RISK ASSESSMENT REPORT

Banner Finance System

TABLE OF CONTENTS

1. Introduction

1.1. Purpose of the Risk Assessment

This risk assessment evaluates the security structure of Atlantic Technological University's (ATU) Banner Finance system, which is the major financial application for managing sensitive financial, accounting, human resources, and payroll data for the college. This assessment identifies vulnerabilities, assesses threats, prioritizes risk levels, and recommends security controls and policies to protect the confidentiality, integrity, and availability of the university's crown jewel, which in this case is its financial information.

Since Banner processes large amounts of money in annual payroll, student fees, and also stores highly sensitive personal data, it is subject to GDPR protection. A comprehensive risk assessment is necessary to ensure regulatory compliance, protect the institution’s assets, and maintain the trust of the college’s stakeholders.

1.2. Risk Assessment Framework

This assessment uses the National Institute of Standards and Technology (NIST) Special Publication 800-30 methodology. (Guide for Conducting Risk Assessments, 2012).

NIST 800-30 provides a well-structured process of identifying and assessing information security risks within organizations. This framework was selected because of its standard recognition, comprehensive coverage of regulations, constant improvements, having resources that are public, and because it also aligns with ISO 27001/27005 standards. (FortifyData, 2025)

This assessment also references ISO/IEC 27001:2022 for guidance on how to handle risk.

ISO/IEC 27005: for an additional framework on how to assess and mitigate risk

ISO/IEC 27001:2013(E): for Controls framework

1.3. Approach Used

This assessment follows the key steps for a NIST 800-30 risk assessment process, which are as follows (Guide for Conducting Risk Assessments, 2012):

- Preparing for the assessment
- Conducting the assessment
- Communicating the results
- Maintaining the assessment

Also, we collected some data that includes document review of ATU security policies, performed on-site interviews with the IT Executive Director (ITED), Banner Security

Administrator (BSA), Operations Supervisor (OS), Systems Administrator (SA), and Network Administrator (NA), plus technical assessment of system configurations like Bring Your Own Device (BYOD) policy, and industry research on Red Hat Enterprise Linux and financial system vulnerabilities.

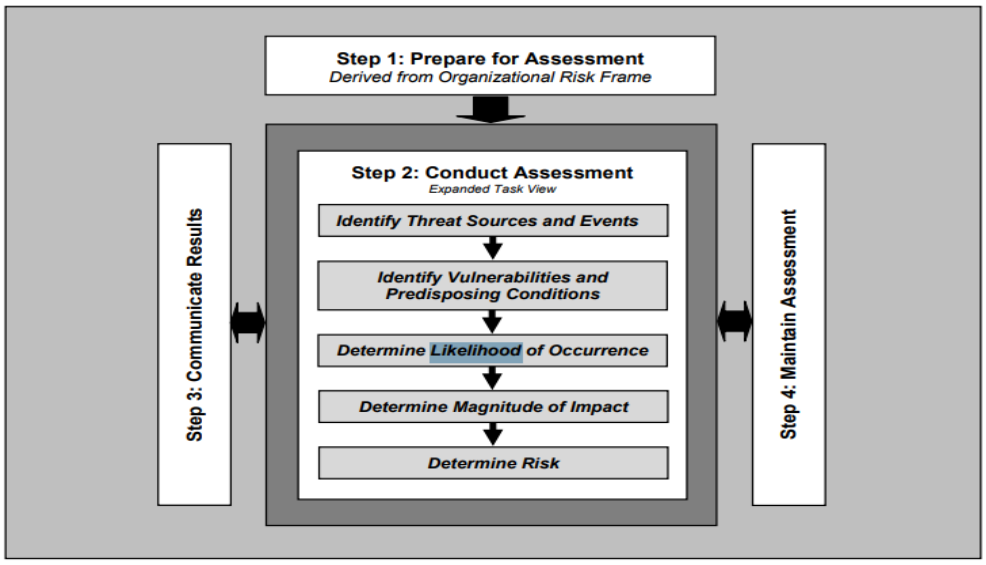

FIGURE 5: RISK ASSESSMENT PROCESS

(NIST, 2012)

2. IT System Characterisation

2.1. System Overview

We'll be using the Banner Finance system and the relevant Physical IT infrastructure of the college for our system scope. Banner is ATU's enterprise system operating on Red Hat Enterprise Linux, providing centralized financial accounting, human resources, and payroll processing. The system handles finances and data for finance personnel, HR staff, payroll administrators, IT support, and executive management, which gives it access to sensitive employee data, student financial records, and university budget information etc.

Physical IT infrastructure, which, as indicated by the Network Admin, contains the networking resources, access to computers, policies guiding the access and authorization of these resources, BYOD, biometric devices, video surveillance, uninterruptible power supplies, backup power generators, etc., using the ISO 27001:2022 Clause 4.1. (HighTable, 2025)

2.2. Assessment Scope and Boundaries

Scope Inclusions: Banner Finance application and all its relevant modules, Red Hat Enterprise Linux operating system, database management system, network infrastructure, physical data centre, user access controls, backup systems, and BYOD devices accessing Banner.

Scope Exclusions/Boundaries: Non-Banner IT systems for the college, e.g., learning management systems, student portals without Banner integration, third-party payment gateways assessed separately under PCI compliance, personal devices not accessing Banner, and university email systems like Outlook, that are not processing Banner data. (ISO 27001:2022 Clause 4.3)

2.3. System Components and Data Sensitivity

Here, we'll be discussing the sensitive data or components within the IT systems at ATU, mentioned in the system overview in (2.1) above.

Critical Components:

• Hardware: Servers/devices, storage systems, network equipment, UPS, backup generators

• Software: Banner Finance application, Red Hat Enterprise Linux, database management system, backup software, and network applications.

• Physical Controls: Biometric access devices, security guards, video surveillance, visitor logs, FM-200 fire suppression, HVAC, raised floors

• Logical Controls: Weak password authentications, inconsistent user access reviews, delayed account deprovisioning, and unapproved changes/controls.

Data Sensitivity Classification:

Data that are being collected and handled by the ATU are being classified based on the following risk levels:

Highly Sensitive Data (GDPR Protected): Employee Personal Identification Info, salary information, student financial records, bank account details, medical insurance selections, which is a special category data under GDPR Article 9. (Intersoft Consulting, 2025)

Business Critical Data: Financial transactions, payroll calculations, budget data, and audit trails required for financial accountability and regulatory compliance.

Data Risk: The risk across the security objectives mentioned above is very high. For example, a confidentiality breach would trigger GDPR penalties up to €20 million against the college, an integrity compromise with the financial department could enable fraud, and an

availability loss would prevent timely payroll and disrupt student billing. (ISO 27005:2022 Clause 7)

3. Risk Identification

In this step, we will identify the threats that can affect certain IT system areas of the ATU, and the vulnerabilities that might be exploited by these threats. Then we'll further discuss the risks that are involved. (NIST 800-30 Task 1-4)

3.1. Vulnerability and Threat Sources (Table 1)

IT Area	Vulnerability	Threat Source	Identifiable Risks
Access Control	Weak password configuration	External attackers, Insider threats (Untrained staff for password policy)	An unauthorized access via password guessing/brute-force will compromise confidentiality and integrity
Access Control	Delayed account deprovisioning from Banner	Terminated employees	A disgruntled former employee can use residual access to steal data or commit fraud.
Change Management	Insufficient approval for changes in updates, tests, and upgrades before launching	Malicious insiders	There could be an unauthorized modification introducing a backdoor access, or even disabling security.
Backup/Recovery	Untested backup restoration	Hardware failure, Ransomware	Loss of critical data
BYOD Security	Unmanaged device access	Lost/stolen devices without proper MFA containing critical data, Malware	A compromised personal device can gain entry to the Banner network
BYOD Security	Data leakage via personal devices	Negligent users	Sensitive payroll data can be leaked on an unencrypted / Phished device belonging to a staff member.

Network Security	Unclear network segmentation / Poor network security	External attackers	An attacker can gain access to the Banner servers after a phishing compromise.
Organization's Device Management	Potential unpatched systems	External attackers	CVE exploitation of an unpatched device / Linux software running the Banner or in the Data center
Physical Security	Single administrator authority	Admin unavailability	Having only 1 ITED might lead to a security failure during an emergency when the ITED is unavailable.

(NIST, 2012)

3.2. Key Observations

The newly implemented BYOD doesn't guarantee security as it even has the most flaws, especially considering how hard it could be to ensure implementation of MFA activities, secured training against phishing, etc, which might allow an intruder to enter the network.

Also, the remaining listed areas, with their corresponding threats, vulnerabilities, and risks, are also crucial, as any attack from them would have a high impact on the college.

4. Control Analysis

For the assessed system, it is necessary that we analyse the existing control measures, review them, and plan new controls either in the form of avoidance or mitigation rules or policies to ensure a secure system. So, for this section, I have documented a list of security control analyses for the IT system.

4.1. Existing Security Controls Assessment within the IT System Infrastructure

- Strong Areas according to the ITED and OS:
    - Physical security is okay, like biometrics, security guards, surveillance, and visitor logs.

    - Environmental protection is available (fire suppression devices, power protection, UPS and backup generators, raised floors),
    - Access segregation (RBAC) within Banner is limited to the ITED.

- Moderate Weakness Area as agreed by SA and BSA
    - Password configuration is below industry standards
    - Reviews of users with access within Banner are not conducted periodically
    - Backup strategy lacks off-site storage and testing.
    - The documentation that supports reviews and removal of user access is not maintained.

- Significant Gaps
    - Account termination of terminated employees is delayed or not even implemented
    - No Device Management for BYOD (multi-factor authentication)
    - No management approval for production changes

Summary: The current controls only effectively address physical and environmental threats, but do not provide sufficient protection against cyber threats. The BYOD policy increased the chances of attacks without initiating any corresponding security controls.

5. Risk Likelihood Determination

Likelihood means the probability of successful threat exploitation/occurrence of the risks we analysed within one year (using NIST 800-30 Task 2-4), to determine the likelihood. I'll be using the NIST table I referenced below, which segments the Likelihood into five levels from 'Very Low - Very High.' (NIST, 2012).

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

(NIST Special Publication 800-30 Revision 1, Table G-3, 2012)

VERY HIGH (10): The likelihood of the threat occurring is very high, this can be because the attacker is extremely motivated, highly capable, and the vulnerabilities are easily exploitable with available tools. Probability 96-100%.

HIGH (8): The likelihood of the threat occurring is likely high since the attacker is also highly motivated and capable, vulnerabilities are easily exploitable, but with fewer resources. Probability 80-95%.

MODERATE (5): The likelihood of the threat occurring is moderate. This is because the attacker is motivated and capable, vulnerabilities are exploitable with just moderate effort and resources, 21-79%.

LOW (2): The likelihood of the threat event occurring is low. Maybe because the attacker has limited motivation or capability, and vulnerabilities are difficult to exploit, requiring complex resources. Probability 5-20%.

VERY LOW (0): The likelihood of the threat event occurring is very low or even unlikely to happen. Attacker lacks motivation or capability, vulnerabilities are extremely difficult to exploit, and require highly complex tools/resources. Probability 0-4%.

Generally, the likelihood of an attack/threat event happening is dependent on:

a. Threat source / Attackers' capability and motivation
b. Vulnerability exploitability characteristicsResources needed to carry out the exploitExisting control effectiveness.

5.1. Likelihood Assessment (Table 2)

IT Area	Vulnerability	Threat Source	Identifiable Risks	Level	Description
Access Control	Weak password configuration	External attackers, Insider threats (Untrained staff for password policy)	An unauthorized access via password guessing/brute-force will compromise confidentiality and integrity	VERY HIGH (10)	Financial data is highly valuable, so it will occur.
Access Control	Delayed account deprovisioning from Banner	Terminated employees	A disgruntled former employee can use residual access to steal data or commit fraud.	MODERATE (5)	Chances for exploitation are low, as the employee can be caught within the window.
Change Management	Insufficient approval for changes in updates, tests, and upgrades before launching	Malicious insiders	There could be an unauthorized modification introducing a backdoor access, or even disabling security.	LOW (2)	Requires insider
Backup/Recovery	Untested backup restoration	Hardware failure, Ransomware	Loss of critical data	MODERATE (5)	Hardware failures don't occur regularly. Ransomware attacks are increasing globally.
BYOD Security	Unmanaged device access	Lost/stolen devices without proper MFA containing	A compromised personal device can gain entry to	HIGH (8)	Unmanaged devices lack antivirus, MFA authentication

		critical data, Malware	the Banner network		
BYOD Security	Data leakage via personal devices	Negligent users	Sensitive payroll data can be leaked on an unencrypted / Phished device belonging to a staff member.	HIGH (8)	Device loss is very common. Unencrypted devices expose data.
Network Security	Unclear network segmentation / Poor network security	External attackers	An attacker can gain access to the Banner servers after a phishing compromise.	HIGH (8)	Lack of network segmentation enables unrestricted internal movement High rates of successful phishing
Organization's Device Management	Potential unpatched systems	External attackers	CVE exploitation of an unpatched device / Linux software running the Banner or in the Data center	MODERATE (5)	Public exploits for Linux vulnerabilities are available on exploit databases.
Physical Security	Single administrator authority	Admin unavailability	Having only 1 ITED might lead to a security failure during an emergency when the ITED is unavailable.	VERY LOW (0)	Most times, the ITED is available, and emergencies requiring immediate physical access are rare.

6. RISK IMPACT ANALYSIS

Impact refers to the level of adverse effects that will affect the college's operations, assets, partners, reputation, etc. Following NIST 800-30 Table H-3 below, there is are five-level scale that evaluates the consequences of these impacts across multiple dimensions (e.g., confidentiality, integrity, availability, financial, operational, reputational, regulatory/legal).

NIST 800-30 Impact of Threat Events Table H-3

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

(NIST, 2012)

VERY HIGH (10): The impact may have multiple severe adverse effects on the organization's operations, assets, individuals involved, or the nation. Including: total college failure, loss of critical operations for long periods, major financial loss (€20 million fine, or up 4% annual revenue), severe reputational damage with international attention, criminal investigations, lawsuits, and serious harm to individuals (loss of life). Probability range: 96-100%.

HIGH (8): The impact could have a severe effect on operations, assets, individuals, organizations, or the nation, like: (i) high loss of functional capability for a long duration, making the college unable to perform primary functions; (ii) major damage to college assets; (iii)

major financial loss; or (iv) severe harm to the organization's reputation with national attention. Probability range: 80-95%.

MODERATE (5): The impact could have a moderate adverse effect on some operations, assets, few individuals involved, but can be contained. Meaning: (i) it can lead to reduced operation but still be effective; (ii) visible but moderate damage to college assets; (iii) moderate financial loss, or (iv) notable harm to individuals requiring medical attention but not life-threatening. Probability range: 21-79%.

LOW (2): The impact may have less adverse effect on college operations, assets, and individuals. This effect can: (i) cause low operational capability, but the college is still able to perform primary functions; (ii) cause minor damage to college assets; (iii) cause minor financial loss; or (iv) cause minor harm to individuals. Probability range: 5-20%.

VERY LOW (0): The impact could have a low or zero adverse effect on college operations, college assets, or involved individuals. Effects would be barely noticeable, and may require no fixes, cause no financial loss, and have no impact on individuals. Probability range: 0-4%.

6.1. Impact Severity (Table 3)

Vulnerability	Threat Source	Identifiable Risks	Level	Impact
Weak password configuration	External attackers, Insider threats (Untrained staff for password policy)	An unauthorized access via password guessing/brute-force will compromise confidentiality and integrity	VERY HIGH (10)	- Complete Banner database compromise (20,000+ records, including salary, bank accounts, PII) - Regulatory penalties (4% annual turnover) - National media coverage
Delayed account deprovisioning from Banner	Terminated employees	A disgruntled former employee can use residual access to steal data or commit fraud	HIGH (8)	- A malicious terminated employee could manipulate payroll, creating fraudulent payments - The exploit might affect other employees' records - Theft of the college's intelligence property
Insufficient approval for changes in updates, tests, and upgrades before launching	Malicious insiders	There could be an unauthorized modification introducing a backdoor access, or even	MODERATE (5)	Users with excessive privileges can view/modify records. Moderate financial / asset loss as these users are/were normally in the higher level

		disabling security.		
Untested backup restoration	Hardware failure, Ransomware	Loss of critical data	HIGH (8)	Payroll failure may prevent timely payment for employees, creating legal wage payment obligations under Irish employment law.
Unmanaged device access	Lost/stolen devices without proper MFA containing critical data, Malware	A compromised personal device can gain entry to the Banner network	HIGH (8)	- A lost/stolen unencrypted device of a high-ranking staff member might expose Banner data for recently accessed records. - Investigation and notification cost money
Data leakage via personal devices	Negligent users	Sensitive payroll data can be leaked on an unencrypted / Phished device belonging to a staff member	MODERATE (5)	- Regional media attention - A GDPR breach notification is required for affected individuals
Unclear network segmentation / Poor network security	External attackers	An attacker can gain access to the Banner servers after a phishing compromise.	VERY HIGH (10)	- An attacker gains initial entry via phishing, then moves laterally to Banner servers due to a lack of network segmentation. - Sensitive data is exposed.
Potential unpatched systems	External attackers	CVE exploitation of an unpatched device / Linux software running the Banner or in the Data center	MODERATE (5)	Impact depends on the specific vulnerability (privilege escalation, remote code execution, etc.)
Single administrator authority	Admin unavailability	Having only 1 ITED might lead to a security failure during an emergency when the ITED is unavailable	VERY LOW (0)	- Security guards can override using manual procedures - There is no data breach

7. Risk-level Determination

In this section, we're calculating the overall risk rating identified in our Table 1.

The overall risk level combines (likelihood + impact) using NIST 800-30, TABLE I-2, and Table I-3 risk determination framework.

NIST 800-30 Table I-3: Level of Risk (NIST, 2012)

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

7.1. Risk Overall Ratings (Table 4)

Risk	Identifiable Risks	Likelihood	Impact	Risk Level
Weak password configuration	An unauthorized access via password guessing/brute-force will compromise confidentiality and integrity.	VERY HIGH (10)	VERY HIGH (10)	VERY HIGH (10)
Delayed account deprovisioning from Banner	A disgruntled former employee can use residual access to steal data or commit fraud.	MODERATE (5)	HIGH (8)	HIGH (8)
Insufficient approval for changes in updates, tests, and upgrades	There could be an unauthorized modification introducing a backdoor access, or even disabling security.	LOW (2)	MODERATE (5)	MODERATE (5)

before launching				
Untested backup restoration	Loss of critical data	MODERATE (5)	HIGH (8)	HIGH (8)
Unmanaged BYOD device access	A compromised personal device can gain entry to the Banner network	HIGH (8)	HIGH (8)	VERY HIGH (10)
Data leakage via personal devices	Sensitive payroll data can be leaked on an unencrypted / Phished device belonging to a staff member.	HIGH (8)	MODERATE (5)	HIGH (8)
Unclear network segmentation / Poor network security	An attacker can gain access to the Banner servers after a phishing compromise.	HIGH (8)	VERY HIGH (10)	VERY HIGH (10)
Potential unpatched systems	CVE exploitation of an unpatched device / Linux software running the Banner or in the Data center	MODERATE (5)	MODERATE (5)	MODERATE (5)
Single administrator authority	Having only 1 ITED might lead to a security failure during an emergency when the ITED is unavailable.	VERY LOW (0)	VERY LOW (0)	VERY LOW (0)

8. Control Recommendations

In this step, I'll be recommending some additional actions that are necessary to respond to the risks we've identified in the IT system, which are relevant to the University's operations. I'll also be prioritizing them based on the level (Critical - High Priority), as this will enable the college to take feasible and fast actions based on the risk impacts involved within these risks. Using the ISO/IEC 27001:2013(E). (International Standard ISO/IEC 27001, 2013)

8.1. Critical Priority Recommendations

a. Weak password configuration

- Strengthen Password Security: The college should implement a quality and industry-standard password policy (minimum of 12 characters; or 14+ for privileged accounts; complexity like uppercase, special characters; 60 – 90

days expiration to ensure it's not dormant) ISO/IEC 27001:2013(E): A.9.4.3. (International Standard ISO/IEC 27001, 2013)
    - Effectiveness: this action will reduce the likelihood of brute-force or password attacks.

b. Delayed account deprovisioning from Banner
    - Terminated Employees' access should be revoked and reviewed regularly: The college admins or relevant staff should ensure that an off-boarded employee/staff access to the college facilities is removed immediately they're terminated from the role. ISO/IEC 27001:2013(E): A.9.2.6. (International Standard ISO/IEC 27001, 2013)
    - Effectiveness: This will ensure that a disgruntled employee can't use residual access to steal data or commit fraud.

c. Unclear network segmentation / Poor network security
    - Deploy Network Segmentation / VLANs for critical servers (Banner)
    - Implement firewall rules for security
    - Effectiveness: An attacker can't gain access to the Banner servers after a phishing compromise. ISO/IEC 27001:2013(E): A.13.1.3. (International Standard ISO/IEC 27001, 2013)

d. Unmanaged BYOD device access
    - Implement a Mobile Device Management policy.
    - Deploy an Enterprise Mobile Application Solution (Microsoft Intune, VMware Workspace, etc.)
    - Enforce strict policy for device enrollment on the Mobile Solution. ISO/IEC 27001:2013(E): A.6.2.1. (International Standard ISO/IEC 27001, 2013)
    - Effectiveness: Compromised devices on the network would be identified on time and risks reduced.

8.2. High Priority Recommendations

e. Insufficient approval for changes in updates, tests, and upgrades before launching
    - Ensure management has control at all change levels: The College should enact a policy that will ensure that all IT changes pass through the appropriate advisory board. ISO/IEC 27001:2013(E): A.14.2.2. (International Standard ISO/IEC 27001, 2013)
    - Effectiveness: No unauthorized modification that may introduce backdoor access would occur.

f. Untested backup restoration
    - The college should establish an off-site backup storage that is to be taken and tested regularly, either weekly or bi-weekly. ISO/IEC 27001:2013(E): A.12.3.1. (International Standard ISO/IEC 27001, 2013)
    - Effectiveness: Loss of critical data will be reduced and avoided entirely

If all the above recommended actions are implemented for the colleges' identified Very High – Moderate Risk vulnerabilities and threats, the adverse impacts will be reduced and making the college data protection secure and compliant.

9. Conclusion

This comprehensive risk assessment of Atlantic Technological University's Banner Finance system identified major security control issues that require immediate action. The assessment evaluated 9 risks across access control, change management, backup/recovery, BYOD security, network protection areas, and physical security.

We discovered 3 critical / very high risks that will need urgent action for security and compliance:

- Weak password configuration
- Unmanaged BYOD device access
- Unclear network segmentation / Poor network security

Next, we recommended immediate actions that are necessary to fix this issue and reduce the occurrence of any threat event that may happen as a result of these risks and the other listed ones. Implementing all the above strategies in the assessment will help ATU's security and compliance infrastructure for sustainable growth and ROI.

References

NIST (2012) Guide for Conducting Risk Assessments, National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed: 08 December 2025)

FortifyData: What is a NIST Risk Assessment?. Available at: https://fortifydata.com/blog/what-is-a-nist-risk-assessment/ (Accessed: 08 December 2025)

HighTable (2025) ISO 27001:2022 Clause 4.1 Understanding the Context of the Organisation Explained. Available at: https://hightable.io/iso-27001-clause-4-1-understanding-the-organisation-and-its-context/ (Accessed: 07 December 2025)

Intersoft Consulting (2025) Art. 9 GDPR Processing of special categories of personal data. Available at: https://gdpr-info.eu/art-9-gdpr/ (Accessed: 08 December 2025)

International Standard ISO/IEC 27001 (2013). Available at: iso27001-2013.pdf (Accessed: 09 December 2025)