TABLE OF CONTENTS

1. Introduction

This section introduces why this report is being conducted, the standard control framework used in writing this report and the scope of the report to assist in properly defining what systems and operations present in the University are under evaluation, and why they are being evaluated using a recognised and accepted standard or methodology.

1.1 Purpose of Assessment

The aim of this assessment is to conduct a full risk management evaluation for Atlantic Technological University's financial application system (Banner Financial System) with a concentrated focus on the identification, assessment and prioritisation of risks based on their probable likelihood and resulting impact and proposition of risk control strategies for each risk using recognised risk control frameworks.

1.2 Framework used

The framework used for this assessment is the NIST 800-30 Revision 1(2012) which is the revised version of the original legacy framework published in 2002. The assessment flow of the framework is:

I. Identify threat sources and events (Nist 800-30 2012).
II. Identify vulnerabilities and predisposing conditions (Nist 800-30 2012).
III. Determine likelihood of occurrence (Nist 800-30 2012).
IV. Determine Magnitude of Impact (Nist 800-30 2012).
V. Determine Risk (Nist 800-30 2012).

1.3 Scope

The scope of this assessment is Atlantic Technological University's financial application system which is known as Banner Finance("Banner").

2. IT System Characterisation

This section gives a comprehensive overview of the University in question particularly its IT department and financial management application system. It exists to give a clearer picture of what is being evaluated and highlights the practical state of the institution and the criticality of the continuous operation of the University to not just the section it inhabits, but to the Irish nation as a whole.

2.1 Organisational Overview

Atlantic Technological University is an Irish Technological University based in the northern section of the country; The University offers a wide collection of degrees ranging

from the undergraduate level to postgraduate level degrees such as master and doctorate degrees in various fields. The University is also an integral part of the Irish educational sector as it boasts 20,000 active attendees.

The University also operates a centralised IT system which means all computer related processes observed by the University are performed by the IT department, which also serves as the only sustainer of the technological, telecommunications and end-user support requirements of the University.

2.2 IT Department Overview

The IT Department consists of 35 staff all under the management of the IT Executive Director (ITED) that are responsible for the systems and applications within the university, which includes documentation and training of procedures and system controls pertaining to various applications. Key management personnel in the IT department that are relevant to this assessment include The IT Executive Director, The Banner Security Administrator, The Operations Supervisor, The Systems Administrator and The Network Administrator.

2.3 System in Scope: Banner Finance

Banner Finance, a financial management application that operates on a Red Hat Enterprise Linux operating system that holds essential and sensitive information about the finance, accounting, Human Resources and Payroll of the University. The personnel which also make use of Banner include the Finance, Accounting, HR and IT support personnel.

2.4 Supporting Infrastructure and Controls

The University already has existing security and access controls such as:

I. The Bring Your Own Device security policy already set in place by the University.
II. Biometric Devices to enforce authentication and authorization control.
III. Presence of human security personnel to ensure monitoring and deterrence.
IV. Video Surveillance Systems.
V. Visitor Logs.
VI. Fire Suppression Equipment (FM-200 and fire extinguishers).
VII. Uninterruptible Power Supply.
VIII. Backup Power Generators.
IX. Raised Floors.
X. Configuration of Password Settings.
XI. Conduction of user access reviews.
XII. Restriction of work changes and modifications by authorized personnel to test environment before implementation in live/production environment.
XIII. Daily Backups.

2.5 Logical Security Posture

1. While some password settings have indeed been configured, the current configurations set in place are not in line with industry best practices.
2. Reviews of user access within Banner is being conducted, however it is not being conducted on a periodical basis. Terminated user accounts in Banner are removed but not usually on time. The Documentation that provides evidence of reviews and the removal of outdated user access is not preserved.
3. Work changes and modifications in Banner by programmers are restricted to the development environment before deployment to production, however results of the test are not reviewed or approved by management before final implementation into production.
4. Although the information on Banner is backed up daily, the operations supervisor made it clear that the backups are only carried out locally as the University has no remote facility set in place for backup storage.

2.6 Sensitivity Classification

Confidentiality: As Banner holds critical and sensitive information such as the financial, accounting, human resources and payroll data, any breach in confidentiality leaves these sensitive pieces of information at severe risk which would not only damage the privacy structure and reputation of the organisation, but it could also potentially lead to financial loss to the University, compliance violations, and legal disputes against the University. Given the degree of loss of confidentiality is breached, the confidentiality of Banner should be treated as a highly confidential asset(Sailpoint, 2025).

Integrity: If the information gotten from Banner undergoes an intentional or unintentional improper alteration such as manipulated payroll amounts or changes in vendor payment details, this could result in serious financial, audit and legal troubles for the University which demands that the integrity status of the system should be pristine and perfect(Sailpoint, 2025).

Availability: As Banner supports essential processes such as finance, accounting, human resources and payroll operations, any change in the availability state of Banner could result in late payroll, unpaid vendors, lack of up-to-date financial overview, and delayed budgeting reports, these could have serious ramifications for the University as any downtime experienced could affect critical University operations. This makes the availability of the Banner application of utmost importance(Sailpoint, 2025).

In summary, the Banner financial system is evaluated as highly sensitive across the confidentiality, integrity and availability elements, this highly sensitive nature will determine the evaluation of the risk impacts and prioritisation of control remediations of vulnerabilities discovered in the Banner financial application system.

2.7 Information System Boundaries for Banner Financial System

Boundaries can be regarded as the edge of a system that connects to the limit of another system. Some boundaries present in the Banner financial system include:

1. Access Control Boundary
2. Physical Boundary Protection
3. Network Boundary Protection
4. Data Boundary Protection
5. Environmental Boundary Protection
6. External Boundary Protection

3. Risk Identification

According to the NIST 800-30 framework, Vulnerabilities can be separated into 3 tiers, with Tier 1 being weaknesses that can be widespread across different organisations and can have significant negative impacts if exploited by threat sources; supply chain attacks are such vulnerabilities on this scale. Tier 2 vulnerabilities are flaws that spread across information system boundaries, and Tier 3 vulnerabilities refer to deficiencies that are limited to specific information system boundaries (Nist 800-30 2012). This section is focused on the identification and categorisation of the vulnerabilities and threat sources that can either potentially exploit or be used to exploit the Banner financial application system. These risks are then presented in a table format to better understand and map what vulnerabilities and threat vectors affect different areas in the security system of the University.

3.1 Vulnerabilities Extracted from Scenario

1. The password configuration policies are outdated and don't align with current industry best practices.
2. Reviews of user access within Banner are not conducted periodically.
3. Lack of Documentation showing evidence of review and removal of user access.
4. Delayed removal of discontinued user accounts.
5. Lack of review and approval of test results before deployment into production by management.
6. Backups are stored only on the premises of the University.
7. The Bring Your Own Device increases the surface of attack of the University.

3.2 Threat Sources

1. Internal human threats.
2. External attackers.
3. Accidental human error.

4. Environmental threats.
5. Compromise of the BYOD system through devices with access to the network.

3.3 Table: Vulnerability and Threat Sources

As referenced in ***appendix table 1,*** a table highlighting the various IT areas with discovered vulnerabilities and potential threat sources is documented. This table helps to provide an overview of the different areas in the IT security system with weaknesses of each area and how those weaknesses can be exploited to gain access using that particularly vulnerable IT area.

4. Control Analysis

The purpose of this section is to identify all existing controls already present in the University and surrounding the Banner system in particular that exist to improve its security posture. This section will help to identify the gaps in each control and how they can be improved in later sections of this report.

4.1 Physical Controls

These controls try to limit physical access to the University's system. The physical controls include:

1. Biometric Devices: Ensures only authorized personnel have access to restricted specific sections in the University.
2. Security Guards: Use of individuals to provide continuous monitoring and enforce access controls to barred facilities.
3. Video Surveillance: A control that offers continuous monitoring and provides post incident evidence of particular sections in the University.
4. Visitors Logs: Provide evidence of entry and exit of personnel into restricted areas to track the timeline of events post incident.

4.2 Environmental Controls

These controls exist to mitigate the effects of natural or environmental disaster on the Banner financial system's operational infrastructure. These environmental controls include:

1. Fire Suppression System (FM-200): Fire suppression systems that automatically go off under specific conditions to protect critical infrastructure.
2. Uninterruptible Power Supplies (UPS): Ensures data availability during outages, preventing data loss and unavailability.
3. Alternate Power Generators: Provides another source of power supply when the UPS power supplying capacity ends.

4. Raised Floors: Protects operational equipment from disasters such as floods.

4.3 Logical Controls

These controls serve as the technical controls implemented to ensure a baseline security posture of the Banner system. These controls include:

1. Configured Password Settings.
2. Restriction of Programmers to test environments during modifications of the Banner system.
3. Daily Backups of the Banner system is conducted by the relevant personnel in the University.
4. Policy Controlling Network Access
5. BYOD Security Policy

4.4 Administrative Controls

Administrative restrictions that limit unlimited access of the network and ensure a procedural operation of activities present within the network. These controls include:

1. Information Systems Operations Policies.
2. Information Security Policies.
3. Restricted Authority in Access Control Changes
4. Conduction of user access reviews within the Banner financial application system.
5. Termination of user accounts that are no longer in use within the Banner financial application system.

5. Risk Likelihood Determination

This section measures the likelihood of each risk found in the University as identified in ***appendix table 1.*** Determining the likelihood that threat events of particular concern could result in certain negative impacts by considering:

I. The attributes of the threat sources that could start the attack.
II. The identified vulnerabilities.
III. The overall strength of the organisation by considering the safeguards implemented by the organisation.

Based on these factors, a likelihood range of low-medium-high is used as a scale to understand how likely that system is to be exploited (Nist 800-30 2012).

5.1 Capabilities of Threat Sources on Each Identified Risk

Password Configuration: Given the outdated status of the password configuration settings and the sensitivity of the information, the likelihood of a threat actor could exploit this vulnerability is regarded as one of moderate likelihood.

BYOD Policy: Given the deployment of security policies on the BYOD scheme and how each device connecting to the network is obligated and forced to follow the security policies to have access to the network, the likelihood of an attack through this surface area is of a low likelihood of occurrence.

User Access Reviews: Reviews of user access are not periodic, however the likelihood of an attack through this surface area is of negligible likelihood due to its nature as a post incident response measure.

User Accounts: The nature of the sensitivity of data under consideration makes the delay in inactive user accounts of very grave concern to the University and the likelihood of an exploit through this means is of very high probability.

Documentation: The likelihood of an exploit through this area is of a very low possibility as documentation is more of a compliance and post incident response measure than a preventative measure.

Application Modifications: The likelihood of an attack on the University through the lack of proper oversight on the modifications made to the application is of very high likelihood.

Backups: The lack of multiple backup sources ensures the likelihood of an attack on the storage systems of the Banner application system is of a very high likelihood.

5.2 Severity of Identified Risks

Password Configuration: Increases the possibility of success of brute-force attacks.

BYOD Policy: Does not pose a severe threat to the organisation as there are enforced policies in place.

User Access Reviews: Increases the possibility of sustained insider attacks or impersonated access for a significant period of time.

User Account: Increases threat of insider attack or unauthorized access of inactive accounts by external entities.

Documentation: Increases the possibility of accidental human error or phishing.

Application Modifications: Increases the likelihood of modifications that are not approved by management.

Backups: Increases likelihood of data loss from ransomware or environmental incidents.

5.3 Existing Control Strengths

Password Configuration: Weak Controls.

BYOD Policy: Strong Controls.

User Access Reviews: Weak Controls.

Documentation: Weak Controls.

Application Modifications: Weak Controls.

Backups: Weak Controls.

6. Risk Impact Analysis

This Section highlights the impacts of the identified vulnerabilities present in the University identified in ***appendix table 1.*** Detrimental impacts are described as possible harm that could be caused to the assets and operations of the University, the location of the possible security incident, and whether the effects of the incident are kept limited or unable to be kept limited are all factors that affect the how severe the impact of the security incident will be. This categorisation will determine the evaluation of the impact of each vulnerability discovered in the University's systems.

6.1 Impact of Identified Risks

As referred to in ***appendix table 2,*** The Assessment of the potential impact of identified vulnerabilities in each IT area was outlined along with their tier priority classification and confidentiality, integrity and availability impact models. Given the sensitivity of the data being handled it became clear all the identified vulnerabilities could have severe consequences on the University if they were ever exploited. The vulnerabilities were found to also cover the three categories of tier prioritisation through infringing on compliance laws, affecting the operational organisational requirements and spreading out to the information systems in the event of a potential breach.

6.2 Existing Controls that Mitigate Impact of Security Incident

1. Biometric Access Controls.
2. Security Guards.
3. CCTV Surveillance.
4. UPS and Backup Generators.
5. Fire Suppression Equipment.
6. Separation of Test Environment from Live Production.

7. Risk Level Determination

This section aims to use factors obtained from earlier sections such as likelihood and impact to properly categorise the level of risk that each identified vulnerability exposes the University to according to the NIST 800-30 standard. As described in ***appendix table 3,*** a risk assessment is carried out using the probability of likelihood and the impact the breach would have to the University for each identified vulnerability area, this assessment helps to better understand what exactly the risks facing the University are and possible threat events that could occur for the different identified weaknesses in the University.

8. Control Recommendations

This section highlights the different safeguards that can be implemented on already existing controls to improve the security posture of the University and enable the institution to properly eliminate or mitigate the effects of the various risks that could be used to exploit critical systems in the University and affect operation and functionality of the institution.

8.1 Administrative Controls

1. Adopt zero trust approach to security(Martinez, 2025).
2. Perform regular reviews of access by users.
3. Ensure timely delay of discontinued user accounts.
4. Ensure approval of any changes to the Banner system by the IT Executive Director.
5. Automate Workflows(Martinez, 2025).
6. Make use of the least privilege principle(Martinez, 2025).
7. Utilize Role-Based Access control and Attribute-Based Access control policies(Martinez, 2025).
8. Perform regular audits(Martinez, 2025).

8.2 Technical Controls

1. Enforce strong password policy(Martinez, 2025).
2. Enforce multi-factor authentication system(Martinez, 2025).
3. Integrate and upgrade firewalls to levels that match current industry best practices(Walkowski, 2019).
4. Implement a trusted and effective anti-virus software across the network(Walkowski, 2019).
5. Ensure data not in active use is encrypted at all times(Walkowski, 2019).
6. Integrate updated Intrusion detection and intrusion prevention systems into the network(Walkowski, 2019).
7. Implement Access Control Lists to control network traffic flow(Walkowski, 2019).

8.3 Physical and Environmental Controls

1. Create off site Backup of Banner system data to mitigate the impact of environmental disasters.
2. Restrict work changes to the Banner system to the premises of the University.
3. Login to the Banner system should be limited to the premises of the University except in cases of emergencies.
4. All connections to the network from remote locations should be logged and strictly monitored.
5. All equipment with access to the Banner system should be kept in secure and restricted areas with regular monitoring of the areas.

8.4 Bring Your Own Device (BYOD) Risk Controls

1. Provide a minimum level of access necessary to mitigate the influence of data leakage(Yacono, 2024).
2. Provide awareness on the importance of downloading applications from legitimate sources like google play store or app store(Yacono, 2024).
3. Make use of application segregation and VPNs to create barricades between personal and work data on personal devices(Yacono, 2024).
4. Implement single sign-on processes for end devices connecting to the network(Yacono, 2024).
5. Use of Intrusion detection and intrusion prevention systems to monitor network traffic for anomalous activity(Yacono, 2024).

9. Results Documentation

This assessment highlights the University's Banner financial application system which contains sensitive financial, HR, accounting and payroll data, which affects the risk and impact a breach could have on the system not only on the data but the operational and compliant requirements of the University. Outdated password configurations, non-periodical review of access to the Banner system by users, Delayed termination of discontinued accounts, unmaintained documentation, lack of review and approval of management to modifications of the Banner system, and a lack of remote backup locations were some identified vulnerabilities that increased the likelihood and risk of an attack against the systems of the University. The presence of the BYOD scheme further spreads the attack area of the University by opening up the possibility of the connection of a corrupted device to the network.

Making use of the Nist 800-30 revision 1 likelihood and impact characterisation methodology, due to both increased chances of exploitability and the resulting effects on the Confidentiality, Integrity and Availability of the data present within the Banner system. While some physical controls helped to mitigate the risks of an incident, the flaws posed by the logical information system boundary were discovered to be too severe to be properly mitigated by existing controls implemented by the University.

Control recommendations that followed the NIST 800-30 revision 1 were identified and documented to solve the problems posed by the identified vulnerabilities. Such controls included the implementation of authentication and automated controls into the university to reduce the risk of compromise, access control policies and lists to control and monitor network activity, audits, documentation of operations, and off-site Backup of data were some of the identified controls that strengthens authentication and account management, enhance supervision and audit abilities, enforces reliable documentation and implements access segmentation for the BYOD scheme.

The findings detailed in this report are to enable the University's IT Executive Director, Banner system administrator and other relevant personnel to understand the current security posture of the University and implementable controls to upgrade existing security posture. This assessment is in compliance with the NIST 800-30 revision 1 standard and helps to create an implementable blueprint to improve functional operation of the Confidentiality, Integrity and Availability of Banner's essential assets.

References

Martinez, J. 2025. 11 Identity & Access Management (IAM) Best Practices in 2025 | StrongDM. [Accessed 5 December 2025]. Available from: https://www.strongdm.com/blog/iam-best-practices.

Sailpoint 2025. CIA triad: Confidentiality, integrity, and availability. [Accessed 30 November 2025]. Available from: https://www.sailpoint.com/identity-library/cia-triad.

Walkowski, D. 2019. What Are Security Controls? [Accessed 5 December 2025]. Available from: https://www.f5.com/labs/articles/what-are-security-controls.

Yacono, L. 2024. The 8 Top BYOD Security Risks (and How to Mitigate Them). [Accessed 5 December 2025]. Available from: https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate.

Appendix

Table 1 – Vulnerability and Threat Sources

IT Area	Vulnerability	Threat Source
Password Configuration	Outdated Configurations of Passwords.	Brute force attacker or a user with a compromised password.
BYOD Policy	Vulnerable personal devices.	Device with access to the network that contains malware or is compromised.
User Access Review	Non-periodical user access	Disgruntled staff or attacker

	review.	that gains access through a compromised account.
User Accounts	Delay in termination of discontinued user accounts.	Disgruntled ex-staff that still possesses access to the account, attacker that gains access through outdated and inactive user accounts.
Documentation	Lack of maintained documentation showing details of user access review and user account termination.	Mistakes by staff, Internal administrative oversight errors.
Application Modifications	Management does not cross examine or personally approve the test results of changes being deployed to live production on the Banner application.	Unauthorized changes, Staff errors.
Backups	Storage is only present on premises.	Environmental disasters, Ransomware.

Table 2 – Assessment of Impact of different vulnerabilities discovered in the University

IT Area	**Confidentiality Impact in event of breach**	**Integrity Impact in event of breach**	**Availability Impact in event of breach**	**Overall Impact**	**Tier of Impact**
Password Configuration	Could lead to leak of sensitive financial data.	Could lead to modification of sensitive personnel and financial data.	Forced Lockouts could impact general University operations.	High	Tier 1, Tier 2, Tier 3.
BYOD Policy	Infected personal devices	Change in sensitive data through	Possible lockout of Banner	High	Tier 1, Tier 2, Tier 3.

	unknowingly releasing data.	access gotten from corrupted personal devices.	system through access to the network by infected end devices.		
User Access Review	Unauthorised or outdated users could use previous access to get information on sensitive data.	Unauthorised inactive users could use previous access to modify sensitive data on the Banner system.	Unauthorised users may trigger network access errors that may affect the uptime of the network. Although this vulnerability is not of critical concern to the availability of the system.	High	Tier 1, Tier 2, Tier 3.
User Accounts	Previous staff can go through or leak sensitive data in the Banner system.	Ex-staff could alter sensitive records.	Ex-staff or compromised accounts could disrupt the uptime of the system.	High	Tier 1, Tier 2, Tier 3.
Documentation	Missing documentation will allow unauthorised access remain undiscovered.	Manipulation of data cannot be properly traced.	Incident recovery may be delayed due to unavailable records.	High	Tier 1, Tier 2, Tier 3.
Application Modification	Unauthorized updates or	Unauthorised	Defective updates	High	Tier 1, Tier 2, Tier 3.

s	changes may create backdoors for data leaks.	modifications could lead to alterable data records.	could lead to system crashes.		
Backups	Theft of Backups could lead to leaks of sensitive data.	Infected backup files could lead to irreversible loss of data.	Critically damaging loss could be experienced which may lead to permanent data loss if an environmental incident were to occur in the University.	High	Tier 1, Tier 2, Tier 3.

Table 3 - Risk Assessment of Identified Vulnerabilities

IT Area	Likelihood	Impact	Risk	Description
Password Configuration	High	High	High	Weak Configuration settings that increase the probability of an attack due to the sensitivity of the data being stored, an attacker can use a brute force attack to get access to the system leading to a data exposure.
BYOD Policy	High	High	High	Students and staff connect to the network

				using personal devices, these devices are not personally managed or monitored by the university which creates an area of attack, compromised devices could be used by an attacker to manipulate Banner system.
User Access Review	Moderate	High	High	Delay in reviews of user access enables late discovery of unauthorised activity within the system, an attacker or insider could've accessed the system or data within the system for a significant amount of time without any suspicions being raised.
User Accounts	High	High	High	Inactive accounts are not removed on time which leaves roles for users that no longer use such roles dormant, an insider or a compromised device could be

				used to access or alter sensitive data.
Documentation	Moderate	High	High	Documentation detailing operations is not maintained, although this may not be directly exploitable but generally leads to weak post-incident responses and auditing, which can make the effects of breaches more devastating.
Application Modifications	Moderate	High	High	Unverified code could be uploaded to the Banner system, potentially leading to backdoors, application instability and data leaks or data alteration.
Backups	High	High	High	An environmental disaster could cripple the entire data infrastructure for the University leading to irreversible data loss and operation disruption.