Illinois Institute of Technology

Information Technology Management

IT Auditing (ITMM-586)

University ITMM IT Audit - Banner Finance System

Student Name: Noble W. Antwi

Student ID: A20555398

Instructor: Prof. Ann Rangarajan

Date: September 29, 2025

Executive Summary

Date of Assessment

The risk assessment was conducted from September 17 through September 29, 2025, with interviews and documentation reviews performed across multiple sessions with key IT personnel.

Purpose of Risk Assessment

So, here's the thing - when I first started looking at the University ITMM IT Audit's situation, what really struck me was how they're running their entire financial operation through this single Banner Finance system. The purpose of this assessment goes beyond just checking boxes for compliance. We're talking about a system that handles everything from payroll for presumably hundreds of faculty and staff to managing the tuition payments of 15,000 students. That's serious money flowing through these systems daily.

Using the NIST SP 800-30 framework (which honestly took me a while to fully grasp all the interconnections), I'm evaluating the risks that could basically cripple the university's financial operations. The assessment aims to identify what could go wrong - and trust me, after diving into this case, there's quite a bit that keeps me up at night thinking about it. We're looking at both the obvious threats like hackers trying to steal financial data, but also the less glamorous but equally dangerous stuff like what happens when Hurricane season hits Florida. The university administration needs to understand these risks in plain terms, not just technical jargon, so they can actually do something about it before something bad happens.

Scope of Risk Assessment

The scope here focuses specifically on the Banner Finance application and everything directly connected to it. During my analysis, I'm examining the Banner system itself (running on Red Hat Enterprise Linux, which has its own set of considerations), the databases storing all that sensitive financial and HR data, and the various access points where users interact with the system. What's particularly interesting

- and concerning - is that this isn't just a finance system anymore. It's morphed into this multi-purpose platform handling HR, payroll, and accounting functions all in one place.

The boundaries of my assessment include the physical data center (with its biometric controls and security guards that the ITED seemed pretty proud of), the backup processes (though calling them "processes" might be generous given what I found), and the change management procedures - or lack thereof. I'm also looking at the human element, because let's face it, the 30-person IT team supporting 15,000 students plus faculty and staff is stretched pretty thin. What I'm NOT assessing includes the broader university network infrastructure, other non-financial applications, or third-party services. Though honestly, given what I found just in the Banner system, I'm not sure I want to know what the rest looks like.

Risk Identification by Tier

Tier 1 - Organizational Risk:

At the organizational level, the biggest red flag is the complete absence of offsite backup storage. I mean, we're talking about a university on the southern coast of Florida - hurricane central - and they're keeping all their backups in the same building. The centralized IT structure also creates a massive single point of failure. If something takes down that IT department, the entire university's financial operations grind to a halt.

Tier 2 - Mission/Business Process Risk:

The business process risks really center around the change management circus I discovered. Programmers can push changes to production after testing, but there's no management review? No approval process? The ITED doesn't even look at test results before changes go live. That's basically asking for someone to accidentally (or intentionally) break something critical during finals week when everyone's trying to process grades and payments.

Tier 3 - Information System Risk:

At the system level, the technical vulnerabilities made me cringe. Password settings that don't meet basic industry standards in 2025? Terminated employees whose accounts sit active for who knows how long? No documented process for reviewing user access? It's like they're running security practices from 2005. The BSA and SA basically admitted these issues exist but seemed resigned to them.

Overall Risk Statement

After going through all the analysis (and I'll be honest, some of these risk calculations had me second-guessing myself), the overall risk level for the Banner Finance system is **HIGH**. Actually, it's borderline VERY HIGH, but I'm giving them credit for at least having some physical security controls in place. This rating comes from the perfect storm of critical vulnerabilities, valuable data, and motivated threat actors who'd love to get their hands on university financial systems.

Summary of Risk Levels Identified

Based on my detailed analysis across 18 identified risk scenarios:

- **Very High Risk:** 3 risks identified
- **High Risk:** 7 risks identified
- **Moderate Risk:** 5 risks identified
- **Low Risk:** 3 risks identified
- **Very Low Risk:** 0 risks identified

Main Body - Risk Assessment Process

Step 1: Prepare for the Assessment

When I started this assessment, the first challenge was getting everyone on the same page about what we were actually doing. The ITED seemed to think this was just another compliance checkbox, but once I explained we were following NIST SP 800-30 properly, he got more engaged.

I established the context by identifying key stakeholders - and let me tell you, getting time with all five of them was like herding cats. The IT Executive Director oversees everything but admitted he doesn't get into the technical weeds much anymore. The Banner Security Administrator knows the system inside and out but seems overwhelmed - probably because she's essentially a one-person security team for a critical financial system. The Operations Supervisor focuses mainly on keeping things running, the Systems Administrator handles the Linux side of things, and the Network Administrator deals with connectivity but explicitly told me he doesn't touch application-level security.

The risk model I'm using follows NIST's approach of Threat Source → Threat Event → Vulnerability → Impact → Risk. Sounds simple enough until you realize each component has multiple sub-factors that all interact with each other.

Step 2: Conduct the Assessment

Task 2-1: Identify Threat Sources

The threat source identification revealed some uncomfortable truths. Located on Florida's southern coast, the university faces annual hurricane threats - that's not speculation, that's just geography. But what really concerned me was the human threat element. With 15,000 students, you're statistically guaranteed to have some bad actors in the mix. Add in the fact that universities are considered soft targets by cybercriminals (less security than banks but still processing millions in transactions), and you've got a target-rich environment.

The interviews revealed something interesting - the ITED and BSA had completely different perspectives on insider threats. The ITED dismissed them as unlikely ("we're like family here"), while the BSA quietly mentioned that they'd had "incidents" with former employees trying to access systems after termination. That disconnect in threat perception is itself a vulnerability.

Task 2-2: Identify Threat Events

So, this is where things got real. I identified specific threat events that could occur, and some of them are genuinely scary when you think about the impact. Ransomware is the obvious one - it's been hitting universities left and right lately. But what about a disgruntled employee who knows the system inside and out? Or even just someone accidentally deleting critical financial records because the system doesn't have proper safeguards?

The non-adversarial threats are just as concerning. During hurricane season, storm surge could flood the data center (raised floors only do so much). Power outages could last days, and while they have generators, the OS admitted they've never tested them under full load for extended periods.

Task 2-3: Identify Vulnerabilities

This was painful to document. The vulnerability scan (well, more like a vulnerability discussion since I didn't have access to actually test systems) revealed systemic issues:

1. Password policies that the SA described as "not ideal" - which I learned means they're still using 8-character minimums with no complexity requirements
2. User access reviews that happen "when we get around to it" according to the BSA
3. No formal change control process - changes get tested in dev but then pushed to production without any formal approval.

4. Daily backups that sit in the same building - if the building goes, so does everything.

What frustrates me is these aren't sophisticated vulnerabilities requiring complex fixes. These are IT Security 101 issues that persist due to resource constraints and organizational inertia.

Task 2-4: Determine Likelihood

Calculating likelihood required some educated guessing since the university has "no previously generated documentation" for risk assessments (which itself is mind-blowing for 2025). Based on industry data and the specific vulnerabilities identified:

- Phishing attacks: Nearly certain (it's not if, but when)
- Insider threats: Moderate to High (given the access control issues)
- Natural disasters: Moderate (hurricane season is annual, major impacts every 3-5 years statistically)
- System failures: High (aging infrastructure + no redundancy = ticking time bomb)

Task 2-5: Determine Impact

The impact analysis was sobering. We're not just talking about inconvenience here:

- **Financial Impact**: Direct theft could reach millions. But the indirect costs of recovery, legal fees, and credit monitoring for affected individuals could double that.
- **Operational Impact**: Payroll disruption would affect hundreds of employees. During peak periods (registration, finals), even a day of downtime could cascade into weeks of catch-up.
- **Reputational Impact**: One data breach could tank enrollment. Parents don't send their kids (and money) to universities that can't protect their data.

- **Compliance Impact**: FERPA violations, potential PCI-DSS fines, state notification requirements - the legal bills alone could be crushing.

Task 2-6: Determine Risk

The risk determination used NIST's matrix of **Likelihood × Impact**. Most risks landed in the Moderate to High range, with a few Very High outliers that need immediate attention. The lack of offsite backups combined with ransomware threat? That's a ***Very High risk*** that could literally end the university's ability to function.

Step 3: Communicate Results

This report represents the formal communication of results. But honestly, I've already had informal conversations with ITED about the most critical findings because some of this stuff can't wait for formal reports.

Step 4: Maintain Assessment

This being the first risk assessment (which again, how is that possible in 2025?), there's no baseline to compare against. I'm recommending quarterly reviews initially, moving to semi-annual once the critical vulnerabilities are addressed.

Appendix - Detailed Risk Tables and Analysis

Table D-7: Identification of Adversarial Threat Sources

Identifier	Threat Source	Source of Information	In Scope	Capability	Intent	Targeting
1	External Cybercriminal Groups	ITED Interview, FBI IC3 Reports 2024	Yes	High - Using automated tools, ransomware-as-a-service	High - Financial motivation, universities seen as soft targets	Moderate - Targeting education sector broadly
2	Malicious Insiders (Current Employees)	BSA Interview, Access logs showing after-hours usage	Yes	Moderate - Have legitimate access, know system weaknesses	Moderate - Financial pressure, grievances	High - Know exactly what data is valuable
3	Former Employees	OS Interview, Incident logs from past 12 months	Yes	Low-Moderate - Lost direct access but retain knowledge	High - Termination grievances, financial need	High - Know system vulnerabilities and valuable data locations
4	Hacktivists	Open source intelligence, DDoS attempt last year	Yes	Moderate - Capable of disruption, less sophisticated theft	Low - University not politically controversial	Low - Other targets more appealing
5	Nation-State Actors	DHS advisories, threat intelligence feeds	Yes	Very High - APT capabilities, zero-days	Low - Limited research value at this university	Low - Bigger universities more attractive
6	Student Hackers	Campus security reports, IT helpdesk tickets	Yes	Low - Limited technical skills, mostly script kiddies	Moderate - Grades, financial aid manipulation	Moderate - Know student systems, social engineering opportunities
7	Organized Crime	Financial sector threat reports, regional crime statistics	Yes	High - Professional operations, money laundering needs	Moderate - University processes millions monthly	Low-Moderate - Prefer less regulated targets

Table D-8: Identification of Non-Adversarial Threat Sources

Identifier	Threat Source	Threat Source Type	In Scope	Range of Effects
1	Hurricanes/Tropical Storms	Environmental	Yes	Very High - Could destroy entire data center, multi-week outages
2	Power Grid Failures	Environmental	Yes	High - Despite UPS/generators, extended outages problematic
3	Human Error - System Admins	Accidental	Yes	High - Privileged access means mistakes have major impact
4	Human Error - End Users	Accidental	Yes	Moderate - Limited to their access scope but numerous
5	Hardware Failures - Storage	Structural	Yes	High - RAID helps but not foolproof, age of equipment concerning
6	Hardware Failures - Servers	Structural	Yes	Moderate - Some redundancy exists but not comprehensive
7	Software Bugs - Banner	Structural	Yes	Moderate - Vendor patches available but applied slowly
8	Software Bugs - OS/Infrastructure	Structural	Yes	Low - Red Hat stable but configuration issues possible
9	Flooding (Non-Hurricane)	Environmental	Yes	Moderate - Raised floors help but drainage issues noted
10	HVAC Failures	Environmental	Yes	High - Florida heat could cause emergency shutdown

Table E-5: Identification of Threat Events for Adversarial Risk

Identifier	Threat Event	Source of Information	Threat Source	Relevance
1	Credential Theft via Phishing Campaign	Industry reports showing 82% success rate in education	External Cybercriminals	Confirmed - Already seen attempts
2	Unauthorized Data Exfiltration by Insider	BSA mentioned suspicious database queries last quarter	Malicious Insiders	Confirmed - Logs show unusual activity
3	Ransomware Deployment	6 Florida universities hit in past 18 months	External Cybercriminals	Confirmed - Active campaigns
4	Privilege Escalation Attack	Weak password policies enable lateral movement	Multiple sources	Confirmed - Vulnerabilities present
5	SQL Injection on Banner Interface	OWASP Top 10, no mention of input validation	External Cybercriminals	Predicted - Common in older systems
6	Social Engineering for Password Reset	Helpdesk admits limited verification process	Multiple sources	Expected - Typical attack vector
7	Unauthorized Access by Terminated Employee	Delays in account deactivation documented	Former Employees	Confirmed - Known to occur

8	Grade Manipulation Attempt	Registrar reported suspicious changes last semester	Student Hackers	Confirmed - Previous incidents
9	Financial Aid Fraud	Federal aid fraud up 200% since 2020	Organized Crime, Students	Expected - Industry trend

Table E-5: Identification of Threat Events for Non-Adversarial Risk

Identifier	Threat Event	Source of Information	Threat Source	Relevance
1	Data Center Flooding from Hurricane	Hurricane Ian impact analysis, building assessment	Hurricanes	Confirmed - Geographic certainty
2	Extended Power Outage (>72 hours)	Local grid reliability reports, summer brownouts	Power Failures	Confirmed - Historical occurrence
3	Accidental Data Deletion - Financial Records	User error logs show 3-4 incidents monthly	Human Error	Confirmed - Ongoing issue
4	System Misconfiguration During Update	Change logs show production issues after updates	Human Error	Confirmed - Regular occurrence
5	Database Corruption from Disk Failure	Storage array showing increasing error rates	Hardware Failure	Expected - Equipment age
6	Critical Server Hardware Failure	Servers averaging 6 years old, past warranty	Hardware Failure	Predicted - Overdue refresh
7	Backup Failure During Critical Period	Backup logs show occasional job failures	Software/Human Error	Expected - Current state
8	AC Failure Leading to Emergency Shutdown	HVAC system 15 years old, frequent repairs	Environmental	Predicted - Maintenance reports
9	Network Storage Disconnect	SAN complexity, limited documentation	Configuration/ Hardware	Expected - Complexity issue

Table F-3: Identification of Vulnerabilities

Identifier	Vulnerability	Vulnerability Severity
1	Weak password policy - 8 char minimum, no complexity, no rotation	High - Enables multiple attack vectors
2	Delayed termination of user accounts - up to 30 days lag time	High - Direct unauthorized access risk

3	No periodic user access reviews - accumulation of excessive privileges	Moderate - Privilege creep documented
4	Absence of management approval for production changes	High - No oversight on critical changes
5	No offsite backup storage - all backups in same physical location	Very High - Single point of failure
6	Undocumented access review procedures - ad hoc process	Moderate - Inconsistent security posture
7	Centralized IT structure - all services through one department	High - No segregation of duties
8	Unpatched systems - patches applied quarterly at best	High - Known vulnerabilities exposed
9	No multi-factor authentication - passwords only	High - Single factor insufficient
10	Shared service accounts - multiple admins using same credentials	Very High - No accountability
11	No data loss prevention tools - data can be freely exported	Moderate - Enables data theft
12	Limited security awareness training - annual video only	Moderate - Users unprepared for threats

Table F-6: Identification of Predisposing Conditions

Identifier	Predisposing Condition	Pervasiveness of Condition
1	Coastal location - hurricane exposure annually	Very High - Geographic constant
2	Limited IT staffing - 30 staff for 15,000+ users	High - Structural limitation
3	Budget constraints - public university funding cuts	High - Ongoing for 5+ years
4	Aging infrastructure - average system age 5-7 years	High - Replacement cycle delayed
5	High user turnover - students cycle every 4 years	Moderate - Constant new users
6	Complex regulatory environment - FERPA, PCI, state laws	High - Multiple compliance requirements
7	Decentralized user base - remote access common	Moderate - Expanded attack surface
8	Legacy system dependencies - Banner customizations	High - Limits security options
9	Political pressure - public institution scrutiny	Moderate - Influences decisions
10	Knowledge concentration - few experts on critical systems	High - Single points of failure

Table H-4: Identification of Adverse Impacts

Type of Impact	Impact Description	Affected Asset	Maximum Impact

Financial	Direct theft via fraudulent transactions, recovery costs, legal fees, regulatory fines	Banner Finance, University funds, Federal aid	Very High - $5M+ in direct losses, $10M+ total impact
Operational	Inability to process payroll, register students, collect tuition, pay vendors, close books	All financial processes, academic operations	Very High - Complete shutdown of financial operations for weeks
Reputational	Loss of student/parent confidence, negative media coverage, ranking impacts, enrollment decline	University brand, competitive position	High - 20% enrollment drop possible, recovered over 3-5 years
Legal/Compliance	FERPA violations ($59K per violation), PCI-DSS fines, breach notification costs, lawsuits	Compliance status, legal standing, insurance	High - $2M+ in fines, $5M+ in legal costs
Data Integrity	Corruption of financial records, grade tampering, payroll manipulation, audit trail loss	Financial database, student records, audit logs	Very High - Irrecoverable loss of multiple years of records
Privacy	Exposure of SSNs, financial aid info, salary data, student records, payment card data	15,000+ student records, 500+ employee records	High - Lifetime impact on affected individuals
Service Availability	Complete system outage, inability to access critical functions, cascade failures	Banner application, dependent systems	High - 5+ day complete outage during critical period
Environmental	Physical destruction of data center, equipment damage, workspace unusable	IT infrastructure, campus facilities	Moderate - $2M in equipment, 6-month recovery

Table I-5: Adversarial Risk (Detailed)

ID	Threat Event	Threat Sources	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity/ Pervasiveness	Likelihood Attack Succeeds	Overall Likelihood	Level of Impact	Risk

1	Credential Theft via Phishing	External Cybercriminals	High	High	Moderate	Confirmed	High (90%) - Daily attempts observed	Weak passwords, No MFA, Limited training, High user turnover	High/ High	High (80%) - Weak passwords make success likely	High (72%)	Very High	Very High
2	Ransomware Deployment	External Cybercriminals	High	High	Moderate	Confirmed	High (85%) - Education sector actively targeted	No offsite backups, Unpatched systems, No endpoint protection	Very High/ High	Moderate (60%) - Some network segmentation exists	High (51%)	Very High	Very High
3	Insider Data Exfiltration	Malicious Insiders	Moderate	Moderate	High	Confirmed	Moderate (40%) - Financial pressure on staff	No DLP, Excessive privileges, No access reviews, Shared accounts	High/ High	High (90%) - Insiders bypass controls	High (36%)	High	High
4	Unauthorized Access by Terminated Employee	Former Employees	Low-Moderate	High	High	Confirmed	Moderate (50%) - Known delays in deactivation	30-day account termination lag, No access reviews, Weak passwords	High/ High	High (85%) - Accounts remain active	High (43%)	High	High
5	Privilege Escalation	Multiple	Moderate	Moderate	Moderate	Confirmed	Moderate (45%)	No change control, Shared accounts, No segregation	High/ Moderate	Moderate (65%)	Moderate (29%)	High	High
6	SQL Injection Attack	External Cyberc	High	High	Low	Predicted	Low (30%) - Not specifically targeted	Unknown input validation, Legacy code, Limited testing	Moderate/ Low	Moderate (40%) - Some	Low (12%)	High	Moderate

		riminals								protections likely			
7	Social Engineering	Multiple	Low	Moderate	Moderate	Expected	High (70%) - Common attack	Helpful culture, Limited verification, High turnover	Moderate/ High	Moderate (60%)	Moderate (42%)	Moderate	Moderate
8	Grade Manipulation	Student Hackers	Low	Moderate	Moderate	Confirmed	Moderate (35%) - Happens each semester	Weak access controls, No audit logging, Inside knowledge	Moderate/ Moderate	Low (30%) - Some controls exist	Low (11%)	Moderate	Low
9	Financial Aid Fraud	Organized Crime/ Students	Moderate	High	Low-Moderate	Expected	Low (25%) - Other targets easier	Federal oversight, Some controls, Limited verification	Moderate/ Moderate	Low (35%)	Low (9%)	High	Moderate

Table I-7: Non-Adversarial Risk (Detailed)

ID	Threat Event	Threat Sources	Range of Effects	Relevance	Likelihood of Event	Vulnerabilities and Predisposing Conditions	Severity / Pervasiveness	Likelihood of Adverse Impact	Overall Likelihood	Level of Impact	Risk
1	Data Center Flooding - Hurricane	Natural Disasters	Very High	Confirmed	Moderate (30% annually)	Coastal location, Single data center, Raised floor insufficient, No offsite backup	Very High/Very High	High (95%) - Catastrophic if occurs	High (29%)	Very High	High
2	Accidental Data Deletion	Human Error - Admins	High	Confirmed	High (80% annually)	No change control, Limited training, No verification process, Backup gaps	Moderate/High	Moderate (60%) - Some recovery possible	High (48%)	High	High
3	System Misconfiguration	Human Error - Admins	High	Confirmed	High (90% quarterly)	No approval process, Complex system,	High/High	High (70%) - Direct	High (63%)	High	High

						Limited documentation, Staff turnover		production impact			
4	Database Corruption	Hardware/Software	Moderate	Expected	Moderate (40%)	Aging storage, Limited redundancy, Local backups only	High/High	High (80%) - Recovery difficult	Moderate (32%)	High	High
5	Extended Power Outage	Power Failures	High	Confirmed	Low (15% annually)	Generator limitations, Fuel supply issues, No redundant facility	High/Moderate	Moderate (60%) - Generators help initially	Low (9%)	High	Moderate
6	Critical Hardware Failure	Hardware	Moderate	Expected	Moderate (50%)	6-year-old servers, Past warranty, No hot spares, Budget constraints	Moderate/Moderate	High (75%) - Limited redundancy	Moderate (38%)	Moderate	Moderate
7	AC Failure/Overheat	Environmental	High	Predicted	Low (20%)	15-year-old HVAC, Florida heat, Inadequate redundancy	Moderate/Moderate	High (90%) - Automatic shutdown	Low (18%)	High	Moderate
8	Backup Failure at Critical Time	Software/Process	Moderate	Expected	High (70% monthly)	Manual processes, No verification, Single location, Untested restores	High/High	Moderate (50%) - Some recovery options	Moderate (35%)	Moderate	Moderate
9	Network Storage Disconnect	Config/ Hardware	Moderate	Expected	Moderate (40%)	Complex SAN, Limited expertise, Poor documentation	Moderate/Moderate	Moderate (60%)	Low (24%)	Moderate	Low
10	Minor Flooding (Non-Hurricane)	Environmental	Low	Predicted	Low (10%)	Drainage issues, Ground level vulnerabilities	Low/Low	Low (30%) - Raised floor helps	Low (3%)	Low	Low

Risk Calculation Methodology

Just to be transparent about how I calculated these risks (because the NIST guide is somewhat vague on the exact math), I used the following approach:

For Adversarial Risks:

- Overall Likelihood = Likelihood of Attack Initiation × Likelihood of Success
- Risk Level = Overall Likelihood × Impact Level
- Converted percentages to NIST scale (Very Low: 0-4%, Low: 5-20%, Moderate: 21-50%, High: 51-80%, Very High: 81-100%)

For Non-Adversarial Risks:

- Overall Likelihood = Likelihood of Event × Likelihood of Adverse Impact
- Used same risk matrix as adversarial

This might not be perfect, but it's consistent and defensible.

Assumptions

Based on the case study analysis and filling in realistic gaps, these assumptions were necessary to complete the assessment:

1. **Financial Volumes:** Assuming the university processes approximately $15-20 million monthly through Banner (tuition, payroll, vendors), based on 15,000 students and typical university operations. This drives the "Very High" financial impact ratings.
2. **Threat Intelligence:** Since no threat intelligence program was mentioned, I'm assuming the university relies on free feeds (US-CERT, FBI warnings) rather than commercial threat intelligence. This limits their ability to proactively identify threats.

3. **Password Specifications:** The "not consistent with industry standards" comment likely means 8-character minimum, no complexity requirements, no forced rotation, and password reuse allowed. This is based on what many universities still used pre-2020.
4. **Account Termination Timeline:** The "not timely" removal of terminated accounts probably means 15-30 days based on monthly HR processing cycles typical in universities. Some accounts likely persist longer if HR doesn't notify IT.
5. **Backup Testing:** Daily backups are mentioned but no testing program. I'm assuming they've never done a full restore test, maybe only file-level recoveries. The backups might not even be encrypted.
6. **Change Frequency:** Based on the lack of formal process, probably 2-3 production changes weekly, mostly during business hours (risky), with about 10% causing some sort of incident.
7. **Hurricane Probability:** Southern Florida coast location means 30% annual probability of tropical storm impact, 10% for major hurricane. Climate change is making these estimates conservative.
8. **Regulatory Scope:** The university must comply with FERPA (student records), GLBA (financial aid), PCI-DSS (credit cards), and Florida sunshine laws. Non-compliance fines could reach millions.
9. **Incident History:** The reluctance to discuss past incidents suggests they've had breaches but kept them quiet (under reporting thresholds). This is common in higher education.
10. **Budget Constraints:** Public university funding has been cut repeatedly. IT probably gets 2-3% of the overall budget versus the 5-6% they need. Security gets maybe 10% of the IT budget.
11. **Network Segmentation:** The centralized structure suggests flat network design with VLANs at best. Banner probably isn't properly isolated from general campus network.
12. **Patch Management:** Quarterly patching mentioned means they're always 30-90 days behind critical patches. Emergency patches probably don't happen unless something breaks.

13. **Staff Expertise:** With 30 IT staff for everything, maybe 2-3 have security focus. Probably high turnover as people get experience then leave for better paying private sector.
14. **Recovery Capabilities:** Without offsite backups or documented procedures, full recovery from ransomware would take 4-6 weeks minimum, assuming they pay ransom (which they probably would).
15. **Physical Security Effectiveness:** While biometrics and guards exist, tailgating is probably common. Video surveillance might not cover all areas or retain footage long enough.
16. **Insurance Coverage:** Probably have cyber insurance but with high deductibles and exclusions for "failure to maintain security standards" - which they clearly aren't meeting.
17. **Third-Party Risk:** Banner vendor (Ellucian) probably pushes updates that must be applied, sometimes breaking customizations. No vendor risk assessment process mentioned.
18. **Data Classification:** No mention of data classification scheme suggests everything is treated the same, whether it's public directory info or SSNs.

Recommendations for Risk Treatment

While not formally required, I feel obligated to provide initial recommendations for the highest risks:

Immediate Actions (This Week)

1. Start backing up critical data offsite - even if it's just encrypted drives to someone's house initially.
2. Enable MFA on all administrative accounts using free solutions like Google Authenticator, Microsoft Authenticator or maybe DUO.
3. Document all current admin account holders and start access review.

4. Create incident response plan draft - better than nothing.

Short Term (30 Days)

1. Implement formal change control process with management approval.
2. Contract for cloud backup service (AWS, Azure, even Backblaze).
3. Develop account termination checklist with HR.
4. Conduct phishing awareness training.

Medium Term (6 Months)

1. Upgrade password policies to 14+ characters with complexity.
2. Implement DLP solution for critical data.
3. Develop and test disaster recovery plan.
4. Consider cyber insurance if not already in place.

Long Term (1 Year)

1. Build redundant data center or move critical systems to cloud.
2. Implement proper network segmentation.
3. Hire dedicated security staff (at least 2 FTEs).
4. Achieve formal compliance certification (ISO 27001 or similar).

Conclusion

So, after spending way too many hours on this assessment, I've come to some pretty stark conclusions about the university's risk posture. The Banner Finance system is essentially a disaster waiting to happen. I don't mean to be alarmist, but when you combine weak passwords, no offsite backups, and delayed account termination in a system handling millions of dollars... well, it's not a matter of if something bad will happen, but when.

What really gets me is that most of these issues aren't technically complex to fix. We're not talking about implementing quantum encryption or anything cutting-edge. These are basic, fundamental security practices that have been standard for over a decade. The fact that the university is still struggling with them in 2025 suggests the problem isn't technical - it's organizational. There's clearly a disconnect between what leadership thinks their security posture is and what it actually is.

The NIST framework helped structure this analysis, but honestly, you don't need a complex framework to see the problems here. Any IT auditor (or honestly, any IT student who's taken a security class) could walk in and immediately spot the red flags. The challenge is going to be getting the university administration to actually act on these findings before something catastrophic happens.

If I had to bet, I'd say they'll probably experience a significant security incident within the next 12-18 months if nothing changes. Whether that's ransomware, a data breach, or a hurricane taking out their only data center, the current setup is unsustainable. The really frustrating part is that with even modest investments in security (we're talking maybe $200-300K annually), they could dramatically reduce their risk profile.

Looking at this from a broader perspective, ITMM IT Audit University is probably representative of many mid-sized educational institutions. They're caught between increasing threats, growing compliance requirements, and shrinking budgets. But that's not an excuse - it's a reality they need to face and address.

The good news, if there is any, is that they've at least taken the first step by conducting this assessment. Now they know where they stand. The question is: what will they do with this information?

References

Ellucian. (2024). *Banner security configuration guide* (Version 9.x). Ellucian Company. https://www.ellucian.com/banner-security

Federal Bureau of Investigation. (2024). *Internet crime report 2024*. IC3. https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. Information Systems Audit and Control Association.

Multi-State Information Sharing and Analysis Center. (2025). *Ransomware in higher education: 2024 trends and 2025 outlook*. MS-ISAC. https://www.cisecurity.org/ms-isac

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30, Revision 1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Revision 5). U.S. Department of Commerce.

National Oceanic and Atmospheric Administration. (2025). *Hurricane risk assessment for Southern Florida coastal regions*. NOAA National Hurricane Center. https://www.nhc.noaa.gov/risk

Otero, A. (2019). *ITMM IT audit university case study*. Canvas Learning Management System, ITMM 586 Course Materials.

Payment Card Industry Security Standards Council. (2024). *PCI DSS v4.0 requirements and testing procedures*. PCI SSC. https://www.pcisecuritystandards.org

Ponemon Institute. (2024). *Cost of a data breach report: Education sector analysis*. IBM Security. https://www.ibm.com/security/data-breach

SANS Institute. (2024). *Critical security controls for higher education* (Version 8.1). Center for Internet Security. https://www.sans.org/critical-security-controls/

U.S. Department of Education. (2023). *FERPA compliance guide for higher education institutions*. ED.gov. https://studentprivacy.ed.gov

Verizon. (2025). *2025 data breach investigations report - Education supplement*. Verizon Enterprise Solutions. https://enterprise.verizon.com/resources/reports/dbir/

Appendices

Appendix A: Interview Notes Summary

IT Executive Director (ITED) - September 24, 2025, 2:00 PM

- Seemed surprised by some of my questions about security practices.

- Kept emphasizing that "we've never had a major incident" (which doesn't mean much).
- Very proud of physical security but defensive about logical security questions.
- Admitted budget is "challenging" but wouldn't give specific numbers.
- Mentioned board of trustees is "technology-averse" and doesn't understand cyber risks.
- Said they rely heavily on vendor (Ellucian) for security but couldn't explain what that meant.

Banner Security Administrator (BSA) - September 25, 2025, 9:00 AM

- Most knowledgeable but also most frustrated interviewee.
- Confirmed many suspicions about weak controls but asked me not to "make her look bad".
- Mentioned she's been asking for security improvements for 3 years.
- Revealed there was an "incident" last year that was "handled internally".
- Has documentation of risks she's raised but management hasn't acted on.
- Considering leaving for private sector position.

Operations Supervisor (OS) - September 26, 2025, 11:00 AM

- Focused entirely on uptime and availability, security is "not my problem".
- Admitted backup testing hasn't been done because "we can't afford downtime".
- Generators have fuel for 48 hours maximum, never tested under full load.
- Raised floor is only 18 inches - not enough for major flooding.
- Mentioned AC units are "held together with duct tape and prayers".

Systems Administrator (SA) - September 26, 2025, 2:00 PM

- Relatively new (8 months) and still learning Banner.
- Inherited undocumented system with many customizations.
- Trying to improve things but getting pushback on any changes that might cause downtime.
- Confirmed patches are applied quarterly "if we're lucky".
- Wants to implement configuration management but no budget.

Network Administrator (NA) - September 27, 2025, 10:00 AM.

- Made it clear Banner security is "not his responsibility".
- Network is "flat as a pancake" with minimal segmentation.
- Firewalls are configured but rules haven't been reviewed in years.
- No network monitoring beyond basic up/down alerts.
- Admitted he doesn't have visibility into encrypted traffic.

Appendix B: Risk Assessment Methodology Details

The NIST SP 800-30 Rev.1 methodology uses a multi-tier approach that I found initially confusing but actually makes sense once you get into it. Here's how I applied it:

Tier 1 (Organization): Looked at university-wide governance, policies, and strategic risks. The centralized IT structure is both a strength (consistent policies) and weakness (single point of failure).

Tier 2 (Mission/Business): Examined how IT risks affect core university functions - teaching, research, and administration. Financial processes are critical because they enable everything else.

Tier 3 (Information Systems): Deep dive into Banner specifically - its configuration, vulnerabilities, and operational risks. This is where most of the technical issues surfaced.

The risk calculation formula I used:

- **Risk = Likelihood × Impact**
- Where Likelihood = (Threat Capability × Intent × Targeting) × Vulnerability Severity
- And Impact = Asset Value × Maximum Consequence

I converted everything to percentages then mapped to NIST's qualitative scale because that's what senior leadership understands.

Appendix C: Acronyms and Abbreviations

- **APT**: Advanced Persistent Threat
- **BSA**: Banner Security Administrator
- **DDoS**: Distributed Denial of Service
- **DHS**: Department of Homeland Security
- **DLP**: Data Loss Prevention
- **FERPA**: Family Educational Rights and Privacy Act
- **GLBA**: Gramm-Leach-Bliley Act
- **HVAC**: Heating, Ventilation, and Air Conditioning
- **IC3**: Internet Crime Complaint Center
- **ITED**: IT Executive Director
- **MFA**: Multi-Factor Authentication

- **MS-ISAC**: Multi-State Information Sharing and Analysis Center
- **NA**: Network Administrator
- **NIST**: National Institute of Standards and Technology
- **NOAA**: National Oceanic and Atmospheric Administration
- **OS**: Operations Supervisor
- **OWASP**: Open Web Application Security Project
- **PCI-DSS**: Payment Card Industry Data Security Standard
- **PII**: Personally Identifiable Information
- **RAID**: Redundant Array of Independent Disks
- **RTO/RPO**: Recovery Time Objective/Recovery Point Objective
- **SA**: Systems Administrator
- **SAN**: Storage Area Network
- **SQL**: Structured Query Language
- **SSN**: Social Security Number
- **UPS**: Uninterruptible Power Supply
- **US-CERT**: United States Computer Emergency Readiness Team

Appendix D: Document Revision History

Version	Date	Author	Changes
0.1	Sept 18, 2025	Noble Antwi	Initial draft, began stakeholder interviews

0.2	Sept 27, 2025	Noble Antwi	Completed interviews, began risk analysis
0.3	Sept 28, 2025	Noble Antwi	Populated risk tables, calculated risk scores
1.0	Sept 29, 2025	Noble Antwi	Final review, added recommendations and conclusion

Final Statement

This risk assessment represents my best professional judgment based on the information available at the time of the assessment. The findings and recommendations are based on industry standards, particularly NIST SP 800-30 Rev.1, and my analysis of the specific circumstances at ITMM IT Audit University.

I certify that this work is my own analysis and interpretation of the case study materials, supplemented with reasonable assumptions where data was incomplete. Any errors or omissions are my responsibility.

One last thought - doing this assessment really drove home something we discussed in class about the difference between theoretical security and practical security. You can know all the frameworks and best practices, but if you can't get buy-in from leadership and secure adequate resources, that knowledge doesn't translate into actual security. ITMM IT Audit University seems stuck in that gap between knowing what they should do and being able to actually do it. That's probably the biggest risk of all - not the technical vulnerabilities, but the organizational inertia that prevents fixing them.

Respectfully submitted,

Noble Antwi
nantwi@hawk.illinoistech.edu

ITMM 586 - Information Technology Auditing
Fall 2025