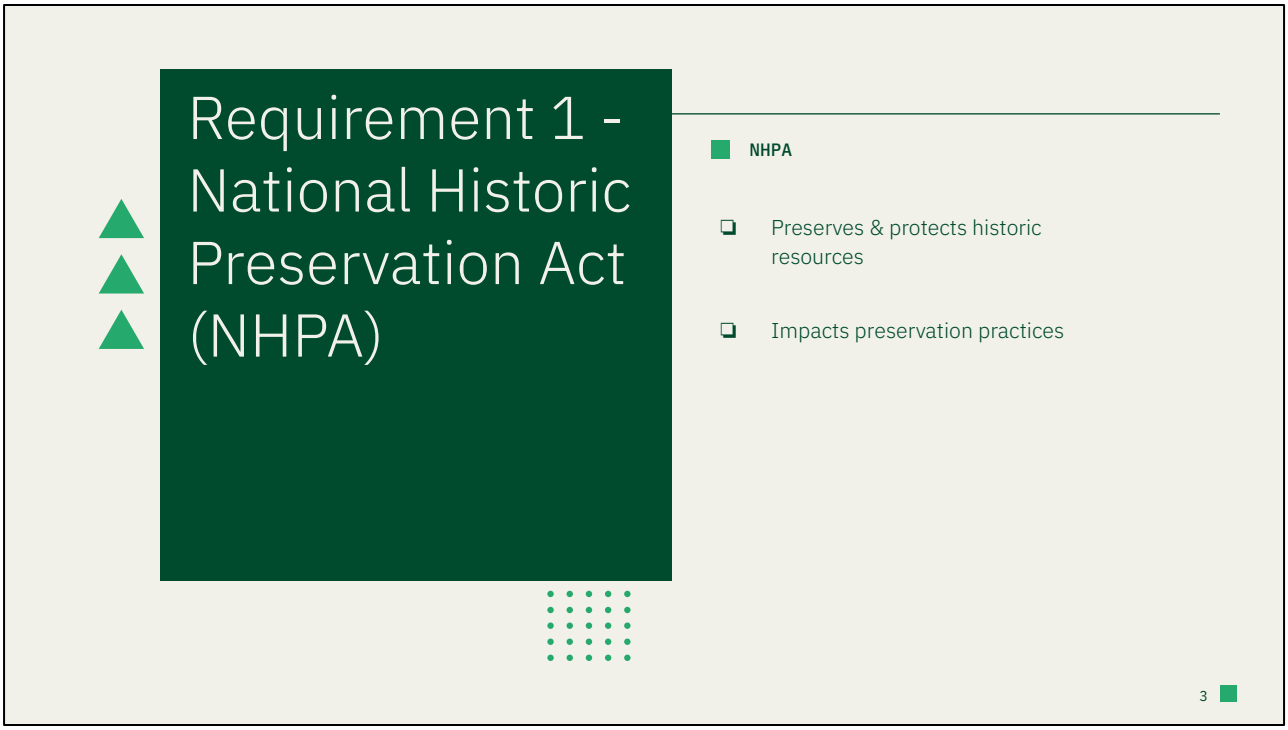
# Information Assurance (IA) Plan for the Tenement Museum

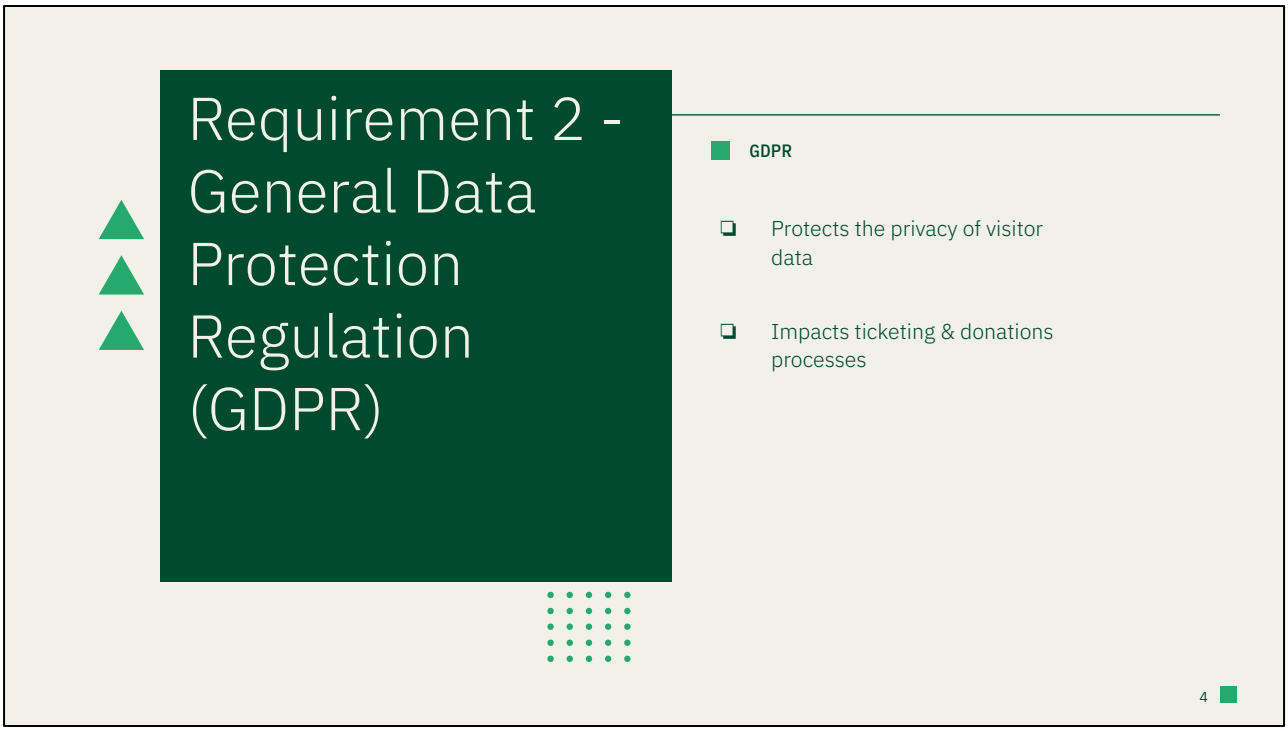


Good afternoon, today I will be presenting my proposal for an Information Assurance (IA) plan to help secure the Tenement Museum's information assets.
(Link to image used: https://www.tenement.org/wp-content/uploads/103-dusk-crop-1.21.14.jpg)

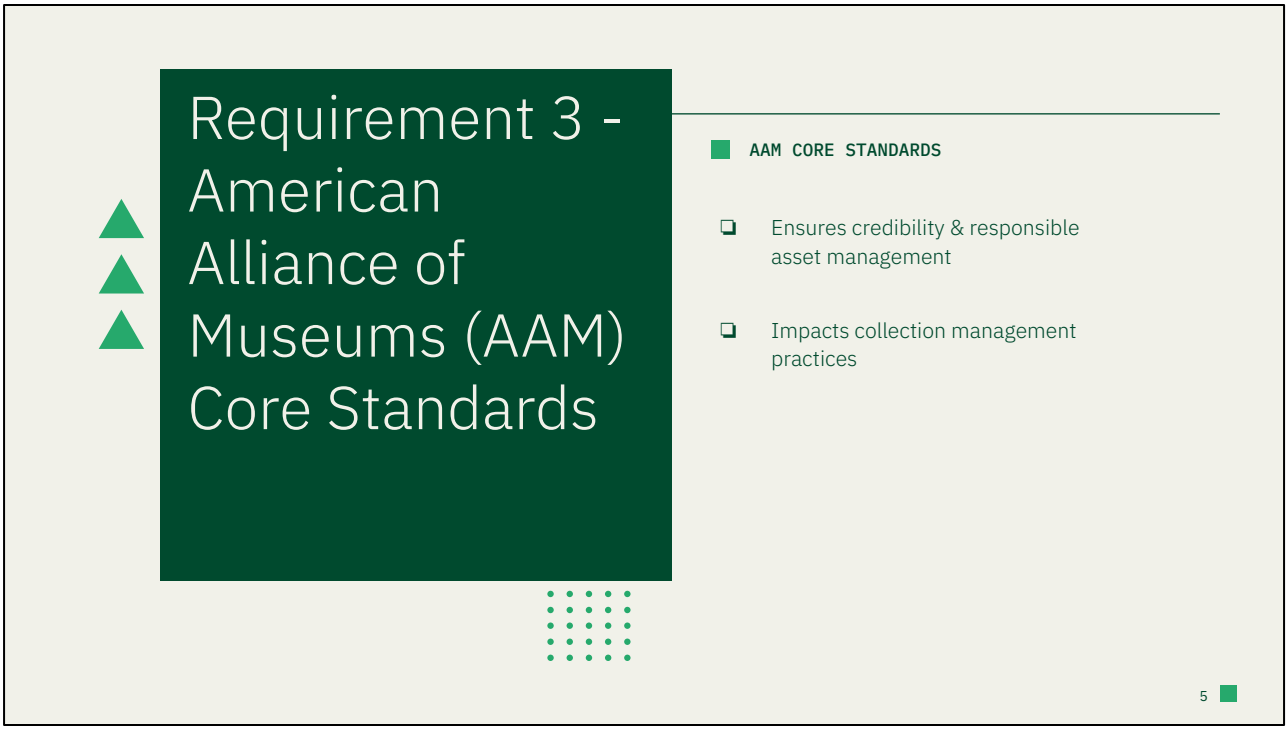

In order to protect the museum's information assets effectively, NIST compliance should be achieved. Ad hoc cybersecurity is insufficient because it is reactive, inconsistent, and uncoordinated. NIST compliance would create a structured risk management process for the museum, helping to ensure continuous data protection and privacy, and maintain institutional trust and funding.
(Source used: AAM, n.d.; Dates, 2025)




Now, I would like to discuss the regulatory and compliance requirements that are critical to the Tenement Museum. The first one is the National Historic Preservation Act (NHPA) due to the museum's designation as a National Historic Landmark and its responsibility to preserve and protect historic resources. The NHPA impacts the museum's preservation practices by ensuring that restoration technologies maintain historical integrity (do not make too many changes). Noncompliance could lead to the loss of federal funding and assistance.
(Sources used: AAM, n.d.; Solomons, 2016)




The next requirement is the General Data Protection Regulation (GDPR) because the museum has a responsibility to protect the personal data of visitors that it collects and processes, and the regulation is referenced in the museum website's Privacy Policy. GDPR impacts ticketing and donations processes by establishing data minimization, collecting only the necessary personal information for each transaction. Noncompliance could result in fines and reputational damage.
(Sources used: AAM, n.d.; Tenement Museum, n.d.)




The third requirement is the American Alliance of Museums (AAM) Core Standards for Museums due to the museum's responsibility to follow best practices to maintain its unique assets. The AAM Core Standards impacts collection management practices by establishing proper acquisition, documentation, and sharing procedures. Noncompliance could result in the loss of the museum's AAM accreditation as well as public trust.
(Source used: AAM, n.d.)

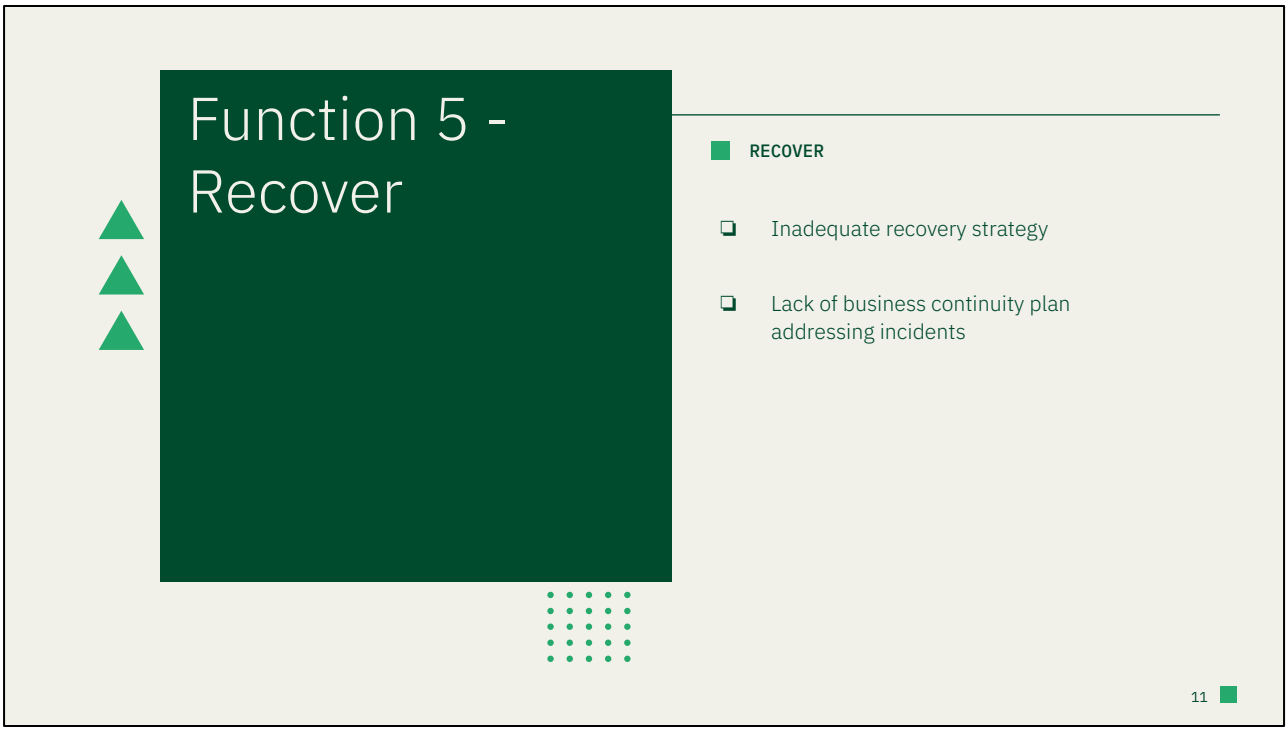

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is built around five core functions: Identify, Protect, Detect, Respond, and Recover. This makes up a structured risk management process, as mentioned previously. By following the NIST CSF, we can take a proactive cybersecurity approach rather than a reactive one. This will help ensure the security of the museum's most critical information assets and services, which include its collections for historic knowledge preservation and sharing, financial records for planning and reporting, and digital platforms for accessibility to museum resources.
(Sources used: Dates, 2025; NIST, 2018)


Now, I would like to cover issues relevant to each function of the NIST CSF, beginning with the first function of the framework, which is to identify. The museum's asset inventory doesn't currently account for all of its digital assets, leading to critical assets being overlooked in security planning, making them vulnerable to attacks. The museum also lacks risk assessment procedures that are tailored to its assets, potentially leading to overlooking data integrity compromises and attacks, which could have reputational and financial consequences.
(Sources used: NIST, 2018; Schou & Hernandez, 2015; Sebastian-Coleman, 2018)


The second function of the framework is to protect. The museum's access control implementation is limited with regards to its digital assets, resulting in overly broad access permissions for staff and a lack of multi-factor authentication for critical accounts, increasing the risk of unauthorized access to systems and data. Current data security measures are also inadequate due to the lack of robust encryption for data at rest and in transit, leaving data vulnerable to breaches.
(Sources used: NIST, 2018; Schou & Hernandez, 2015; Sebastian-Coleman, 2018)

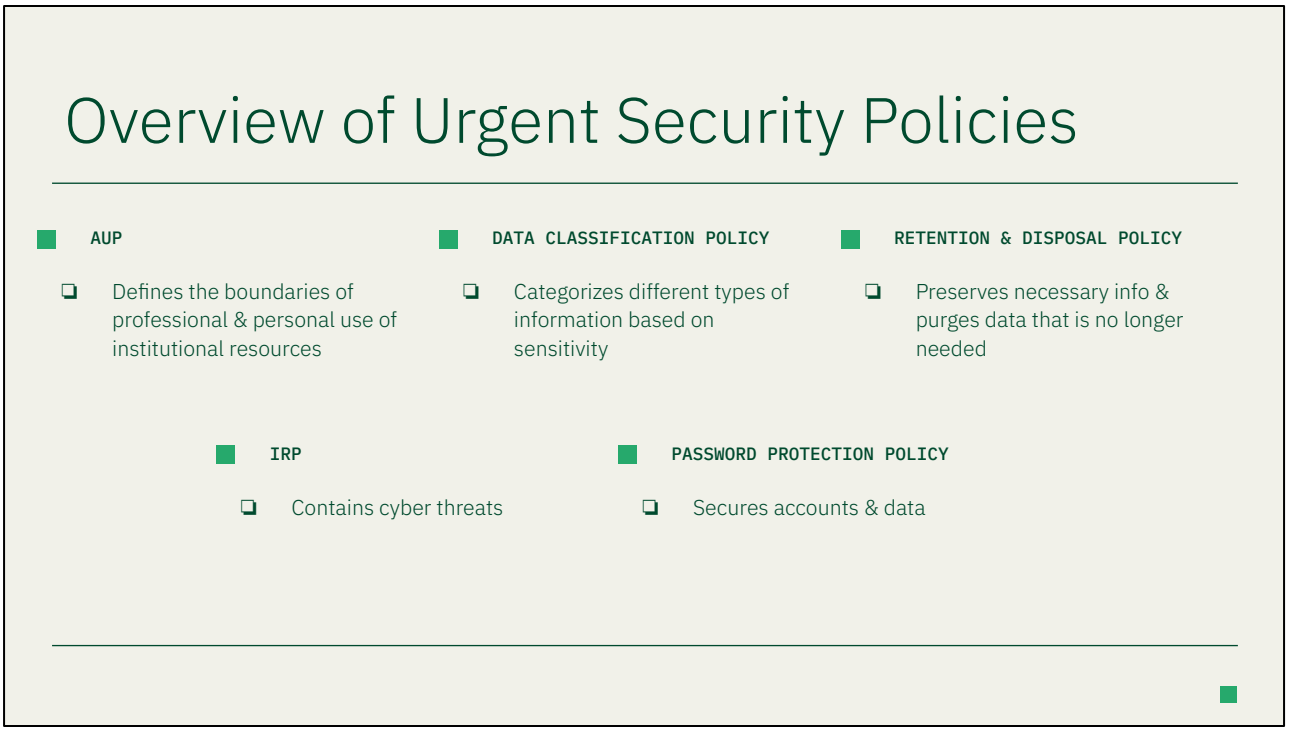

The third function of the framework is to detect. The museum currently lacks continuous monitoring for its networks, systems, and applications, resulting in delayed detection of anomalous activities, allowing threats to persist before being identified. The museum also does not have sufficient resources and expertise to effectively analyze event logs for anomalies, leading to indicators of compromise potentially being missed.
(Sources used: NIST, 2018; Schou & Hernandez, 2015; Sebastian-Coleman, 2018)


The fourth function of the framework is to respond. The museum currently lacks a well-defined incident response plan, which could lead to prolonged downtime and increased data loss in the event of a cyberattack. There are also limited communication protocols in place during a cybersecurity incident, which could result in uncoordinated reactions and reputational damage due to delayed or unclear public statements.
(Sources used: NIST, 2018; Schou & Hernandez, 2015; Sebastian-Coleman, 2018)



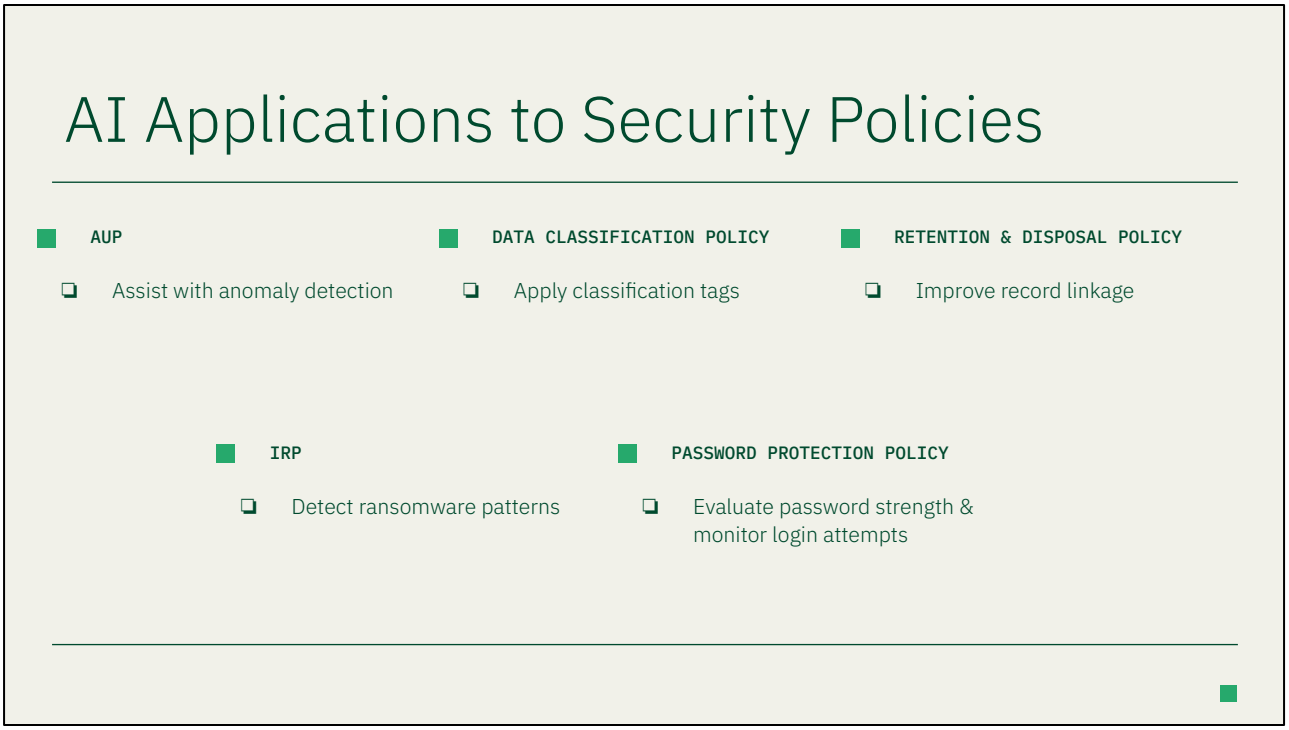

The fifth function of the framework is to recover. The museum's lack of a comprehensive recovery strategy for critical systems and data could lead to permanent data loss and prolonged operational disruption in the event of a cyberattack or system failure. The museum also does not have a detailed business continuity plan that addresses how to maintain essential operations in the aftermath of a cyber incident, which could lead to significant financial losses and a failure to fulfill its mission during a crisis.
(Sources used: NIST, 2018; Schou & Hernandez, 2015; Sebastian-Coleman, 2018)


To review, the NIST CSF has five core functions: Identify, Protect, Detect, Respond, and Recover, which make up a structured risk management process, helping ensure the security of the museum's most critical information assets in a proactive way. (Sources used: Dates, 2025; NIST, 2018)



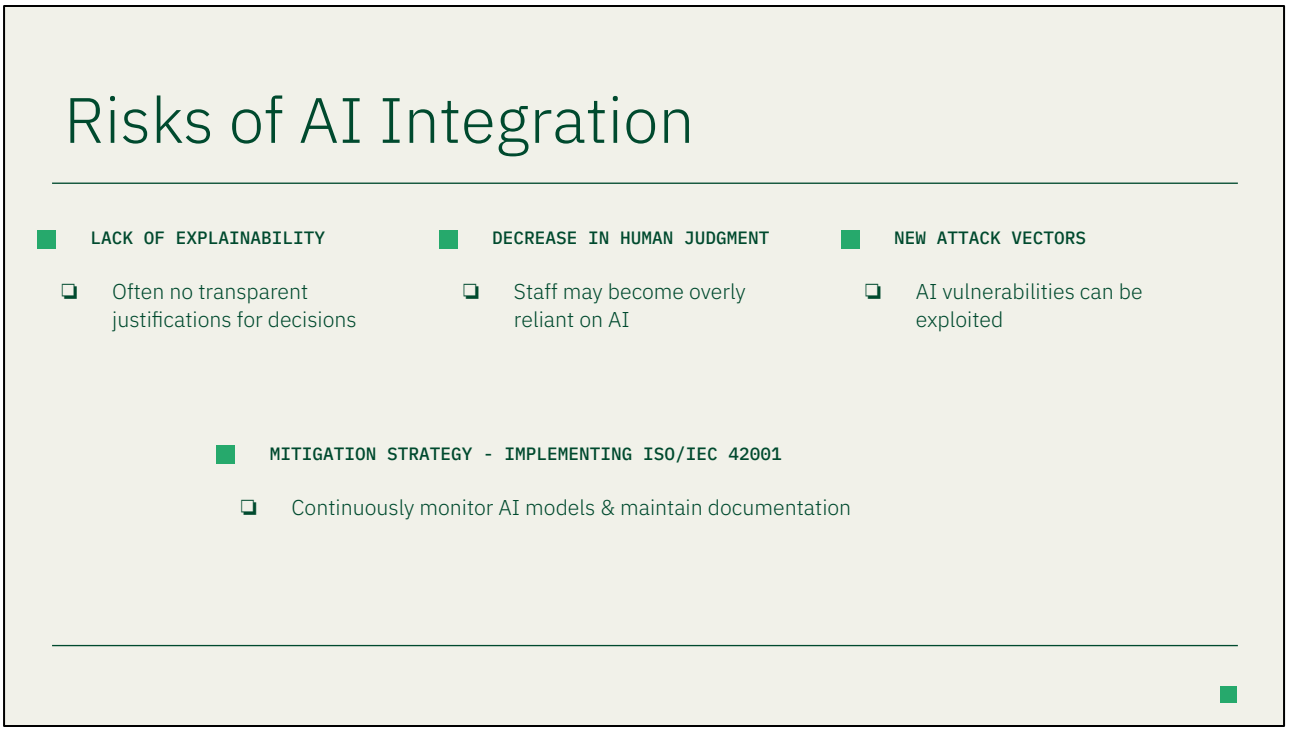

Five security policies that the Tenement Museum should prioritize urgently are an Acceptable Use Policy (AUP), Data Classification Policy, Retention & Disposal Policy, Incident Response Policy (IRP), and Password Protection Policy. An AUP matters to the museum because it is essential to defining the boundaries of professional and personal use of institutional resources for a diverse staff of historians, educators, and administrative personnel. A Data Classification Policy is critical for the museum to categorize its different types of information based on its level of sensitivity (such as confidential financial data vs public historic data), allowing security controls to be implemented accordingly. A Retention & Disposal Policy is important because it balances the museum's need to preserve history with its legal obligation to purge sensitive personal data that is no longer needed. An IRP is significant because it ensures the museum can quickly contain a threat, as well as preserve evidence for law enforcement and maintain the continuity of its educational mission. A Password Protection Policy is crucial because it helps secure accounts and data across the museum's various platforms (like ticketing systems and email), mitigating risks like credential harvesting.

(Sources used: AAM, n.d; CIS, n.d.)



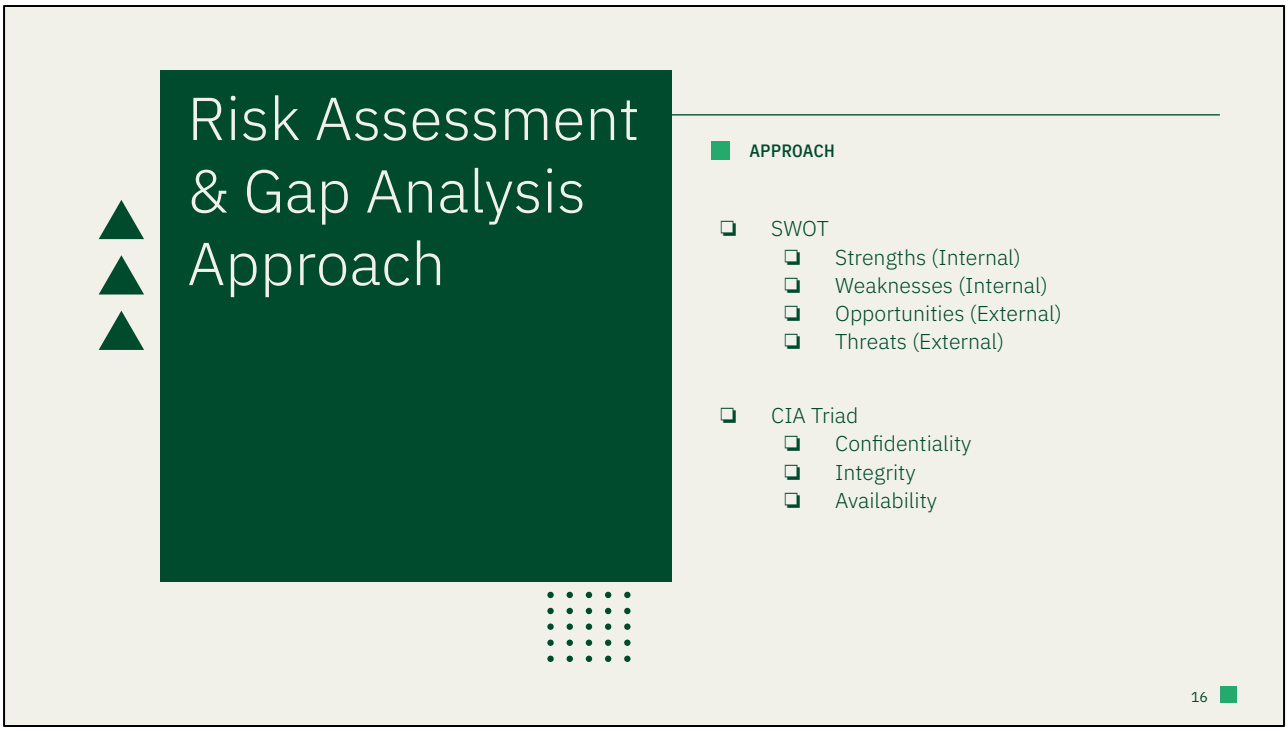

For an AUP, AI could be applied to assist with anomaly detection by establishing a baseline of normal museum employee activity and flagging deviations (like a staff member attempting to access prohibited sites). AI can assist with a Data Classification Policy by understanding the context of a document (like a public historic record vs a private donor agreement) and apply the appropriate classification tag (the tagging would likely also need human review in order to ensure accuracy). Beyond automation, AI could assist with a Retention & Disposal Policy by improving record linkage, like being able to find a donor or visitor's data across disparate systems (such as ticketing, email, and archives) to ensure a complete purge when they request data deletion under GDPR. For an IRP, AI can assist by detecting ransomware patterns, analyzing log data to identify the root cause of the incident, and suggesting policy updates to prevent a recurrence. AI can assist with a Password Protection Policy by evaluating the strength of staff passwords during the creation process and monitoring for anomalous staff login attempts (perhaps triggering Multi-Factor Authentication [MFA] requirements in response). The use of AI is practical for the museum in regard to the efficiency gains it brings about, but has limitations regarding cost and explainability.

(Sources used: AAM, n.d.; NordVPN, 2020; PANW, 2015; Shu, n.d.)




Integrating AI-driven technologies with security policy execution at the Tenement Museum could introduce risks regarding a lack of explainability, a decrease in human judgment, and the potential introduction of new attack vectors. AI models often do not provide transparent justifications for their decisions and could be affected by algorithmic biases, making it difficult to trust AI's assessments. Information technology and security staff may also become overly reliant on AI for anomaly detection and analysis, when AI should be used as additional protection rather than a replacement for human intuition. It is also possible for malicious actors to exploit AI vulnerabilities through tactics such as prompt injection to trick the AI into misidentifying or ignoring a threat. To mitigate these risks, the museum could implement ISO/IEC 42001 (an international standard for responsible AI Management Systems [AIMS]), emphasizing continuous monitoring of AI models to ensure accuracy and maintaining documentation of data provenance and model training to ensure transparency.

(Sources used: Microsoft, 2025; NordVPN, 2020; PANW, 2015)




I would recommend performing a SWOT analysis to determine the museum's internal strengths and weaknesses as well as external opportunities and threats. Analyzing the weaknesses and threats in particular will help us determine what gaps exist at the museum. We can then prioritize which gaps we would like to mitigate first by consulting the CIA triad (Confidentiality, Integrity, and Availability). This will help us keep our planning from a perspective of Information Assurance (IA).

(Sources used: AAM, n.d.; Renault, 2025; Sebastian-Coleman, 2018)

# SWOT & Gap Analysis Insights

**STRENGTHS**

- Unique historical assets
- Robust educational programming

**WEAKNESSES**

- IT resource limitations
- Disparate information systems

**OPPORTUNITIES**

- Digital expansion
- Grants for digital preservation & security

**THREATS**

- Unauthorized access attempts
- Volatile budget

Key insights from the SWOT analysis are that the museum's strengths lie in its unique historical assets involving its tenement buildings and robust educational programming. Its weaknesses include IT resource limitations due to its non-profit nature and disparate systems for information regarding collections, donors, and visitors. Opportunities include digital expansion by integrating software platforms as well as grants for digital preservation and security. Some threats are cybersecurity risks as hackers could try to gain access to sensitive donor financial information as well as a volatile budget due to fluctuations in tourism and government funding. These insights support IA planning and resource prioritization by indicating that we should prioritize confidentiality due to threats to donor data, ensure integrity of historical information by prioritizing resources towards immutable storage and digital signatures, and maintain availability by shifting resource allocation from on-premise servers to cloud-based hosting with robust Disaster Recovery (DR) plans.

(Sources used: AAM, n.d.; Renault, 2025; Sebastian-Coleman, 2018)


The findings from the SWOT analysis are relevant to the CFO's work because it demonstrates that potential revenue from tourism and grants may be better applied towards IT and digitization efforts. The SWOT analysis results are also relevant to the CIO's work because the disparate information systems and need for cybersecurity measures demonstrate the gap between traditional archival methods and more modern methods, calling for the modernization of the museum's information systems.

(Sources used: AAM, n.d.; Sebastian-Coleman, 2018)

# Summary

**REQUIREMENTS**

- ❏ NHPA
- ❏ GDPR
- ❏ AAM Core Standards
- ❏ NIST Compliance

**NIST CSF**

- ❏ Identify
- ❏ Protect
- ❏ Detect
- ❏ Respond
- ❏ Recover

**SECURITY POLICIES + AI**

- ❏ AUP
- ❏ Data Classification Policy
- ❏ IRP
- ❏ Password Protection Policy
- ❏ Balancing AI's pros & cons

**SWOT GAP ANALYSIS**

- ❏ Strengths
- ❏ Weaknesses
- ❏ Opportunities
- ❏ Threats
- ❏ CIA Triad
- ❏ C-Suite Considerations

In summary, our IA plan should consider regulatory requirements and standards, take a structured approach to risk management using the NIST CSF, include security policies that protect the museum's information assets, utilize AI for policy enforcement and execution, consider the museum's strengths, weaknesses, opportunities, and threats, apply the CIA triad to help bridge these gaps, and involve museum executives in the gap mitigation process.
(Sources used: AAM, n.d.; CIS, n.d.; Dates, 2025; NIST, 2018; Renault, 2025; Sebastian-Coleman, 2018)

# References


- American Alliance of Museums (AAM). (n.d.-b). *Core Standards for Museums*. https://www.aam-us.org/programs/ethics-standards-and-professional-practices/core-standards-for-museums/
- Center for Internet Security (CIS). (n.d.). *SANS Policy Templates*. https://www.cisecurity.org/wp-content/uploads/2019/08/NCSR-SANS-Policy-Templates.pdf
- Dates, E. (2025, March 7). *Everything You Need to Know About NIST Standards*. VComply. https://www.v-comply.com/blog/nist-standards/
- Microsoft. (2025, April 25). *ISO/IEC 42001:2023 Artificial Intelligence Management System Standards - Microsoft Compliance*.
- NIST. (2018). The CSF 1.1 Five Functions. *NIST*. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions
- NordVPN. (2020). *Artificial intelligence in cybersecurity*. YouTube. https://www.youtube.com/watch?v=GJMevKox_Q8
- Palo Alto Networks (PANW). (2015). *What Are the Barriers to AI Adoption in Cybersecurity?* https://www.paloaltonetworks.com/cyberpedia/what-are-barriers-to-ai-adoption-in-cybersecurity
- Renault, V. (2025). *SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats*. Community Tool Box; University of Kansas. https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/main
- Schou, C., & Hernandez, S. (2015). *Information assurance handbook: Effective computer security and risk management strategies*. McGraw-Hill Education.
- Sebastian-Coleman, L. (2018). *Navigating the labyrinth : an executive guide to data management*. Technics Publications.
- Shu, D. (n.d.). *How to use AI for security compliance? Arphie.ai. https://www.arphie.ai/glossary/how-to-use-ai-for-security-compliance*
- Solomons, G. (2016). *Parks and Preservation.* Tenement Museum. https://www.tenement.org/blog/parks-and-preservation/
- Tenement Museum. (n.d.). *Privacy Policy*. https://www.tenement.org/privacy-policy/




These are the references I used to create this presentation.

# Thank you!



Thank you very much for your time and consideration.