Contents

Introduction

The purpose of this report is to risk assessment of the existing or possible risks in the current system under inspection. The inspected company is The Atlantic Technological University, which has about 20 thousand students and staff directly involved in teaching, university services and other necessary areas. According to the established policy, the university allows teachers and students to bring their own devices to the campus (‘acceptable-usage-policy.pdf’ n.d.). This policy is called BYOD. During the risk assessment, key persons from various departments of the university were contacted and provided important information on various aspects of the current system security. This assessment focuses on a resource management system called Banner Finance, which is used by the staff of The Atlantic Technological University to perform their daily operational tasks (‘Ellucian Banner: Leading ERP & SIS for Higher Education’ 2024). The system allows you to manage finances, workflows and provides access to grants, fund management, payroll, etc. The scope of this risk study aims to examine this financial software in the context of the university's organization, its departments and operational tasks. Therefore, this system contains a huge amount of Individual Sensitive Information, which contains personally identifiable information known as PII and Sensitive Personal Identifiable Information – SPII (‘What is Personally Identifiable Information (PII)? | IBM’ 2022). This information is extremely important because it contains personal data of people or data that may have a certain value. Such data is a priority target for any attacker because if it is stolen or simply leaked by an unintentional mistake, a company can suffer significant financial or reputational losses, and often both. Due to the high importance of such data, in many countries, including the European Union, it is protected according to certain standards that are unified and provide for certain requirements and criteria that must be met. Organizations and/or software applications that process and store such data as described above must comply with several standards. One of the key ones is the GDPR. This is a European standard called the General Data Protection Regulation, and it includes some of the necessary rules that organizations must follow.

The main principles of this standard include limiting the purposes of data use, accountability, lawfulness, etc. In our case, the university and the software used are also subject to the regulation of this standard, so the risk assessment will also cover this area. Among other standards, it is also worth highlighting PCI DSS, which is used in areas related to financial transactions, in particular, interaction with banking data, such as cards, financial accounts, etc ('PCI_DSS-QRG-v3_2_1.pdf' n.d.).

In the process of risk management, it is worth using one of the most commonly used risk assessment frameworks for this type of task. These include:

1. ISO 31000:2018. This standard can be applied to any project or area, and is particularly relevant to our case study. A visualization of the principles is shown in Figure 1 ('ISO310002018.pdf' n.d.).

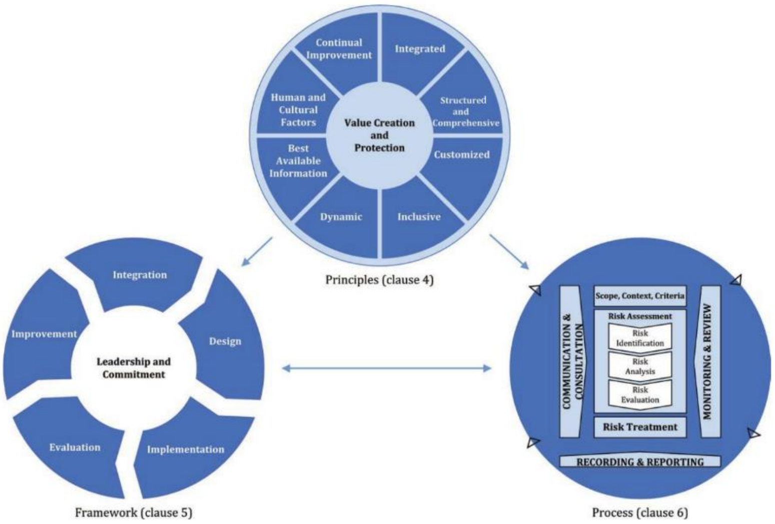


Figure 1 - ISO 31000:2018

2. NIST. This is a well-known framework that is widely used to assess cybersecurity risks. The key steps in this framework are: Identify, Protect, Detect, Respond, and Recover. A visualization of these stages is shown in Figure 2 (National Institute of Standards and Technology 2024).

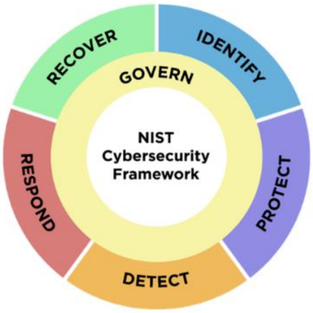


Figure 2 – NIST Framework

3. COBIT. The model consists of 40 key elements related to governance and management. The model is relevant to our case study at the university, but at the same time, it can be slightly more complex because it deals with a more differentiated system. The COBIT visualization is shown in Figure 3 ('Using ITIL and COBIT 2019 integrated I&T framework | Axelos' 2024).The key process in this model that is relevant to our case is APO12 (Manage Risk), which is located at the Align, Plan and Organize stage.

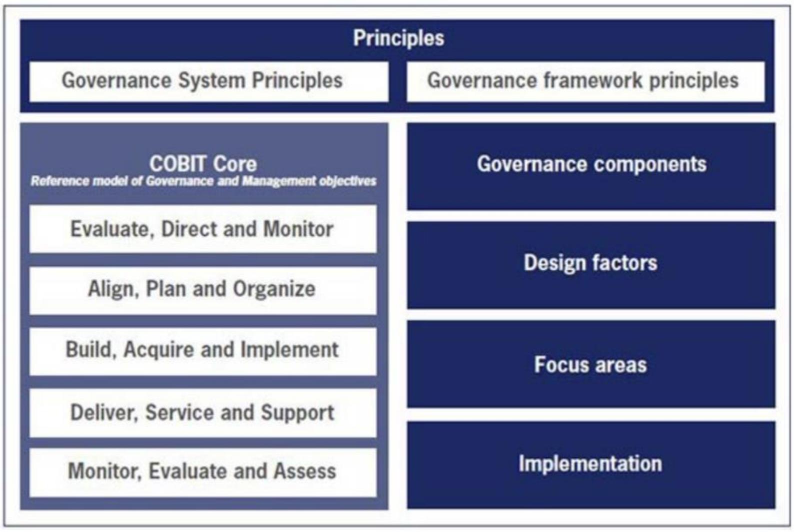

Principles
Governance System Principles
Governance framework principles
COBIT Core
Reference model of Governance and Management objectives
Evaluate, Direct and Monitor
Align, Plan and Organize
Build, Acquire and Implement
Deliver, Service and Support
Monitor, Evaluate and Assess
Governance components
Design factors
Focus areas
Implementation

Figure 3 – Principles of the COBIT model.

4. OCTAVE. This framework focuses on critical assets, which can include the financial system considered in this case study. It is people-oriented, involving key stakeholders in the risk assessment, in our case the IT Executive Director (ITED), Banner Security Administrator (BSA), and Systems Administrator (SA). The framework contains several main phases, the OCTAVE visualization is shown in Figure 4 (‘Formal Risk Analysis Structures: OCTAVE and FAIR > Securing IoT | Cisco Press’ 2024).

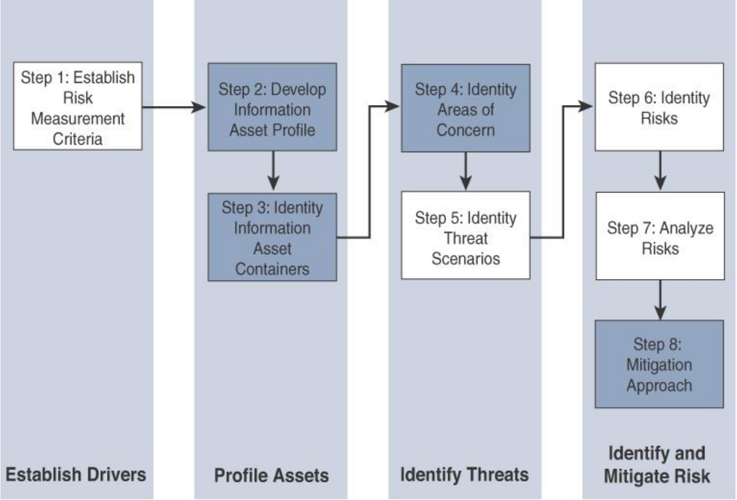

Step 1: Establish Risk Measurement Criteria
Step 2: Develop Information Asset Profile
Step 3: Identity Information Asset Containers
Step 4: Identity Areas of Concern
Step 5: Identity Threat Scenarios
Step 6: Identity Risks
Step 7: Analyze Risks
Step 8: Mitigation Approach
Establish Drivers
Profile Assets
Identify Threats
Identify and Mitigate Risk

Figure 4 – The OCTAVE model.

In summary, the goal is to assess the risks of the Banner system in interaction with other related areas of the university, and it is also important to inspect the risks associated with regulations at the state level. It is also necessary to investigate what theoretical risks may arise in terms of current policies and procedures in place at the university. One of the frameworks presented above can be used in the risk assessment, as they are relevant to the case of the university under consideration, it will be most appropriate to use NIST to identify and assess risks.

IT system characterization

As noted earlier, the focus of the risk assessment is on the Banner Finance system and its organizational context. A visualization of the Banner Finance system is shown in Figure 1. (‘banner-overview-brochure.pdf’ n.d.). The Banner system runs on Red Hat Enterprise Linux and is accessible to employees from the finance, HR, accounting and IT departments.

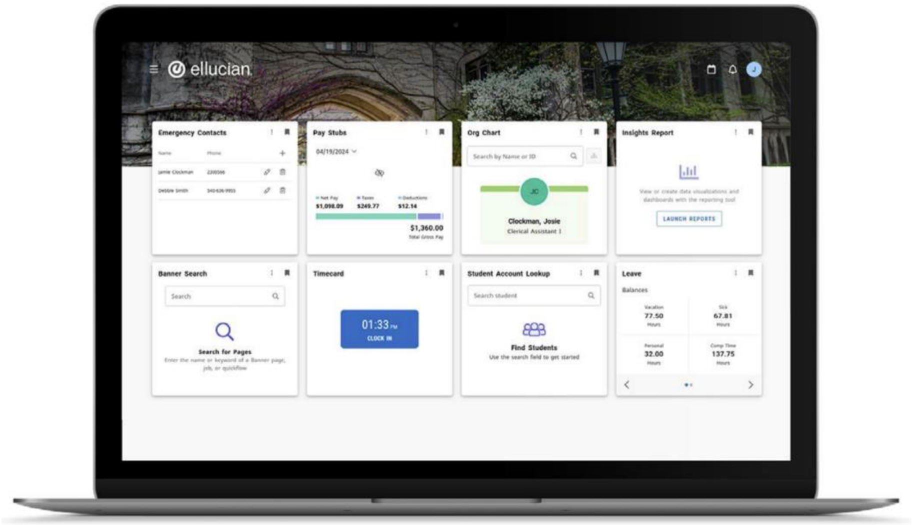
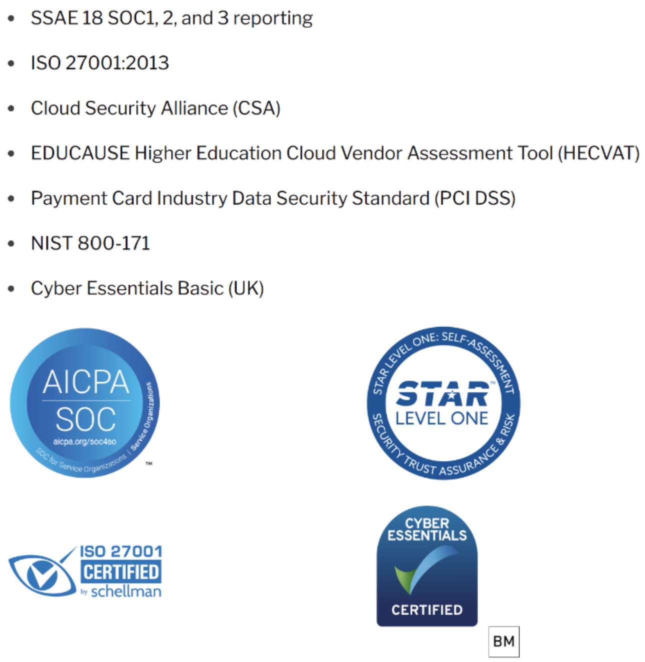


Figure 5 - Banner Finance

When checking the software itself, it was found that the developer claims to be quite compliant with the required standards. In particular, the software is aligned with ISO 27001:2013, NIST 800-171, PCI DSS and others (‘Cloud Security at Ellucian’ 2024).



- SSAE 18 SOC1, 2, and 3 reporting
- ISO 27001:2013
- Cloud Security Alliance (CSA)
- EDUCAUSE Higher Education Cloud Vendor Assessment Tool (HECVAT)
- Payment Card Industry Data Security Standard (PCI DSS)
- NIST 800-171
- Cyber Essentials Basic (UK)

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
STAR LEVEL ONE: SELF-ASSESSMENT
STAR
LEVEL ONE
SECURITY TRUST ASSURANCE & RISK
ISO 27001
CERTIFIED
by schellman
CYBER ESSENTIALS
CERTIFIED
BM

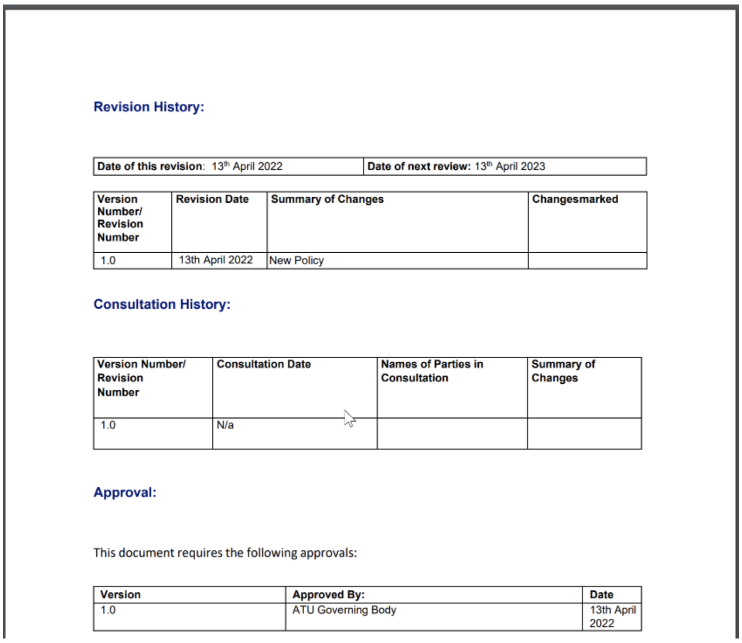
Figure 6 - Banner compliance

The system operates in the university data center, all backups are made daily but are stored only on local storage, without duplication to the cloud. Since all data is stored locally at the university, the physical security of the data center is especially critical. At the time of the assessment, several access control processes exist, including:

- Biometric devices are used and only authorized personnel have access to them.
- Monitoring by cameras.
- There is a visitor log.

Risk Assessment. NIST

According to the first step of the NIST framework, the risk assessment and identification were conducted. The risk assessment included information gathered through interviews with employees, posted university policies, and software documentation. The university provides an opportunity for staff and students to bring their own devices, as noted during the interview, they should be subject to the BYOD policy. During the inspection of the current documentation on the university website, it was found that the 2022 version was posted, which, according to the documents, was to be revised in 2023 (‘acceptable-usage-policy.pdf’ n.d.).



Revision History:

Date of this revision: 13th April 2022	**Date of next review:** 13th April 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changesmarked
1.0	13th April 2022	New Policy	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	N/a		

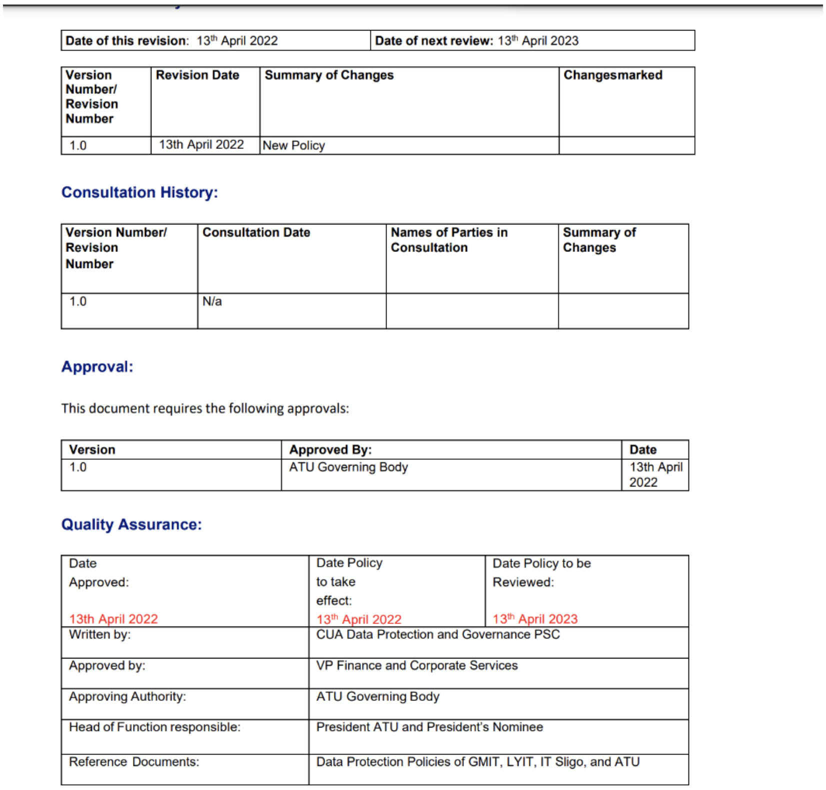
Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	ATU Governing Body	13th April 2022

Figure 7 - The Acceptable Usage Policy

According to the quality assurance, the policy was due for review on 13 April 2023. As of the time of the inspection, the website contained all the versions that were approved in 2022, so they were almost 3 years old. It is not known whether the Banner system was in use when these policies were approved, but all documents show signs of not being up-to-date. Therefore, new versions of the documents were either not posted on the website or have not been reviewed since their approval, which violated the regulations of the document quality assurance section (‘data-protection-policy.pdf’ n.d.).



Date of this revision: 13th April 2022	Date of next review: 13th April 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changesmarked
1.0	13th April 2022	New Policy	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	N/a		

Approval:

This document requires the following approvals:

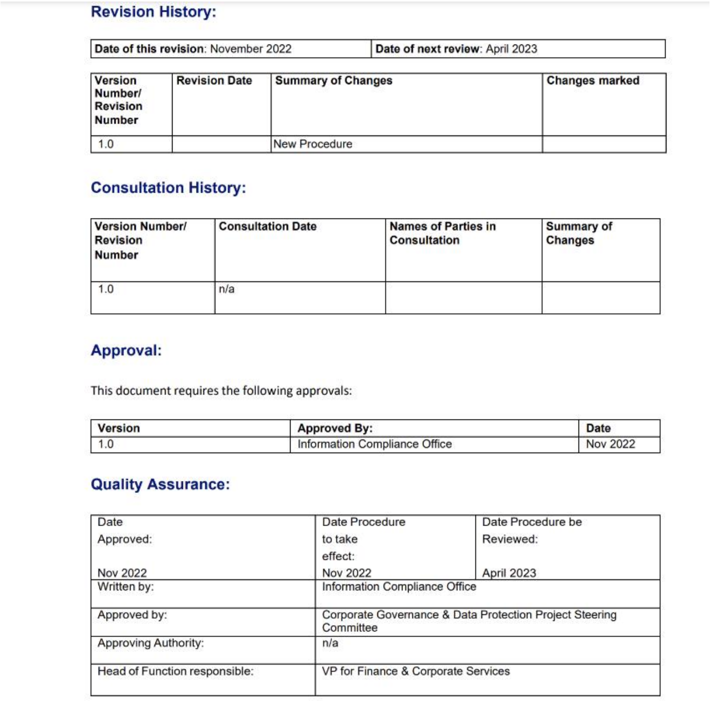
Version	Approved By:	Date
1.0	ATU Governing Body	13th April 2022

Quality Assurance:

Date Approved: 13th April 2022	Date Policy to take effect: 13th April 2022	Date Policy to be Reviewed: 13th April 2023
Written by:	CUA Data Protection and Governance PSC	
Approved by:	VP Finance and Corporate Services	
Approving Authority:	ATU Governing Body	
Head of Function responsible:	President ATU and President's Nominee	
Reference Documents:	Data Protection Policies of GMIT, LYIT, IT Sligo, and ATU	

Figure 8 - The Data Protection Policy

The Data Subject Rights Procedure document has a similar status, shown in Figure 9 ('data-subject-rights-procedure.pdf' n.d.).



Revision History:

Date of this revision: November 2022	Date of next review: April 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changes marked
1.0		New Procedure	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	n/a		

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	Information Compliance Office	Nov 2022

Quality Assurance:

Date Approved: Nov 2022	Date Procedure to take effect: Nov 2022	Date Procedure be Reviewed: April 2023
Written by:	Information Compliance Office	
Approved by:	Corporate Governance & Data Protection Project Steering Committee	
Approving Authority:	n/a	
Head of Function responsible:	VP for Finance & Corporate Services	

Figure 9 - Data Subject Rights Procedure

The interviews also revealed that the policy on setting and using passwords does not comply with best practices. These practices include: using passphrases, not using simple words and their combinations, using separate passwords for each resource, etc (‘Create and use strong passwords - Microsoft Support’ 2024).

It was found that access to the Banner system has several problems, specifically:

- Access to the system is not removed in time for those users who have already stopped working with it for one reason or another.
- No records of user access are kept.

It is important to emphasize that the system backup is stored only at the university, which is a potential problem in many cases. The interviews also indicated that in the event of changes or modifications to the Banner software, the final implementation is not approved by management.

Risk Identification and Analysis

Based on the problems described, current risks that could lead to further issues at the university were identified. The risks and their evaluation are presented in Table 1.

Risk number	Risk description	Impact on CIA	Likelihood	Impact	Risk level
1	Weak password policies	Confidentiality, Integrity	Hight	Hight	Hight
2	Delayed user deprovisioning from Banner	Confidentiality	Hight	Hight	Hight
3	Lack of documentation for access reviews	Integrity	Moderate	Moderate	Moderate
4	Lack of backup copies of the Banner system outside the campus	Availability	Hight	Hight	Hight
5	Unapproved changes to the software	Integrity, Availability	Moderate	Hight	Hight
6	BYOD devices are increasing the number of cyber threats	Availability, Confidentiality	Hight	Hight	Hight
7	The policy documentation has not been updated	Availability	Hight	Hight	Hight

Table 1 - Identified risks

In order to mitigate the consequences and reduce the likelihood of threats associated with the risks listed in Table 1, it is recommended to apply the following risk control actions, which are listed in Table 2.

Risk number	Risk description	Control strategy	Control description	NIST Function
1	Weak password policies	Mitigation	Implement best-practice requirements for passwords and set password expiry dates. Establish multi-factor authentication.	Protect
2	Delayed user deprovisioning from Banner	Mitigation	Automate the process of providing access to user accounts, and additionally implement periodic (quarterly or every 3 months) checks of all current accounts in case of an error.	Protect
3	Lack of documentation for access reviews	Mitigation	Create and maintain a register of user access, according to the automation created in the previous point. This register should be kept for at least 1 year. The register should be backed up in the cloud.	Protect
4	Lack of backup copies of the Banner system outside the campus	Mitigation	Create securely protected (encrypted, restricted access) backups in the cloud, outside the university. Create a log of cloud backups and a log of access to these backups.	Recover
5	Unapproved changes to the software	Mitigation	Implement mandatory approval of new software releases by a responsible person (or persons) after changes have been made to the previous release.	Protect
6	BYOD devices are increasing the number of cyber threats	Mitigation	It is recommended to separate networks into topology levels used for training and those where the Banner is used and PII and SPII are stored. It is recommended to use different network VLANs, configure access control lists, and, if possible, physically separate these networks.	Protect
7	The policy documentation has not been updated	Mitigation	It is recommended to update the current policy documents posted on the website. Conduct an	Protect

			inspection of their relevance, add new points and corrections if necessary. Identify the responsible person or department and the date of the next review.	

Table 2 – Control actions

Conclusions and recommendations

As a result of the risk assessment, a number of risks were identified that could lead to potential reputational and financial losses for the university. Among the risks with a high priority, it is worth highlighting risk number 4 (Lack of backup copies of the Banner system outside the campus) - in case of loss of the only available backup on the university campus, this could lead to large financial losses, as the backup contains important financial information. Risk number 2 is also highlighted - the current situation with access to the Banner system may allow employees who have quit but continue to have access to the system to operate with financial information. Risk number 7 is also important - as these are publicly stated official university policies that are outdated, this could lead to potentially severe fines if the university is audited for compliance with GDPR and other regulations.

Therefore, the risk control actions listed in Table 2 should be primarily applied to risks 4, 2 and 7. Secondly, to risks 1 and 6, and then 3 and 5. If possible, all control actions should be applied as soon as possible.

References

‘acceptable-usage-policy.pdf’ (n.d.) available: https://www.atu.ie/app/uploads/2024/11/acceptable-usage-policy.pdf [accessed 7 Dec 2024].

‘banner-overview-brochure.pdf’ (n.d.) available: https://www.ellucian.com/assets/en/brochure/banner-overview-brochure.pdf [accessed 5 Dec 2024].

Cloud Security at Ellucian [online] (2024) available: https://www.ellucian.com/security [accessed 7 Dec 2024].

Create and Use Strong Passwords - Microsoft Support [online] (2024) available: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb [accessed 8 Dec 2024].

‘data-protection-policy.pdf’ (n.d.) available: https://www.atu.ie/app/uploads/2024/10/data-protection-policy.pdf [accessed 8 Dec 2024].

‘data-subject-rights-procedure.pdf’ (n.d.) available: https://www.atu.ie/app/uploads/2024/11/data-subject-rights-procedure.pdf [accessed 8 Dec 2024].

Ellucian Banner: Leading ERP & SIS for Higher Education [online] (2024) available: https://www.ellucian.com/solutions/ellucian-banner [accessed 5 Dec 2024].

Formal Risk Analysis Structures: OCTAVE and FAIR > Securing IoT | Cisco Press [online] (2024) available: https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4 [accessed 7 Dec 2024].

‘ISO310002018.pdf’ (n.d.) available: https://governance.ie/uploads/files/Internal%20Control/ISO310002018.pdf [accessed 7 Dec 2024].

National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, available: https://doi.org/10.6028/NIST.CSWP.29.

‘PCI_DSS-QRG-v3_2_1.pdf’ (n.d.) available: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf [accessed 7 Dec 2024].

Using ITIL and COBIT 2019 Integrated I&T Framework | Axelos [online] (2024) available: https://www.axelos.com/resource-hub/white-paper/using-itil-cobit-2019-create-integrated-environment [accessed 7 Dec 2024].

What Is Personally Identifiable Information (PII)? | IBM [online] (2022) available: https://www.ibm.com/topics/pii [accessed 5 Dec 2024].