ed., pp. 156, 172-173, 216, 510, 516). Jones & Bartlett Learning.