Project Status Report, Acme Manufacturing IRM

Introduction:

Acme Manufacturing requires more supply chain management flexibility, scaling production to match demand. Consequently, IT risk consultants (team four) have been retained to assess three Enterprise Resource Planning (ERP) solutions then assess the recommended solution's information risk. This status report provides the assessment recommendation, proposed risk management approach and disaster recovery solution overview to ensure ERP availability.

Approach

An ERP solution failure will cascade impacts throughout ACME's operations necessitating an information risk focused Enterprise Risk Management (ERM) assessment. The Open FAIR risk management framework will be used to extend the NIST Cyber Security Framework (CSF) (Fig. 2) beyond cyber security, allowing analysis of information risk receptors required for strategic business decisions (Carlson, 2016) like accurate data-based decisions or technical debt. Organizations are comprised of many subsystems in which information security risk can be created or realized (Fig. 1) (Hoffman et al 2016), Open FAIR enables the defensible measurement of that risk (Schmoller, 2020).

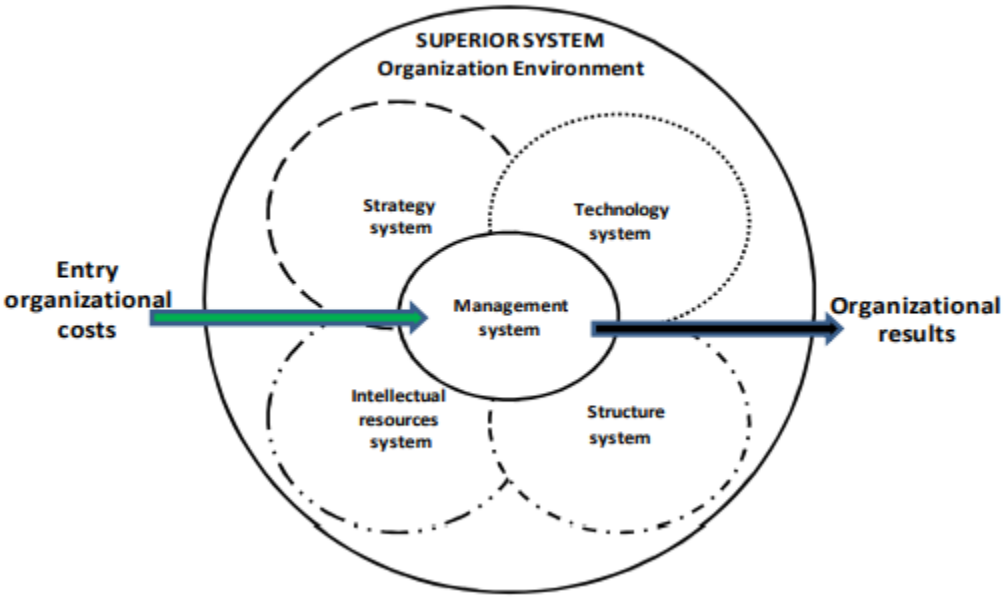


Figure 1 Organizational subsystems (Hoffman et al, 2016)

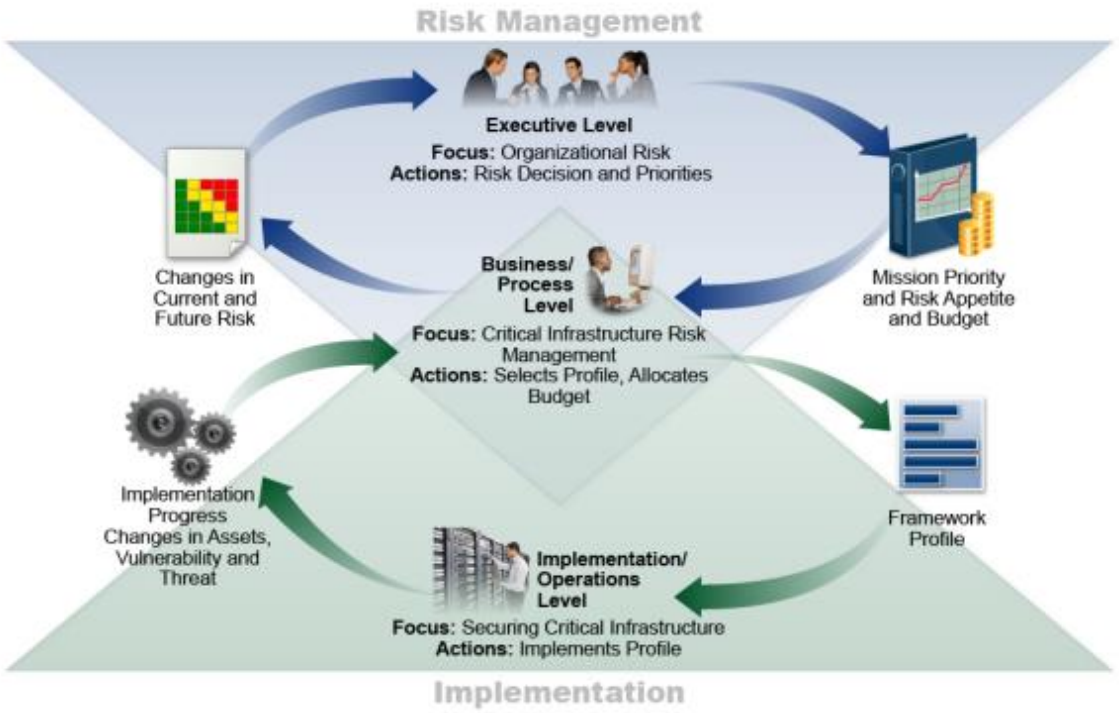


Figure 2 Open FAIR extension of NIST CSF (Carlson, 2016)

ERP Recommendation

Team four recommends ACME pursue the implementation of the commercial off the shelf (COTS) ERP solution as it provides the best balance of capabilities, supportability, and implementation effort for the lowest total cost of ownership over five to seven years.

ACME staff input was unavailable; therefore, to understand ACME's needs ERP solution requirements were identified through literature review (Iskanuis, 2010; Seo, 2013; Fruhlinger et al, 2020) and industry experience. Key requirements were assigned weighted values (Appendix 1), analysts independently scored how solution options met each requirement, then program evaluation and review technique (PERT) applied to the scores addressing potential estimate bias (Freund & Jones, 2014).

Project Deliverables

A cost benefit analysis of ERP solution options (see Appendix 1) and information risk assessment (see Appendix 2) of the recommended selection based on the following inputs:

- ERP critical success factors:
  - Feature capabilities align with ACME business priorities and processes
  - Data integration with external partners, internal manufacturing, and inventory systems
  - Granular access controls needed for accurate financials, production management, and fraud protection
  - Quick complete transition from identified legacy systems
  - Low total cost of ownership over five-to-seven-year period
  - Cyber security attack resistance

- Risk Assessment Methodology
    - Research ERP implementation risks
    - Identify credible threats to ACME information systems
    - Define scope of assessment
    - Estimate each risk's impact and frequency
    - Quantify expert assessments, reduce bias via PERT
    - Develop prioritized risk register, provide risk treatment recommendations
- Reporting Format
    - Decision factor summary
    - Selection criteria rationale
    - Selection scoring table
    - Information risk analysis of recommended solution

A disaster recovery solution design for restoring ERP capability within the four-hour recovery time objective (RTO) including:

- Conceptual architecture
    - Essential system components, primary and failover
    - Data replication strategy
- Recommended response plan
    - Response team roles and responsibilities defined
    - Breach reporting requirements identified
    - Potential ERP service disruption scenarios and responses
- Recommended Recovery Plan
    - Application recovery roles and responsibilities defined
    - Potential ERP service disruption scenarios and recovery measures
- Recommended Governance
    - Response and Recovery plan testing
    - Post-incident review for testing and actual incidents
    - Defined owners for response and recovery decisions
    - Service level agreements (SLA) and recovery timetables

Next Steps

Upon ACME's acceptance of the ERP solution recommendation team four will perform a comprehensive risk assessment using the earlier defined approach. A preliminary list of information risks based on team four's current understanding of ACME (Appendix 2) has been included for stakeholder review and amendment suggestions. In tandem with risk assessment activities, remediation controls based on NIST 800-53r5 (NIST, 2020) will be identified and ERP application recovery design will be completed.

The proposed project timeline is included (Appendix 3) for client review. Upon approval this schedule shall form the notice to proceed (NTP) for advancing the final report and recovery plan.

(Assumption – Schedule based on due dates in module info)

References

Carlson, C. (2016) *The Open FAIR - NIST Cybersecurity Framework Cookbook.* 1st ed. Reading, Berkshire: The Open Group.

Freund, J. & Jones, J. (2014) *Measuring and Managing Information Risk.* 1st ed. Waltham: Butterworth-Heinemann.

Fruhlinger, J., Wailgum, T. & Sayer, P. (2020) 16 famous ERP disasters, dustups and disappointments. Available from: https://www.cio.com/article/2429865/enterprise-resource-planning-10-famous-erp-disasters-dustups-and-disappointments.html [Accessed 21 August 2021].

Hoffmann, R., Kiedrowicz, M. & Stanik, J. (2016) Risk management system as the basic paradigm of the information security management system in an organization. MATEC Web of Conferences 76(1): 4 - 10

Iskanuis, P. (2010) Risk management of ERP projects in manufacturing SMEs. *Information Resources Management Journal,* 23(3), pp. 61-67.

National Institute of Standards (2020) NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. Available from: https://doi.org/10.6028/NIST.SP.800-53r5 [Accessed August 28, 2021]

Schmoller, D. (2020) Pros and Cons of the FAIR Framework. Available from: https://reciprocity.com/pros-and-cons-of-the-fair-framework/ [Accessed 2018 August 2021].

Seo, G. (2013) *Challenges in Implementing Enterprise Resource Planning (ERP) System in Large Organizations: Similarities and Differences Between Corporate and University Environment.* S.M. Thesis, Massachusetts Institute of Technology, Sloan School of Management. Available from: http://hdl.handle.net/1721.1/80683 [Accessed 27 August 2021].

Appendix 1

Details regarding the criteria considered for each functional and non-functional requirement have been removed due to space constraints. Criteria will be further explained in the final report.

Functional and Non-functional Requirements	Weighting	COTS	Opensource project	Internal development
Technical support availability	5	21.67	7.5	11.67
Security vulnerability fixes	4.5	16.5	9	9
Professional services support for ERP Implementation	4	16	5.34	4
Software security accountability	4	20	4.67	6
IT Staff requirements	3.875	18.08	7.75	3.875
System responsiveness	3.875	14.21	9.69	10.34
End of life transition options	3.75	12.5	8.13	7.5
Feature Development	3.75	13.13	6.25	8.125
Implementation time requirements	3.75	14.375	11.25	10
System integration, expansion, and growth	3.5	15.17	5.83	5.83
Alignment with ACME business processes	3.25	5.96	7.58	15.17
Damage recovery if ERP implementation fails or exposes ACME to liability	3.125	12.5	1.04	2.08
Total cost of ownership	3.0625	12.76	7.15	6.64
Reference installations to validate suitability	3	8	4.5	1
Requirements score		200.85	95.68	101.23

Appendix 2

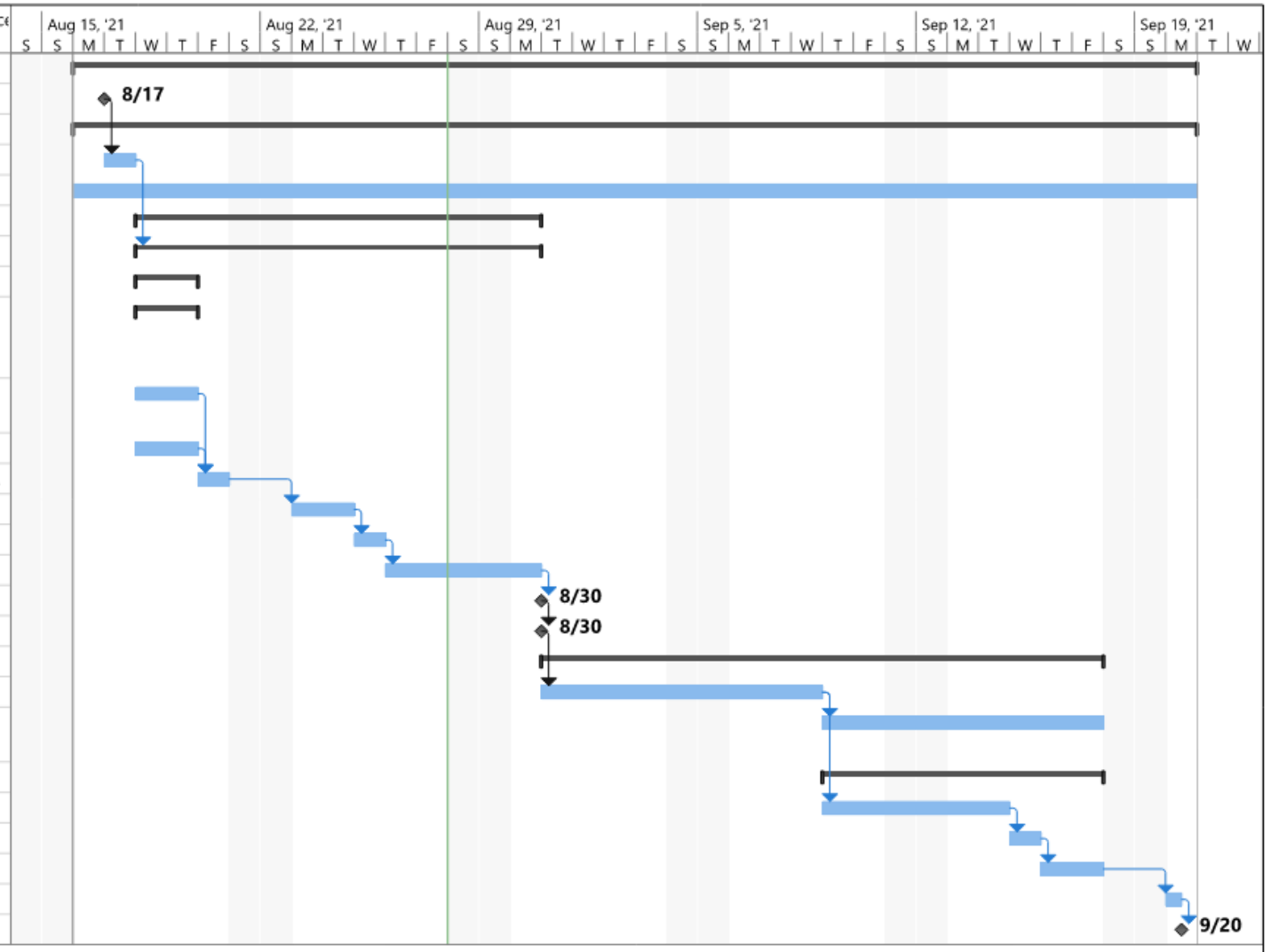
The information risks listed below have been completed without ACME stakeholder input. ACME leadership is encouraged to review the table to confirm key information risk concerns and receptors are identified.

Risk	Risk Receptor	Primary or Secondary Loss	Potential Impact Description
Initial customization creates future maintenance difficulties and technical debt	Operational, Financial, Reputational (including this team who recommended the selection)	Secondary	Limitations with the ERP selected can only be resolved through bespoke modifications
ERP software obsolescence due to vendor failure or development team failure	Operational, Financial, Reputational	Secondary	All software will become obsolete, which lifecycle management approach best fits ACME
Difficulty/inability to import or export data leads to solution lock-in or parallel systems	Loss of revenue, loss of efficiency/employee satisfaction	Primary	Existing organizational data must put into the ERP, data will need to be extract in the future when moving to a new platform
Lack of legal recourse to recover costs due to ERP implementation or performance failure	Financial	Secondary	Damage claims by ERP clients are not uncommon
ERP implementation delays lead to cost overruns	Financial	Primary	Existing business process(es) require ERP software configuration outside of standard implementation
Organizational change delays lead to cost overruns	Financial, reputational (internal stakeholders)	Primary	Business process changes to meet ERM requirements difficult to implement in various Acme business areas
ERP implementation requirements create resource conflicts with existing operational staff	Financial, reputational (internal stakeholders)	Primary	Current business operations need to run in parallel while new ERP is implemented, tested, and transferred into production
A data breach within the ERP system could result in customer record loss or compromise	Financial (fines, settlements) Reputation (customer confidence)	Primary & Secondary	Unauthorized access or release of PII or intellectual property

ERP developers can not produce vulnerability fixes at the rate Acme requires	Full Spectrum of risk based on exponential impact to multiple systems	Primary	Software updates will be needed to mitigate security vulnerabilities when they are discovered - Custom solutions result in delays (extended vulnerability timeframe)
ERP Developers fail to timely, discover, inform and patch for new vulnerabilities.	Full Spectrum of risk based on exponential impact to multiple systems	Primary	Security Patches are not implemented quickly enough to prevent a breach or exploited vulnerability
CIRT does not maintain high level of readiness through regular CIRT exercises in response/recovery.	Full Spectrum of risk based on exponential impact to multiple systems	Primary & Secondary	Response/recovery in real world incident is delayed and ineffective
ERP Developer does not offer Cyber Incident Response Team (CIRT) support	Full Spectrum of risk based on exponential impact to multiple systems	Primary	In-house staff must be trained in specialty skills or external cyber consultant retained to be part of CIRT
ERP implementation unavailable or unusable	Financial (productivity),	Primary	The system performance results in workers taking longer to perform their tasks than with the existing spreadsheet systems
Business decision errors resulting from incomplete or inaccurate data	Financial (forecasting, reporting)	Primary	The ERP may continue to generate data output that appears correct until reviewed by another party.
Customer service issues resulting from incomplete or inaccurate data	Reputation (customers: missed deliveries, invoicing mistakes) Financial (performance penalties)	Secondary	The ERP may continue to generate data output that appears correct until reviewed by another party.
Modifications to one ERP module unknowingly affect other modules resulting in incomplete or inaccurate data	Full Spectrum of risk based on exponential impact to multiple systems	Primary	Delay in discovery of erroneous data use or malware spread results in multiple system involvement, delayed response/recovery and potential fines or civil litigation

ACME IT department unable to adequately support ERP environment	Full Spectrum of risk based on exponential impact to multiple systems	Primary	Unplanned service disruptions to certain ERP capabilities or the entire system extend for hours, days or occur frequently in business hours
Limited benefits realization results in board of directors/investor confidence issue	Business operations, financial, reputational	Secondary	Implementation issues lead to only basic ERP capabilities in place or inability to retire some legacy processes
ACME staff slow or resistant to adopting ERP workflow	Business operations, financial, reputational	Primary	Users and business functions continue to rely on legacy spreadsheet mode of operation
ERP developers can not produce feature enhancements Acme requires	Business operations, financial, reputational	Primary	Changes to business operational requirements over time must be anticipated
ERP solution lacks adequately robust role-based access controls to enforce the segregation of duties required	Business operations, financial	Primary & Secondary	Segregation of duties is a key control for preventing fraud, misuse, or misallocation of enterprise resources
ERP solution lacks reporting capability for transactions that potentially violate segregation of duties controls	Financial, reputational (internal stakeholders)	Secondary	The ability to monitor transactions for potential issues and highlight those that must be manually reviewed is an important detective control

ID	Task Mode	Task Name	Duration	Start	Finish	Predece
1		**Acme Manufacturing ERP - IRM Project**	**26 days?**	**Mon 8/16/21**	**Mon 9/20/21**	
2		Primary Notice to Proceed (Team Formed)	0 days	Tue 8/17/21	Tue 8/17/21	
3		**Project Management Tasks**	**26 days?**	**Mon 8/16/21**	**Mon 9/20/21**	
4		Team Contract - Division of Duties	1 day?	Tue 8/17/21	Tue 8/17/21	2
5		Recurring Team Meetings	26 days?	Mon 8/16/21	Mon 9/20/21	
6		**Deliverables**	**9 days?**	**Wed 8/18/21**	**Mon 8/30/21**	
7		**Project Status Report**	**9 days?**	**Wed 8/18/21**	**Mon 8/30/21**	4
8		**Preliminary Work**	**2 days**	**Wed 8/18/21**	**Thu 8/19/21**	
9		**Select Recommended Implementation Model - COT, Open Source, Internal Development**	**2 days**	**Wed 8/18/21**	**Thu 8/19/21**	
10		Enterprise Risk Management Evaluation - Open FAIR	2 days	Wed 8/18/21	Thu 8/19/21	
11		Cost Benefit Analysis	2 days	Wed 8/18/21	Thu 8/19/21	
12		Outline Team Approach to IRM	1 day?	Fri 8/20/21	Fri 8/20/21	10,11
13		Describe Risk Assessment Methodology	2 days	Mon 8/23/21	Tue 8/24/21	12
14		Discuss Selection of Controls Methodology	1 day	Wed 8/25/21	Wed 8/25/21	13
15		Discuss Approach to System Recovery	3 days	Thu 8/26/21	Mon 8/30/21	14
16		Submit Status report	0 days	Mon 8/30/21	Mon 8/30/21	15
17		ACME approval to proceed per project status rep	0 days	Mon 8/30/21	Mon 8/30/21	16
18		**Comprehensive Risk Assessment Report**	**14 days**	**Tue 8/31/21**	**Fri 9/17/21**	
19		Review of Risk Assessment Methodology	7 days	Tue 8/31/21	Wed 9/8/21	17
20		Table of Identified Risk with Recommended Controls	7 days	Thu 9/9/21	Fri 9/17/21	19
21		**Disaster Recovery Solution Design**	**7 days**	**Thu 9/9/21**	**Fri 9/17/21**	
22		Approach to Disaster Recovery	4 days	Thu 9/9/21	Tue 9/14/21	19
23		Discussion of RPO and RTO	1 day	Wed 9/15/21	Wed 9/15/21	22
24		Presentation of High-level Design	2 days	Thu 9/16/21	Fri 9/17/21	23
25		QC/QA of final Report	0.5 days	Mon 9/20/21	Mon 9/20/21	24
26		Submission of Final Report	0 days	Mon 9/20/21	Mon 9/20/21	25



Project: ACME IRM Project
Date: Sat 8/28/21

Task	Project Summary	Manual Task	Start-only	Deadline
Split	Inactive Task	Duration-only	Finish-only	Progress
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress
Summary	Inactive Summary	Manual Summary	External Milestone

Appendix 3
Project Schedule