AuditCon

by ACUA

Louisville Kentucky | September 14-18, 2025

ACUA

September 17, 2025 | 10:15 AM – 11:05 AM EST

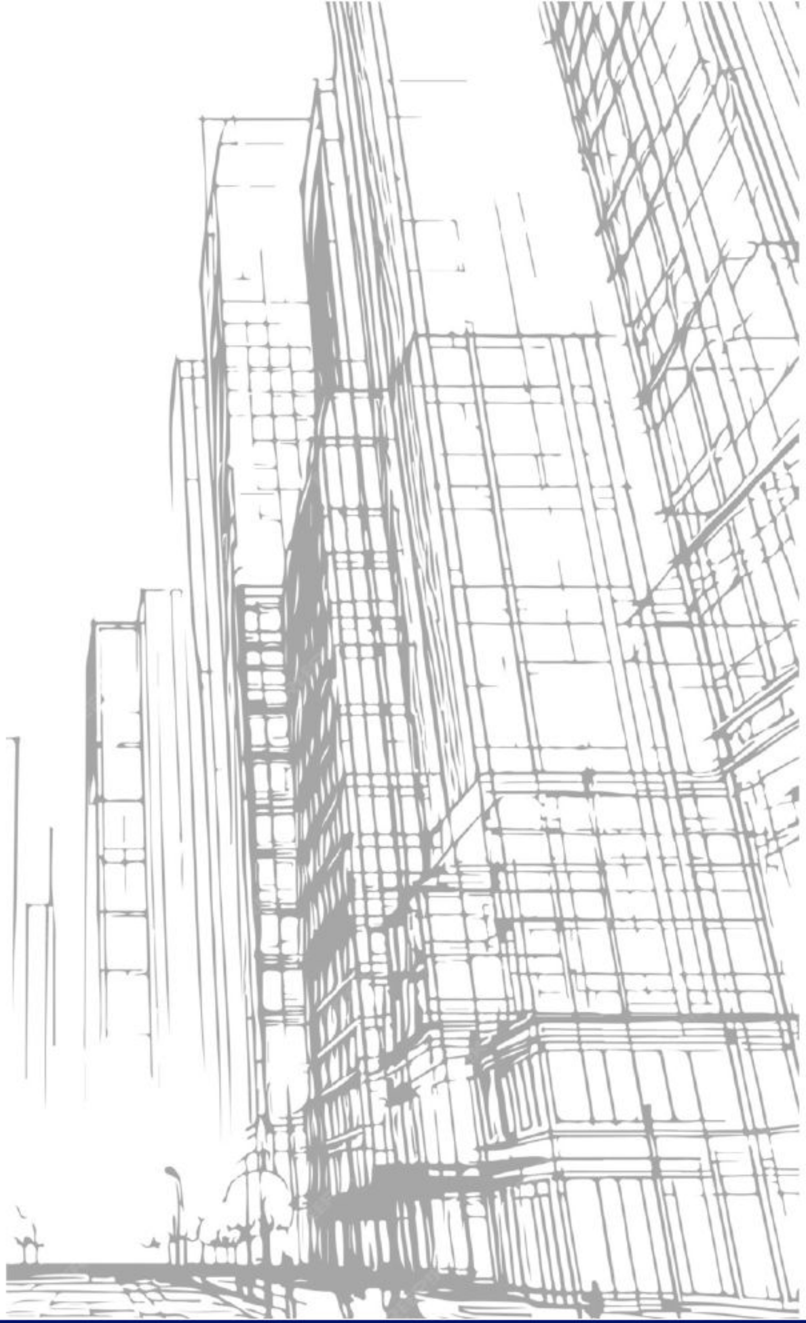
C09 - Facilities Risk Assessments: Enhancing Risk Mitigation in Capital Projects and Facilities Management

Presenters:

Curt Plyler
Principal
cplyler@forthillassociates.com

Ruhtab Sahota
Associate Director
rsahota@forthillassociates.com

- Why facilities & capital project risk assessments matter to higher education institutions (budget strain, compliance, deferred maintenance).



Why Facilities & Capital Project Risk Assessments Matter to Higher Education Institutions?

1. Budgetary Impact

- **Capital Intensity:** Universities often manage billion-dollar physical plant portfolios, making facilities a major budget driver.
- **Deferred Maintenance:** Chronic underfunding leads to compounding liabilities (e.g., HVAC failures, code compliance upgrades).
- **Cost Overruns:** Construction projects without proper risk assessments frequently exceed budgets, forcing reallocation from academic priorities.

2. Compliance & Regulatory Pressure

- **Federal & State Oversight:** Higher ed must comply with state procurement laws, OSHA, ADA, and fire safety codes.
- **Audit & Accreditation:** Non-compliance in facilities management can jeopardize accreditation or federal funding.
- **Environmental & Sustainability Mandates:** ESG reporting and carbon-reduction goals tie directly to facilities risk.

3. Operational & Institutional Risks

- **Mission Disruption:** Facilities failures (lab shutdowns, housing outages) directly impact teaching, research, and student experience.
- **Outsourced Service Providers:** Risks from vendors (custodial, dining, energy) affect daily campus operations.
- **Continuity & Safety:** Emergency preparedness gaps in facilities planning can expose institutions to liability.

4. Reputational Risk

- **Student & Parent Expectations:** Facilities condition influences recruitment and retention.
- **Public Scrutiny:** Headlines about failed capital projects, vendor scandals, or unsafe buildings can damage donor confidence.
- **Community Impact:** Universities are often anchor institutions; project mismanagement impacts surrounding communities.

Why Risk Assessments are Essential?

1. Budgetary Impact
2. Compliance & Regulatory Pressure
3. Operational & Institutional Risks
4. Reputational Risk

Risk Assessment

Structured Oversight:
Provides a systematic lens to prioritize projects and risks against institutional strategy.

Data-Driven Decision-Making:
Moves facilities planning from reactive to proactive, with quantified risk exposure.

Integration with ERM:
Links facilities risk with broader enterprise risks (financial, operational, reputational).

Long-Term Sustainability:
Enables lifecycle planning, capital renewal strategies, and funding justifications to boards and state agencies

Our Plan

ERM Framework
How ERM applies to higher ed facilities.

Project Risk Management
PMI-based methodology in action

Procurement Risk
Oversight, vendor scorecards, risk tools.

Risk Assessment
Turning information into actionable insights.

AI Tool
Real-time monitoring for payment applications.

Case Insights
Real-world examples, lessons learned, and leading practices.

ERM In Higher Education For Facilities & Capital Projects
Quick Primer On ERM And Its Relevance

Risk Categories Mapped To Higher Ed Context:

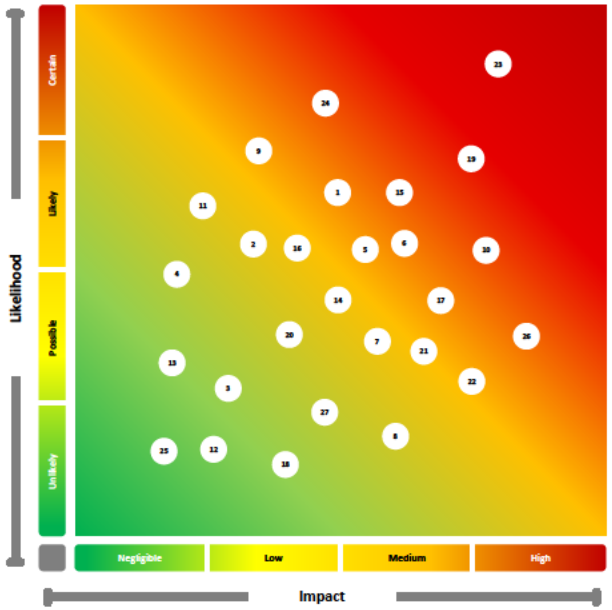
Strategic Risks
(capital planning misalignment with institutional mission)

Financial Risks
(budget overruns, contract leakage)

Operational Risks
(facilities downtime, deferred maintenance)

Compliance Risks
(statutory monitoring, O&M obligations)

Sample ERM Risk Matrix:



Risk Legend

1. Deferred Maintenance Risk
2. Compliance Risk
3. Operational Downtime
4. Funding & Budget Uncertainty
5. Health & Safety Risk
6. Schedule Delays
7. Cost Overruns
8. Technology & Systems Risk
9. Contractor & Vendor Risk
10. Design Errors & Omissions
11. Staff & Working Gaps
12. Reputation Damage
13. Regulatory & Permitting Risk
14. Scope Creep
15. Pandemic & Public Health
16. Stakeholder Dissatisfaction
17. Supply Chain Disruptions
18. Weather & natural Disasters
19. Space Utilization Inefficiencies
20. Long-Term Debt Obligations
21. Economic Conditions
22. Construction Safety Risk
23. Variance Analysis
24. Escalating Operating Costs
25. Sustainability Failure
26. Underfunding of Maintenance
27. Overestimation of Funding Sources

Impact & Likelihood Scales

High Impact	Medium Impact	Low/Negligible Impact
Risk is not certain, but very severe if it does occur. Financially, this could be a loss of revenue or increase in expenses of greater than $10 million. Legally, this could be external agency sanctions, civil issues, criminal liability.	Risk is not certain, but medium impact if it does occur. Financially, this could be a loss of revenue or increase in expenses between $1 million and $10 million. Legally, these could be restrictions or requirements placed on the University's operational activities.	Risk is not certain, but low/negligible if it does occur. Financially, this could be a loss of revenue or increase in expenses of less than $1 million. Legally, this could be regulatory fines of less than $1 million.

Certain or Almost Certain Likelihood	Likely Likelihood	Possible/Unlikely Likelihood
Risk presents moderate consequences, but certain or almost certain to occur	Risk presents moderate consequences, but it is likely to occur	Risk presents moderate consequences, but possible or unlikely to occur

ERM & Professional Standards Alignment

1. Internal Audit Standards (IIA IPPF – International Professional Practices Framework)

- **Standard 2010 – Planning:** Requires internal auditors to develop risk-based plans to determine audit priorities.
- **Standard 2120 – Risk Management:** Internal audit must evaluate the effectiveness of risk management processes.
- **Standard 2130 – Control:** Internal audit must assess adequacy and effectiveness of controls in responding to risks.

Application to Facilities & Capital Projects:

- Use risk assessments to select projects for audit (e.g., high deferred maintenance backlog).
- Evaluate risk responses like vendor monitoring, contract controls, and compliance programs

2. COSO ERM Framework

- **Components:** Governance & Culture, Strategy & Objective Setting, Performance, Review & Revision, Information & Communication.
- **Risk Assessment:** Central step — identify events, assess likelihood and impact, prioritize responses.

Application:

- Facilities risk assessment feeds into enterprise-wide risk registers.
- Capital project risk scoring (likelihood × impact) links to institutional performance objectives.

3. ISO 31000 (Risk Management Standard)

- **Principles:** Risk management should be structured, customized, inclusive, dynamic, based on best available information.
- **Process: Establish context → Risk identification → Risk analysis → Risk evaluation → Risk treatment.**

Application:

- Facilities downtime **risk = identified → analyzed → scored → mitigation plan developed.**
- Fits well with higher ed where risks span compliance, finance, safety, and strategy.

4. PMI Standards (PMBOK – Project Risk Management)

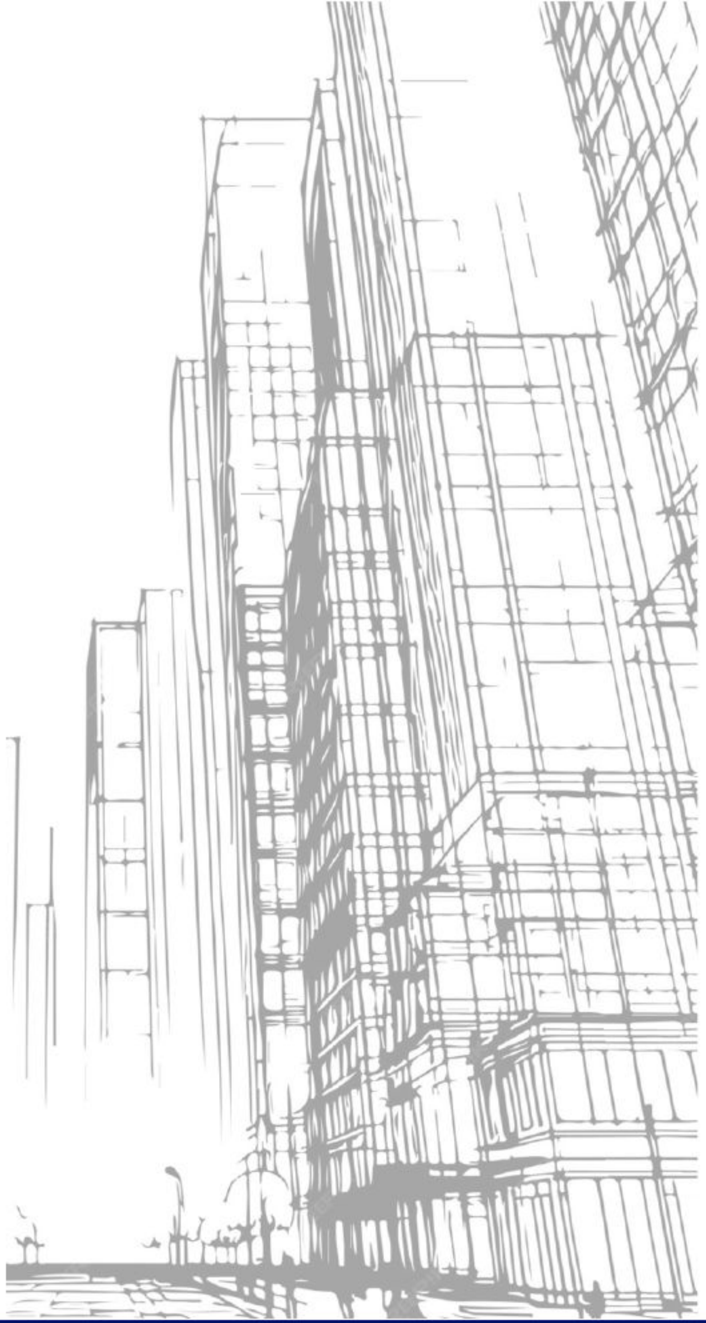
- **Steps: Identify Risks → Perform Qualitative Analysis → Perform Quantitative Analysis → Plan Risk Responses → Monitor & Control Risks.**

Application:

- Capital construction projects: change orders, design delays, vendor non-performance.
- Risk registers from projects roll up into institutional ERM.

5. Government & Higher Education Guidance

- **OMB Circular A-123 (for federally funded institutions):** Requires institutions to integrate ERM into internal control processes.
- **Accreditation & State Oversight:** Many accrediting bodies require evidence of risk-based planning in facilities management and compliance reporting.



Risk categories mapped to higher ed context

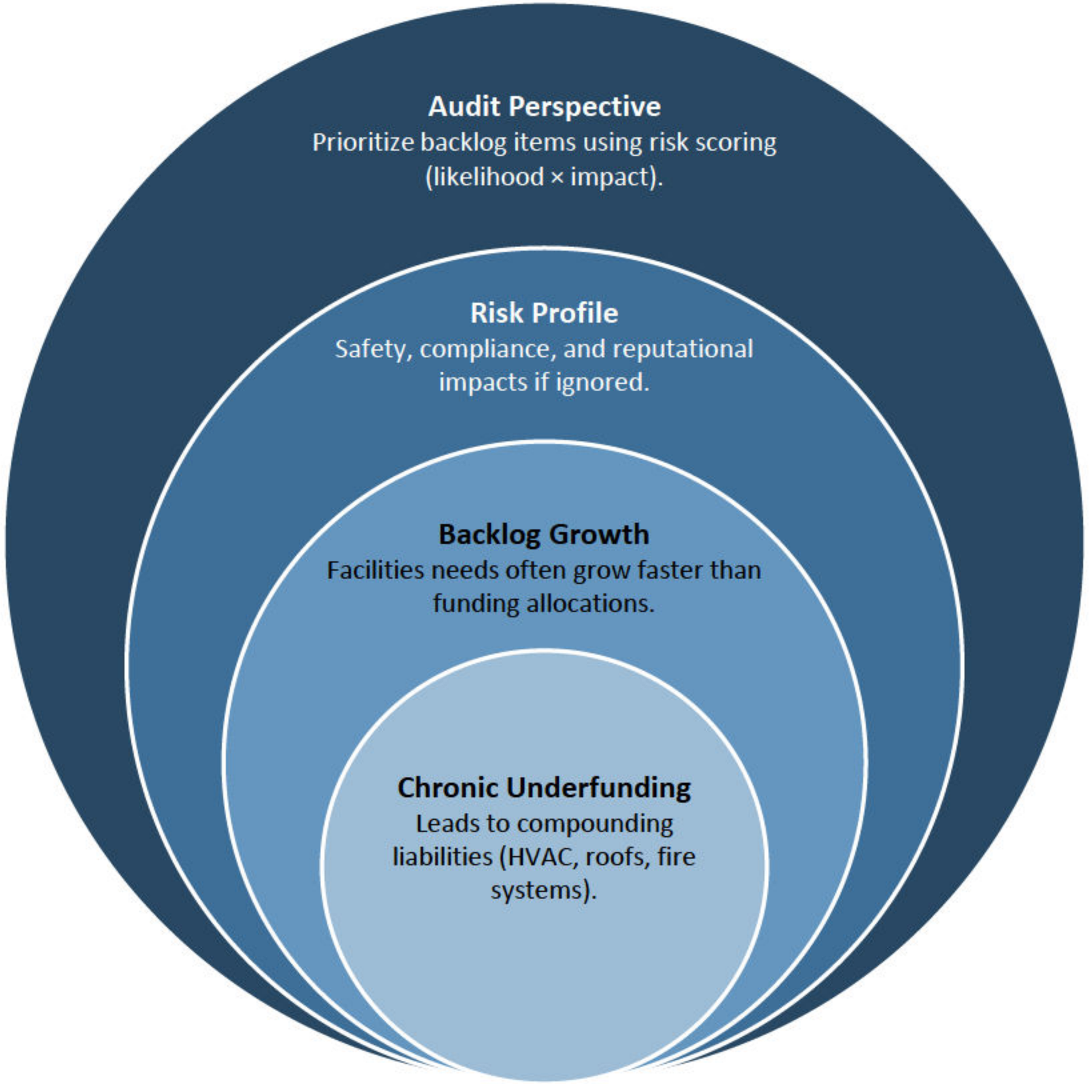
A comprehensive risk assessment framework for university facilities, encompassing a wide array of potential issues.

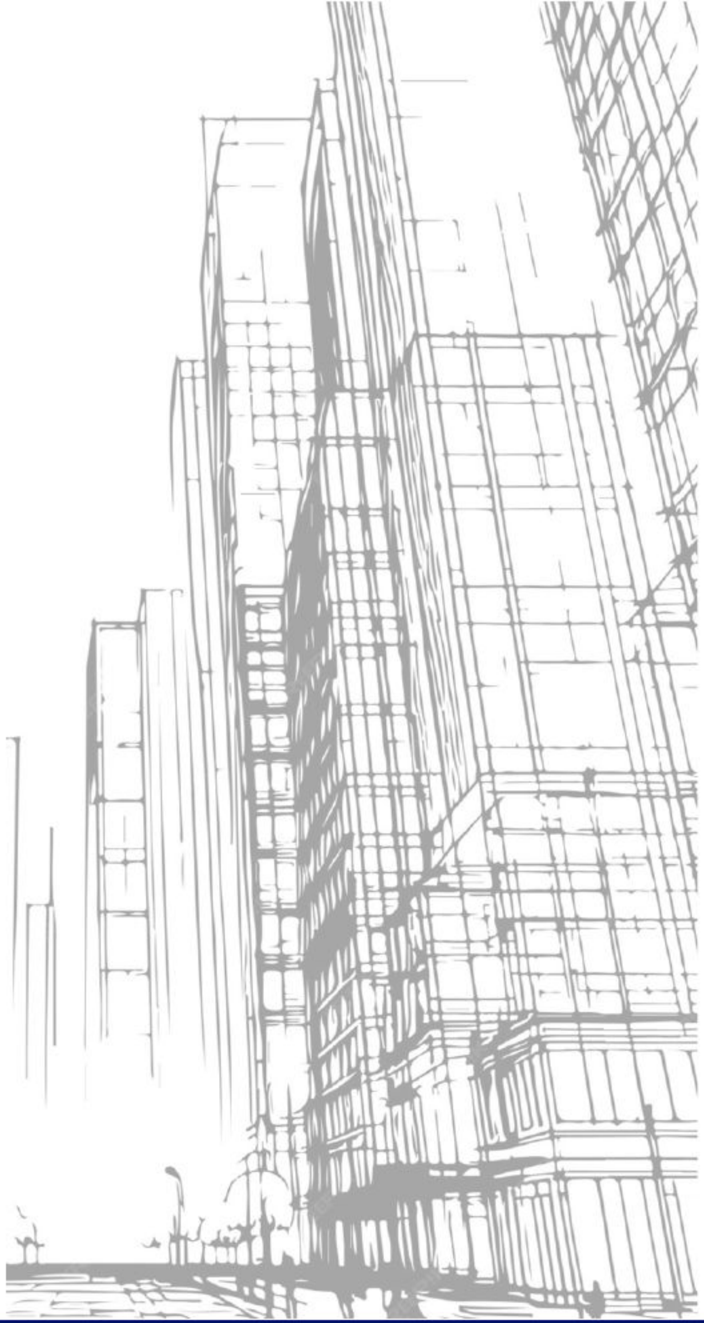
It systematically categorizes risks into several key areas:

1. Deferred Maintenance
2. Health & Safety
3. Operational Downtime
4. Staffing & Workforce Gaps
5. Compliance
6. Technology & Systems
7. Financial Risks
   Cost Overruns, Schedule Delays, and Funding Uncertainty
8. External factors
   Weather Events, Economic Conditions, and Supply Chain Disruptions

The framework should examine internal operational challenges related to space utilization, sustainability, stakeholder satisfaction, reputation, and the financial management of maintenance and capital projects. Each risk area is accompanied by specific audit questions and descriptions of the associated potential impacts, aiming to identify vulnerabilities and guide strategic planning.

Deferred Maintenance: A Growing Risk





Linking Risk Assessments to Long-Term Capital Planning

Life-Cycle Planning:
Use risk insights to schedule replacements & capital renewal.

Capital Prioritization:
Rank projects based on risk exposure, not just funding availability.

Integration:
Feed results into ERM dashboards for board visibility.

Risk-adjusted budget forecasting.

Use of condition assessments + cost modeling.

Regular updates tied to accreditation & state oversight.

BEST PRACTICES

Facility Condition Index (FCI): What Auditors Need to Know

Definition of FCI:
- Ratio of **deferred maintenance cost ÷ current replacement value** of a facility.
- Benchmark metric for assessing facility condition.

How FCI is Used in Facilities:
- Provides a quantifiable measure of building health.
- Helps prioritize funding for repairs, renewals, or replacements.
- Supports long-term capital planning and resource allocation.

What FCI Does for Decision-Making:
- **FCI < 0.05** (Good condition).
- **FCI 0.05 – 0.10** (Fair condition).
- **FCI > 0.10** (Poor condition → higher risk).
- Guides whether to **maintain, renovate, or replace (0.4)** a facility.

Auditor's Perspective on FCI:
- Validate use of FCI in deferred maintenance.
- Assess whether FCI data is updated regularly and consistently across campus.
- Evaluate if FCI is integrated into **budgeting and risk assessment processes**.
- Look for gaps: **"Are high FCI buildings being addressed in capital planning?"**

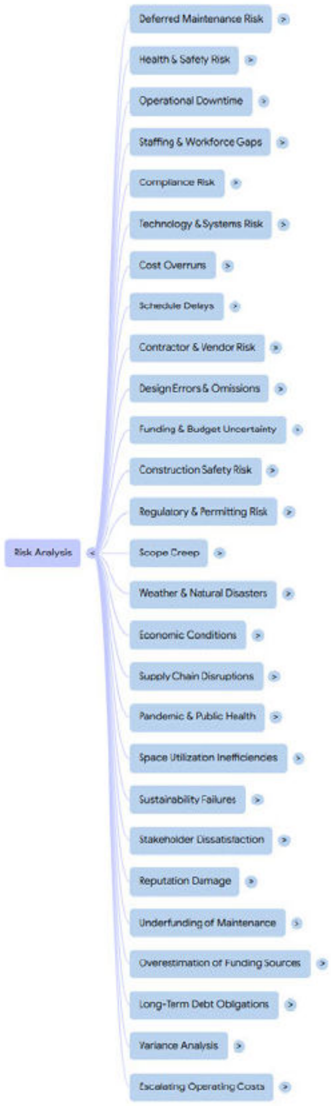
Example:

Building A: $10M deferred maintenance / $80M replacement = FCI 0.125 → Poor."

The Facility Condition Index, or FCI, is one of the most common metrics in higher ed facilities management. It's a ratio of deferred maintenance to replacement value. An FCI under 0.05 is considered good; anything above 0.10 is poor.

For auditors, the key is to validate that the data behind FCI is accurate and that institutions actually use it to inform capital planning. An institution may report FCI, but if they're not tying it into funding decisions, it's a red flag.

How? Risk categories and 4 Step Process



Step 1: Survey Questionnaires How is the survey typically administered

Who? Our Office of IA launches formal surveys for us.
How? This can be more formal, or via email, word document.
Target? How many folks do you think we will need to share with to have a representative sample?

Develop customized questionnaires tailored to key risk areas:

- Architectural Services
- Business Operations
- Auxiliary Services

IA will distribute the questionnaires to relevant stakeholders and ensure timely responses.

Step 2: Compilation and Analysis

- Review and analyze survey responses to identify gaps, high-risk areas, for actionable insights.
- Determine the necessity of follow-up discussions based on the depth and quality of responses.

Step 3: Stakeholder Conversations (if required)

- Conduct discussions (if needed) with key personnel to review questionnaire responses and refine risk rankings.

Step 4: Risk Assessment Compilation

- Aggregate survey responses into a structured risk assessment report.
- Prioritize risks based on likelihood, impact, and contributing factors.
- Provide an audit roadmap for 2026.

Risk categories 4 Step Process

Audit Area → Question → Risk → Likelihood → Impact → Description → Risk Score → Risk Level

Deferred Maintenance Risk	What percentage of maintenance projects are delayed due to funding constraints?	Risk of deferred maintenance and operational setbacks due to funding shortfalls.
	To what extent and with what frequency are preventative maintenance (PM) schedules reviewed and optimized?	Risk of increased asset wear and failure due to poorly optimized preventive maintenance practices.
	Have you identified equipment or systems with a high frequency of maintenance requests, and if so, how many?	Risk of operational inefficiency due to over-reliance on reactive maintenance for failing assets.
	For those identified equipment or systems, have replacement or upgrade plans been established, documented, and verified?	Risk of prolonged equipment failure due to absence of clear replacement or upgrade strategies.
	Has deferred maintenance led to unplanned service interruptions in past?	Risk of critical service disruptions stemming from unresolved maintenance backlogs.
	To what extent and with what rigor is formal root cause analysis conducted for repeated safety-related or maintenance issues?	Risk of recurring issues due to inadequate investigation into maintenance failure causes.
	Are there strategies in place to reduce the backlog of deferred maintenance projects?	Risk of mounting deferred maintenance due to absence of effective backlog reduction strategies.
Staffing & Workforce Gaps	Does the University have an incentive program to improve staff retention in high-turnover roles?	Risk of high turnover and skill gaps due to absence of staff retention incentives.
Cost Overruns	What percentage % of capital projects have exceeded their original budget estimates in the past three years?	Risk of capital inefficiency and budget strain due to recurring cost overruns in project execution.
	Does the University conduct post-project reviews to analyze cost overruns?	Risk of repeated financial inefficiencies due to lack of learning from historical cost performance.
Weather & Natural Disasters	Does your department have a documented emergency response plan for extreme weather events?	Risk of chaotic response and service disruption from absence of formal emergency planning.
Space Utilization Inefficiencies	Have there been assessments conducted to optimize space utilization?	Risk of space underutilization and inefficiency due to lack of utilization assessments.
	To what extent and with what rigor are decisions on space allocation tied directly to operational efficiency or strategic priorities?	Risk of strategic misalignment in facility use due to non-prioritized space allocation decisions.
	With what frequency and rigor is space utilization analyzed, and are underutilized areas systematically reviewed for repurposing or optimization?	Risk of operational inefficiency from unreviewed underutilized spaces.
Underfunding of Maintenance	How frequently are facilities condition assessments conducted?	Risk of unaddressed facility degradation due to infrequent condition assessments.
	Are consistent cost estimation methods used across all building systems for repair or replacement projects?	Risk of budget inconsistencies and estimation errors from lack of standardized cost methods.
	How are estimated project costs integrated with the organization's budgeting and capital planning processes?	Risk of inaccurate funding allocations due to weak integration between cost estimates and capital planning.
	Have potential operational risks from identified poor-condition assets been documented?	Risk of asset failure and service disruption from undocumented high-risk infrastructure.
	What is the current prioritization method for addressing critical condition deficiencies?	Risk of inefficient resource use from unclear or inconsistent prioritization of critical deficiencies.
	Do you have a standardized risk-based prioritization system using condition data to better align maintenance actions with operational risk and strategic objectives?	Risk of misaligned maintenance actions from absence of a standardized risk-based prioritization system.

Procurement Risks in Facilities Maintenance & Construction

Facilities Maintenance Risks:
- Sole sourcing of O&M contracts (HVAC, custodial, landscaping).
- Lack of transparency in preventive vs. reactive maintenance invoicing.
- Weak SLA monitoring → **missed service calls, safety lapses.**

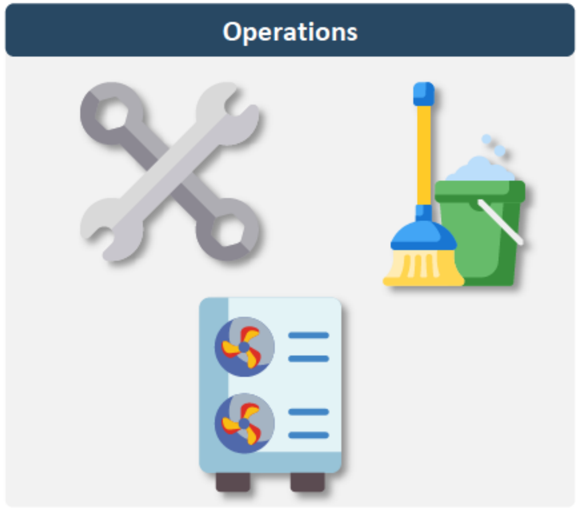
Facilities Construction Risks:
- Bid rigging or non-competitive subcontracting.
- Poor change order management inflating project costs.
- Inadequate oversight of materials/equipment procurement.

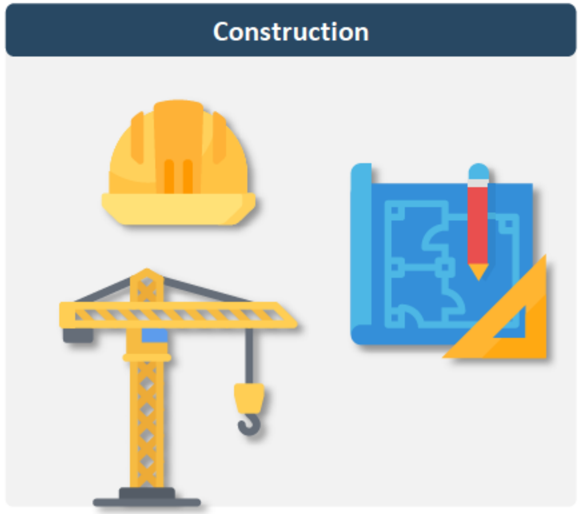
Risk Assessment Checklist (Facilities Lens):
- Are O&M contracts competitively bid?
- Is spend aligned to approved maintenance plans?
- Are construction bids benchmarked against market pricing?
- Is there consistent SLA/compliance tracking?

Vendor Oversight & Real-World Case Example
- **Vendor Scorecards for Facilities**
- **O&M:** SLA adherence (response times, preventive maintenance completion).
- **Construction:** Schedule adherence, change order frequency, safety incidents.
- **Shared metrics:** Invoice accuracy, compliance with contract terms.

Case Example – Custodial/O&M Contract:
- Audit revealed SLA non-compliance costing $250K annually (missed shifts, inflated overtime billing).
- Weak monitoring → gaps in service delivery & inflated costs.
- Implemented vendor scorecards: tracked SLA % met, response time benchmarks, cost variance.

Construction Tie-In:
Similar approach for GCs and subcontractors → metrics on cost variance, safety, change orders.



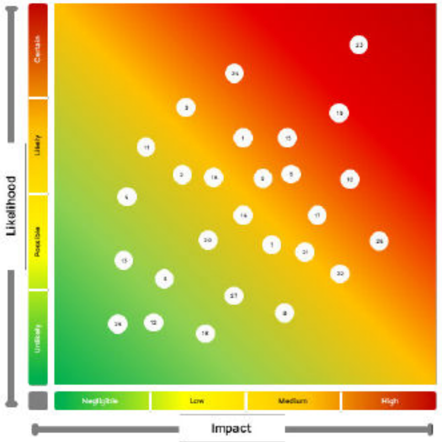


Case Insights
Live Tool Demo
Risk Assessment
Procurement Risk
Project Risk Management
ERM Framework

So How does it all Tie Together?

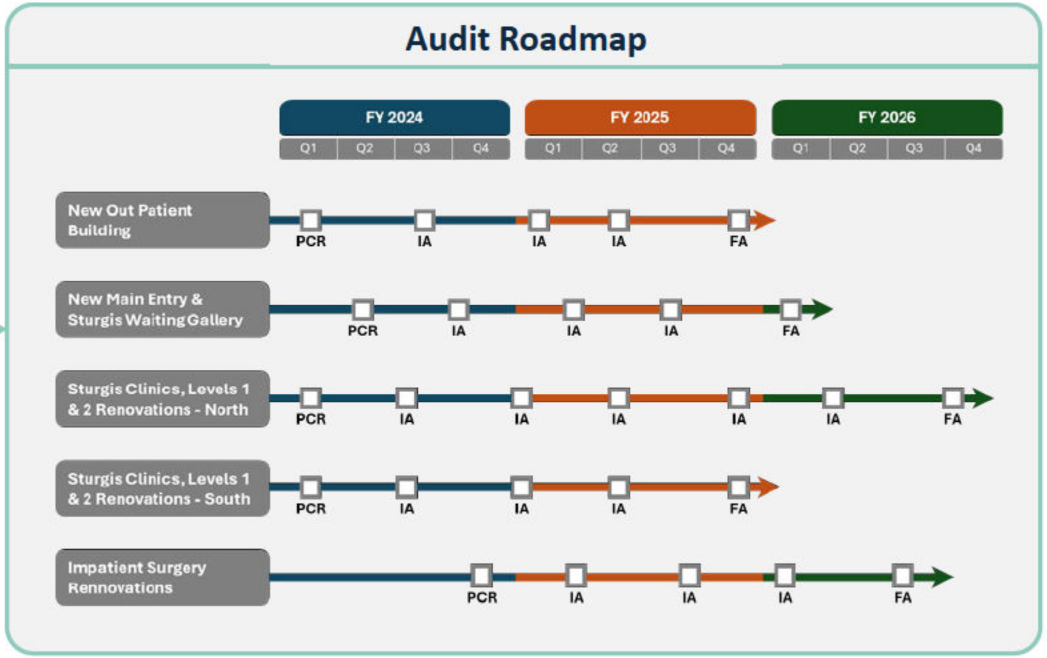
Risk Matrix + Heatmap = Audit Roadmap

Sample ERM Risk Matrix:



Risk Legend

- Deferred Maintenance Risk
- Compliance Risk
- Operational Downtime
- Funding & Budget Uncertainty
- Health & Safety Risk
- Schedule Delays
- Cost Overruns
- Technology & Systems Risk
- Contractor & Vendor Risk
- Design Errors & Omissions
- Staff & Working Gaps
- Reputation Damage
- Regulatory & Permitting Risk
- Scope Creep
- Pandemic & Public Health
- Stakeholder Dissatisfaction
- Supply Chain Disruptions
- Weather & natural Disasters
- Space Utilization Inefficiencies
- Long-Term Debt Obligations
- Economic Conditions
- Construction Safety Risk
- Variance Analysis
- Escalating Operating Costs
- Sustainability Failure
- Underfunding of Maintenance
- Overestimation of Funding Sources



Capital Project Risk Tracker

PMI Risk Management Process - PMI (PMBOK) framework:

- **Identify Risks –** Gather potential risks from stakeholders, contracts, past projects.
- **Analyze Risks –** Qualitative (likelihood/impact ranking), Quantitative (cost/schedule modeling).
- **Plan Risk Responses –** Avoid, Transfer, Mitigate, or Accept.
- **Monitor & Control –** Track risks throughout project lifecycle.

Risk Responses

- **Avoid:** Redesign before construction begins.
- **Transfer:** Push cost liability to design consultant via contract clause.
- **Mitigate:** Accelerate procurement and add overtime labor.
- **Accept:** Delay opening; communicate early to stakeholders.
- Stress that the choice depends on institution's risk appetite and budget flexibility.

Construction Project Delay (Design Change Risk)

- **Scenario:** University science building project. Midway through construction, scope change for lab ventilation redesign.
- **Potential impact:** 3-month delay, $2.5M cost increase.
- **Qualitative Analysis:** Likelihood = High, Impact = High → Critical Risk.
- **Quantitative Analysis:** Monte Carlo simulation / schedule modeling shows 70% chance project completion slips into next academic year.
- Qualitative tells us **"big problem,"** Quantitative tells us **how big (probability + financial impact).**

Monitoring & Control

- Use risk registers to track status and residual risk.
- Integrate with project dashboards.
- Regular updates at project steering committees.

Key Takeaway

- PMI risk framework provides structure for managing uncertainties in capital projects.
- Both qualitative & quantitative methods are essential.
- Risk registers = bridge between project-level risks and institutional oversight.

Construction Risk Register

PROJECT RISK REGISTER EXAMPLE – ADVANCED

REF ID	DATE RAISED	RISK CATEGORY	RISK DESCRIPTION (INCLUDING IF / THEN STATEMENT)	PROBABILITY 1 – 5	IMPACT 1 – 16	RISK SEVERITY SCORE Prob x Impact	LIKELY TIMING OF RISK	RISK TRIGGER	MITIGATION / RESPONSE PLAN	STATUS OF MITIGATION / RESPONSE	OWNER	OTHER NOTES
10001	MM/DD/YY	Materials	If there are changes in architectural plans that require additional or different resources, then there will be delays.	1	8	8	The risk is present throughout the process of finalizing architectural plans.	There are changes in the architectural plans.	A designated team member will continually monitor any proposed changes in architectural plans and ensure communication between architectural and construction teams about proposed changes.	No current issues	Joe Smith; architectural liaison	
10002	MM/DD/YY	Contracts	If contractual issues among contractors, subcontractors, or vendors arise, then there will be delays or cost overruns.	2	4	8	The risk is present before most contract work commences. However, the risk will also be present when additional contracts are added in the early phases of construction.	The contracts manager reports any potential contract issues.	The contracts manager will continually monitor contracts, alert the team when there are issues, and ensure that the team addresses and resolves contract issues before they cause delays.	Working on one unresolved issue with the electrician's contract; meeting set for May 2nd	Sue Johnson, contracts manager	
10003	MM/DD/YY	Permits / Regulations	If obtaining appropriate construction permits takes longer than planned, then there will be delays.	2	8	16	The risk is present throughout the construction phase of the project, including when securing required permits at the beginning of construction.	Construction permits do not arrive within the required timeframe.	The construction manager, or another designated team member, will monitor the project schedule and deadlines and ensure that all permits can accommodate the project's construction schedule.	All deadlines currently being monitored	Dale Swenson, construction manager	
10004	MM/DD/YY	Construction Site	If unexpected hazardous waste is found on the property, it will require mitigation or cleanup.	1	8	8	The risk is present throughout the project, especially toward the beginning when conducting site preparation work.	On-site managers report an issue, especially during site preparation.	The construction manager will assign a team member to monitor and explore any possible issues with hazardous waste.	No issues found to this point	Jeff Baker, construction assistant	
				1	1	1						
				1	2	2						
				1	4	4						
				1	8	8						
				1	16	16						

PROBABILITY | 1 – 5	IMPACT | 1 – 16	PI SCORES | 1 – 80
1 - RARE	1 - INSIGNIFICANT	1 – 2 = NEGLIGIBLE
2 - UNLIKELY	2 - MINOR	3 – 8 = LOW
3 - POSSIBLE	4 - MODERATE	10 – 16 = MEDIUM
4 - LIKELY	8 - MAJOR	20 – 32 = HIGH
5 - ALMOST CERTAIN	16 - SEVERE	40 – 80 = EXTREME

IMPACT \ PROBABILITY	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
4	4	8	12	16	20
8	8	16	24	32	40
16	16	32	48	64	80

AI for Gathering Real-Time Insights

1 Spend Analysis

Compare planned vs. actual spend across O&M and construction contracts.

2 Invoice Reviews

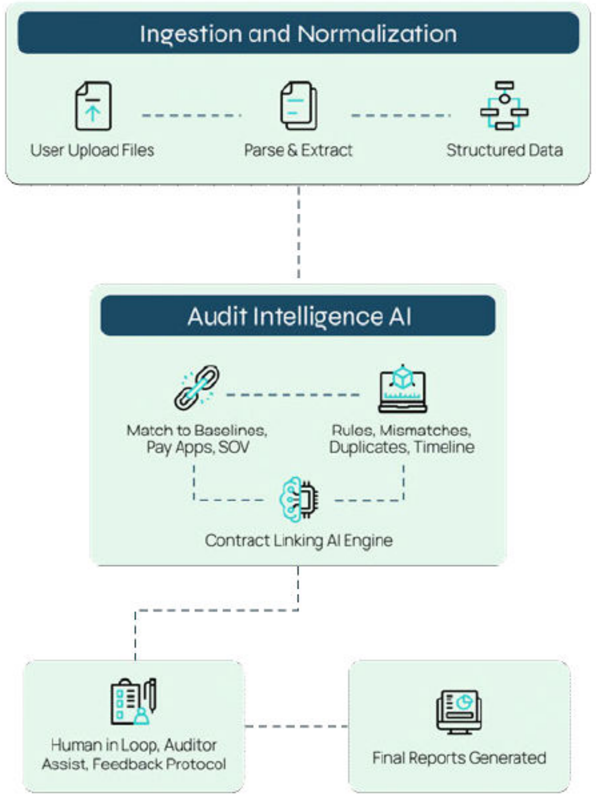
Detect deviations in labor, material, or GC costs.

3 Financial Risks

Track SLA compliance, invoice accuracy, and performance trends.

Turning Data into Insights

- Use dashboards and visualizations to spot red flags early.
- Prioritize risks based on cost impact, frequency, and compliance exposure.
- Create actionable intelligence for leadership and audit committees.



Transition to Real Time

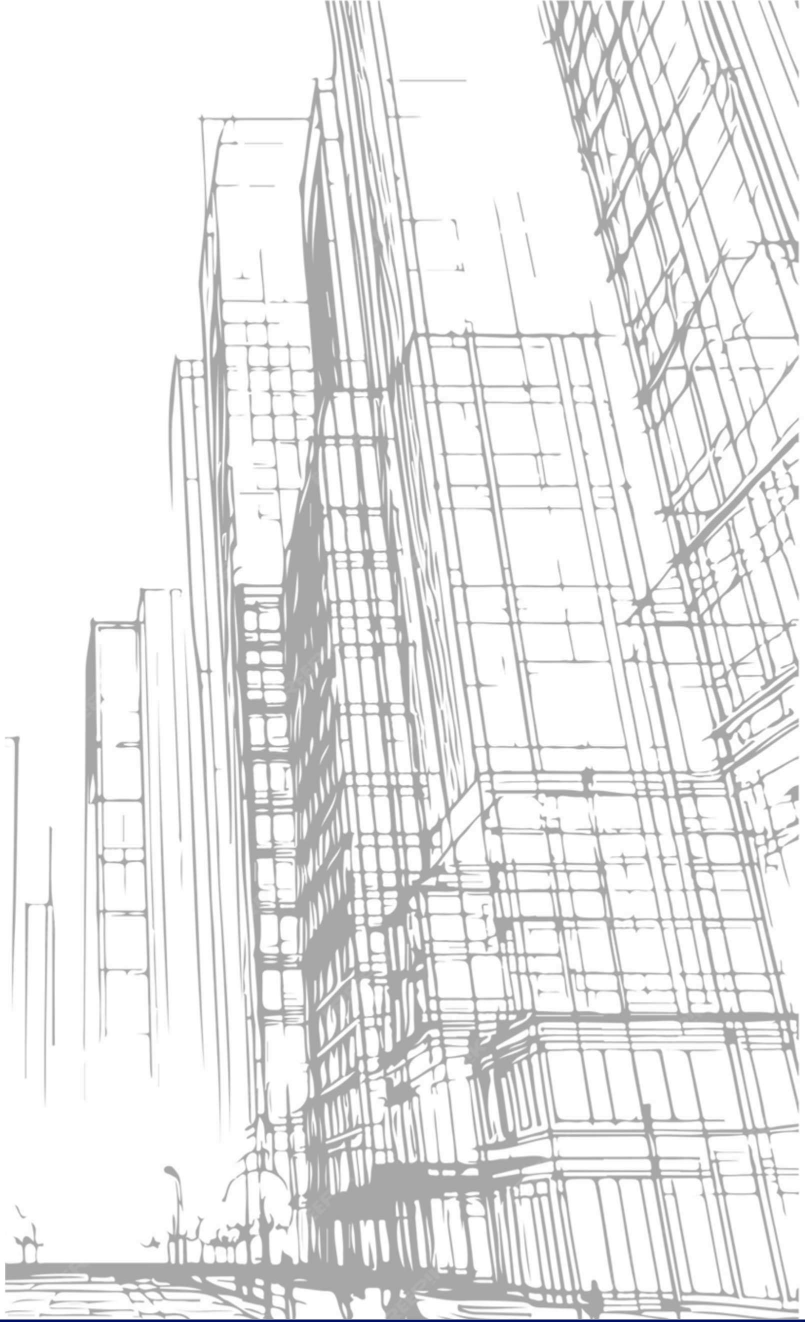
- "This is where tools transform audit insights into **real-time compliance monitoring**."
- AI ingests invoices and **flags payment line items** against contract Terms & Conditions.
- Provides real-time feedback loop: *Is the cost valid? Is it compliant? Is it within SLA?*

Recap and Questions

- **ERM Framework –** Align risks to institutional oversight.
- **PMI Risk Management –** Project-level identification, analysis, response.
- **Procurement Oversight –** Checklist + vendor scorecards for facilities & construction.
- **Data-Driven Insights –** Spend analysis, variance reporting, vendor audit data.
- **Real-time invoice validation** against O&M contracts.

3-Step Starter Roadmap for Attendees

- Build a Risk Register aligned to ERM
- Capture facilities, project, and vendor risks in one structure.
- Integrate Procurement & Project Risk Assessments
- Apply checklists, scorecards, and PMI methodology consistently.
- Leverage Tech-Enabled Compliance Tools
- Move from point-in-time audits → continuous monitoring.



Thank You!