Imperial College Union
Finance, Audit & Risk / 12 February 2026

Critical Systems Overview

Author(s): Ashley Cory (Director of Support Services)
Purpose: To set out risks and mitigations surrounding critical bespoke systems
Decision(s): To note

1. Purpose

This paper provides an overview of the union's critical back-end systems that are developed and maintained in-house and are not fully supported by third-party suppliers. It highlights the inherent risks associated with bespoke systems, particularly single points of failure arising from system dependency and specialist staff knowledge, and sets out current, short-term and longer-term mitigations.

The paper is intended to support the Committee's oversight of operational resilience, business continuity and technology risk, rather than to propose immediate investment decisions.

2. Current Operating Context

The union relies on a small number of bespoke applications to support core financial, governance and democratic processes. These systems integrate with university-managed platforms (notably SAP Business One and SUMS) and with internally managed databases.

There are currently three members of staff within the organisation with sufficient technical capability to diagnose and maintain these systems. Recent work to improve documentation and to spread technical knowledge between these staff has materially reduced risk, though it has not eliminated reliance on specialist capability.

Where "external support" is referenced in this paper, this refers to engaging external agencies or consultants and/or recruiting replacement in-house technical capacity.

There are also several external systems that are third party supported that are not in scope of this risk assessment. These include the core management system, SUMS, and the finance system, SAP Business One.

3. Risk Assessment Approach

Each system is assessed against:

- **Criticality to operations**
- **Key risks**, including single points of failure
- **Short-term mitigations** (immediate continuity measures)
- **Medium to long-term mitigations** (risk reduction and resilience)

4. System-by-system risk assessment

4.1. Unifi App and Web Reporting

Function	Financial document processing and workflow. Integrates eActivities with SAP Business One.
Current Position	The UniFi App and WR and associated workflows have been documented, including key processes and database tables. Knowledge risk is therefore partially mitigated.

Key risks	• Reliance on specialist knowledge, particularly in the absence of the Financial Controller. • Failure would disrupt automated financial document processing.	
Short-term mitigations	• Manual file transfer between eActivities and SAP Business One in event of failure. • Continued access to documented processes and database structures.	
Medium to long-term mitigations	• In the event of failure seek technical support from elsewhere within the organisation or externally if required. • Maintain and periodically review documentation to ensure it remains current and usable by non-authors.	
Overall risk rating	**Inherent: L=3 I=4 Total=12**	**Residual: L=2 I=3 Total=6**
Comment	Low risk mitigated by documentation and manual fallback processes.	

4.2. eActivities

Function	Management of union financial documentation and limited operational management. Bespoke PHP application incorporating e2 modules and legacy components.	
Current Position	Many functions of eActivities have been made redundant with the use of SUMS. The development roadmap for the system is to reduce the scope, modernise and make modular.	
Key risks	• Single point of failure if the system fails in the absence of in-house technical resource. • Direct impact on the processing of clubs and societies financial documentation.	
Short-term mitigations	• Establish manual processes for handling clubs and societies financial documentation in the event of failure. • Direct access to existing financial documents via the underlying database.	
Medium to long-term mitigations	• Source technical resource externally or via the university to stabilise or repair the system. • Where feasible, migrate non-critical management functionality into SUMS, accepting some short-term disruption.	
Overall risk rating	**Inherent: L=3 I=5 Total=15**	**Residual: L=3 I=3 Total=9**
Comment	High operational impact. Financial processes are critical, but workable manual mitigations exist. Further development will reduce risk.	

4.3. Golem

Function	Data synchronisation and scheduled tasks between systems. Bespoke C# application.
Current Position	This is a simpler system with readily understandable code base. Failure is less disruptive than other systems and it is generally robust and requiring little maintenance.
Key risks	• Failure would interrupt automated data flows and scheduled tasks. • Does not typically prevent systems from operating, but increases operational burden.
Short-term mitigations	• Manual transfer of key data between systems.

Medium to long-term mitigations	• Seek external technical support if internal expertise is unavailable.	
Overall risk rating	**Inherent: L=3 I=3 Total=9**	**Residual: L=2 I=2 Total=4**
Comment	Failure increases operational burden but does not prevent system operation. Manual data transfer significantly reduces impact.	

4.4. eVoting

Function	Elections platform. Laravel 9.x application with modernised features layered over a legacy system wrapped within a controller..	
Current Position	This is a critical bespoke system, with plans to shift to the third-party supported SUMS election platform to de-risk. SUMS is already available as an emergency platform in the event of failure while migration timeline is considered.	
Key risks	• High impact if unavailable during statutory election periods. • Reputational and governance risk if elections cannot be delivered reliably.	
Short-term mitigations	• Emergency transfer of elections to the third-party supported SUMS solution. • As a last resort, manual voting processes.	
Medium to long-term mitigations	• Full migration of elections to the third-party supported SUMS platform. • Retention of eVoting code repositories as fallback	
Overall risk rating	**Inherent: L=3 I=5 Total=15**	**Residual: L=2 I=3 Total=6**
Comment	High impact in the event of failure. Risk is actively reducing due to availability of a supported alternative.	

4.5. NewerPol SQL Server

Function	Core database feeding data into eActivities and SUMS.	
Current Position	Hosted, backed up and manageable via the university, with established ICT support arrangements.	
Key risks	• Database failure or corruption could result in temporary data loss or service interruption. • Dependency on university ICT response times and resilience.	
Short-term mitigations	• Immediate escalation to university ICT support. • Use of backups and rollbacks, acknowledging some risk of partial data loss.	
Medium to long-term mitigations	• Continued alignment with university database management and backup standards. • External specialist support if required for complex recovery scenarios.	
Overall risk rating	**Inherent: L=3 I=5 Total=15**	**Residual: L=2 I=3 Total=6**
Comment	Medium impact, low likelihood. Strong institutional controls reduce overall exposure.	

4.6. SUMS Integration (ISI)

Function	Integration layer between internal systems and the SUMS platform.
Current Position	This is a recently developed application to enable data flow into SUMS. The code repository is well documented and available via GitHub.
Key risks	• Failure would disrupt data exchange rather than core system availability. • Reliance on bespoke integration code.

Short-term mitigations	• Manual data transfer between systems where necessary.	
Medium to long-term mitigations	• External technical support or redevelopment if required. • Longer-term rationalisation of integrations as reliance on SUMS increases.	
Overall risk rating	**Inherent: L=3 I=4 Total=12**	**Residual: L=2 I=3 Total=6**
Comment	Medium impact, low to medium likelihood.	

5. General risk mitigation

The following general risk mitigations are in place:

- There are currently three staff with technical capability to diagnose and maintain systems.
- Recent efforts to spread technical knowledge and improve documentation materially reduce key-person risk.
- Bespoke system code is held in controlled GitHub repositories, providing version control, audit history and recoverability in the event of system failure or staff unavailability.
- Manual process fallbacks exist for all financially critical systems, though these increase workload and error risk.
- A general technical wiki is maintained within the SIT issue tracker.
- The increasing availability of third-party supported solutions (notably SUMS) provides a clear pathway to reducing bespoke system risk over time.

6. Summary

The union operates a small number of critical in-house systems that present identifiable single-point-of-failure risks. These risks are currently mitigated through documentation, shared technical knowledge, manual fallback processes and access to university and external support.

Notable risk relates to elections delivery, for which a clear mitigation pathway already exists through migration to a third-party supported platform. Overall, risks are understood, monitored and proportionately managed, with a credible route to further reduction over the medium term.