Project Final Report, Acme Manufacturing IRM

# Recommendation Decision Factor Summary:

ACME’s initial request for an Enterprise Resource Planning (ERP) system highlighted the need for supply chain management flexibility when modifying production levels to meet demand. Therefore, the project team’s assumes ACME’s primary business focus is manufacturing with a cost focused competitive strategy (University of Cambridge Institute for Manufacturing, n.d.) and information technology (I.T.) is a supporting rather than innovating business function (Jafari, 2014). COBIT 2019 recommends three I.T. governance and management objectives for companies pursing a cost leadership strategy: resource optimisation (EDM04), I.T. budget management (APO06) and vendor management (APO10) (ISACA, 2018).

### Cost Benefit Analysis

ERP solution requirements weighted highly by the team align with COBIT 2019 guidance and literature review of ERP implementation challenges (Iskanius, 2010; Seo, 2013; Fruhlinger et al, 2020), supporting the solution recommendation. Requirements were individually scored then balanced using program evaluation and review technique (PERT) analysis (Freund & Jones, 2014) to remove bias (Team 4, 2021a).

Implementing and maintaining an ERP solution will require additional technology workers; economic trends (Fig. 1) confirm cost management threats to ACME’s competitive position. (CompTIA, 2021). Consequently, requirements were scored within the context of ACME I.T. efforts for initial implementation and maintaining the solution going forward

|  |  |
| --- | --- |
|  |  |

Figure 1 Technology worker cost and availability trends (CompTIA, 2021)

All scoring and requirements assessed are available online for ACME stakeholder review with the following requirements identified as most impactful to implementation and long-term operational success. A commercial off the shelf implementation scored consistently higher than either the open source or fully internal development approaches.

* Technical Support availability
* Security vulnerability fixes
* Professional services support for ERP Implementation
* Software Security Accountability
* IT Staff requirements

### Selection Risk Analysis

COTS solutions allow service level agreements (SLA) to be defined for technical support, hyper care during disaster recovery situations, software fixes for security issues, functionality bugs and version upgrades. Installation and maintenance phases of the software development lifecycle (SDLC) are timelier and more cost effective with COTS solutions since both alternative solutions require ACME I.T. staff to resolve all issues with no recourse for delays.

A COTS solution also reduces cost savings and risk during the SDLC development and testing phases because ACME does not require development or security testing capacity in-house. The same cannot be said for internally developed or open-source solutions as cybersecurity and development resources command a premium within the tight technology labour market, threatening cost competitiveness.

Commercial software and support contracts align with the NIST CSF Tier 2 - Risk Informed implementation (NIST, 2021). The provider is accountable for assuring ERP information confidentiality and integrity during normal operations. It is recommended ACME ensure sufficient oversight and legal advice on software development practices, commitments, and vulnerability management history, during vendor contract negotiations.

# ERP Project Risk Assessment:

The project status report identified critical success factors for implementation and ongoing operations as well as risk assessment methodology. ERP systems affect the entire organization, therefore business cases focused on organizational fit, operational disruption risks during cost/benefit analysis. The previous status report (Team 4, 2021b) and supporting data have been archived online for ACME stakeholder review with hyperlinks provided in the references section.

After ACME’s approval of the ERP solution recommendation the project team assessed the top information risks identified in the status report with required assumptions based on operational needs and risk tolerance of a manufacturing organization. The ISO 27001 “Top 10” (Biscoe, 2017) (Table 1) was also reviewed to ensure common cyber security threats were considered. Whereas the ERM risks in figure 3 support the business case decisions, ISO 27001 risk in table 1 represent the common cybersecurity risks that should be protected against by the vendor throughout the product lifecycle. It is recommended that ACME include this support in the vendor SLA and include benchmarks for security patching and firmware upgrades.

Due to time constraints, no similar implementation precedent and lack of ACME financial data, quantifiable information related to risk outcomes is not available. Therefore, the Open FAIR risk assessment framework (The Open Group, 2020) was selected to assess information risks pertaining to ERP implementation and operation due to its flexibility (Schmoller, 2020) when calculating risks to inform business decisions without quantifiable data (Fig. 2).

Diagram

Description automatically generated

Figure 2 Open FAIR risk taxonomy abstraction (The Open Group, 2020)

### Qualitative Data Assumptions:

* 10 Monte Carlo simulations (Freund & Jones, 2014) due to limited underlying factor data
* Minimum and maximum impact values ensured widest reasonable loss magnitude range
* PERT applied to loss event frequency, ensuring only loss magnitude variability calculation

Without financial quantification, risks with highest consequence or likelihood can be prioritized by median or maximum risk scores (Fig. 3) to drive project governance, assuming best-case and worst-case impacts reside within the minimum and maximum qualitative project team member estimates.

### ERM Implementation Top Risks:

Monte Carlo simulations performed for Open FAIR analysis consistently identified the highest potential risk in three areas: cybersecurity, data quality and integrity, and system functionality (Fig 3).

The ERP solution will store and potentially exchange customer and business partner data, a breach of which could result in fines and permanent revenue loss. Extensive attention to cybersecurity controls during implementation design and penetration testing post installation (National Cyber Security Center, n.d.) are critical risk mitigations. Data quality issues within ERP can be hard to detect via unit testing, therefore extensive user acceptance testing (UAT) be completed with business users, including legacy system parallel processing to validate results is recommended. ERP systems require effort to fully bring online, often resulting in delays, functionality, and performance issues (Seo, 2013). Recommended risk mitigations are strong project management practices, especially for vendor selection, defining requirements, system design and UAT.

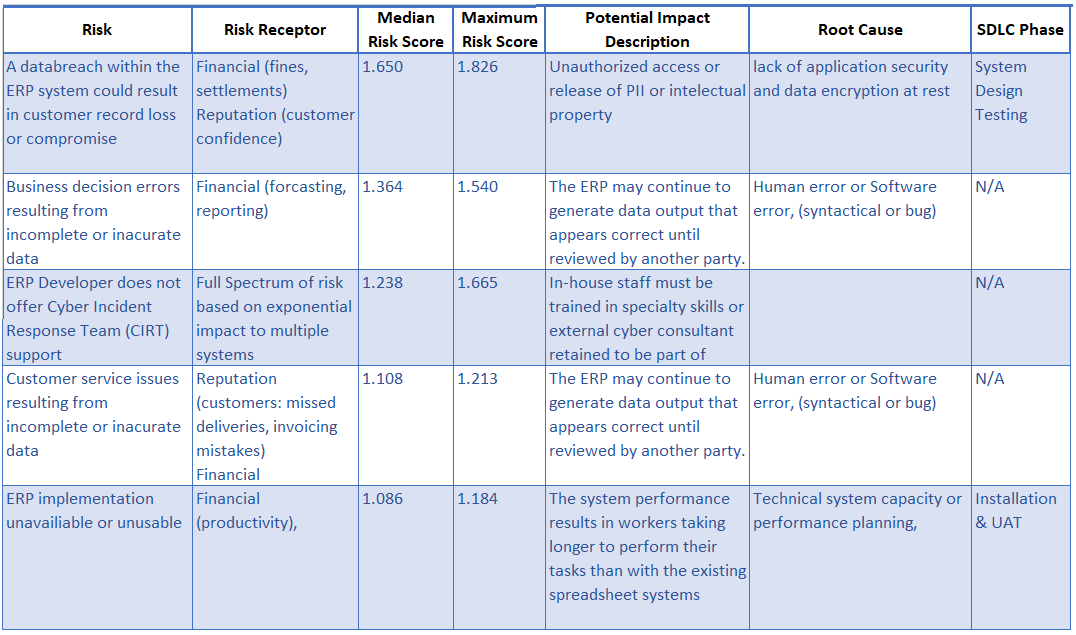


Figure 3 Top ERM risks

The *ERM Assessment Summary* (Team 4, 2021c), is a complete list of all ERM risks, risk receptors, impact descriptions and recommended controls. Since project management can align to SDLC phases, when applicable, SDLC phases have been associated to ERM risks identifying the potential need for additional governance (Fig. 4).

Figure 4 Risks by SDLC category



Table 1 ISO 27001 Top 10 Cybersecurity Risks and Recommended Controls

# Disaster Recovery Plan:

The presented plan refers to the recovery of the ERP application, thus it does not include scenarios related to outage of the on-premises infrastructure (Fig. 2) beyond the ERP system, it is considered an application recovery plan (ARP) rather than a comprehensive disaster recovery plan (DRP). Within the ARP context it is assumed a commercial ERP solution designed for small to medium enterprises such as Microsoft Dynamics 365 ERP is implemented rather than a large-scale ERP such as SAP or Oracle Fusion Cloud ERP.

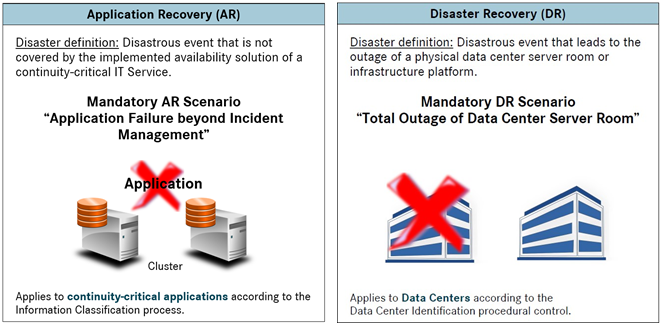


Figure 5 Application Recovery and Disaster Recovery definitions

Reduction in recovery time is inversely proportional to cost (Fig. 6), therefore ACME must determine how long they can reasonably expect to operate without an ERP solution. The business impact assumption is ERP failure will not affect ACME manufacturing capabilities for at least 24 to 48 hours, resulting in a combined warm standby, cold standby (Sutton, 2014) approach. The on-premises ERP database and supporting systems will utilize cloud backup technology to meet the fifteen-minute recovery point objective (RPO) and resilience requirements. A prebuilt virtual private cloud environment will be actively maintained, and ERP virtual servers built on demand using pretested system build scripts, commonly called *infrastructure as code.* Rebuilding systems on demand may possibly exceed the four-hour recovery time objective (RTO) by a few hours but will cost more than four thousand dollars a month to maintain a complete warm standby environment in the cloud (Table 2). There is a modest ongoing operational cost to maintaining an active private cloud environment to enable faster recovery when needed as well as an on-demand test environment for periodic upgrades and ARP validation.

A picture containing text, electronics

Description automatically generated

Figure 6 Recovery strategies

|  |  |  |  |
| --- | --- | --- | --- |
| Cost of High Availability Infrastructure (On-Premises / IaaS) | | | |
| **Equipment** | **Specifications** | **On-Premises Infrastructure** | **Cloud** |
| Application Server | CPU: 4x4 core  RAM: 32-64 GB  Storage: 128 GB |  | $ 525,60 / Month |
| Web Server | CPU: 2x4 core  RAM: 32 GB  Storage: 128 GB |  | $ 525,60 / Month |
| Database Server | CPU: 2x8 core  RAM: 128 GB – IO Optimized  Storage: 1 TB |  | $ 3,431 / Month |
| **Total** |  | **$ 1069/ month** | **$ 4,482.20 / Month** |

Table 2 Infrastructure pricing (Dell, 2021; Microsoft 2021)

## Solution design overview

The ERP conceptual architecture provides performance, resilience, and core ERP component protection from cyber-attacks from within ACME local area networks, through virtualization and network segmentation. The hybrid architecture incorporates on-premises equipment for the primary ERP solution with application recovery utilizing commercial cloud infrastructure, pre-provisioning measures and cloud storage for data backup and system recovery. Assuming ERP access is normally from internal networks, on-premises costs less than comparable cloud infrastructure with fewer connectivity and latency issues associated with internet hosted systems. Virtualization technologies enable hosting presentation and application systems on modest server hardware at lower capital and environmental costs than running each system on individual hardware (Belanger & Casemore, 2019). Virtualization savings also allow fully redundant hardware for additional on-premises resilience (Fig 4) for less than Diagram

Description automatically generatednon-redundant dedicated servers (Dell, 2021).

Figure 7 ERP Hybrid Resilience

To thwart modern adversarial activity, utilize TLS communications and isolate ERP servers from user networks with firewalls (Paloalto Networks, 2021). Place ERP components in different zones with interzone communications protected via VLAN specific policies within a Next Generation firewall. Additionally, cloud storage communications should take place over dedicated private circuits isolating backup traffic from ERP users and reducing segmentation firewall load (Fig. 5).



Figure 8 User LAN and zone segmentation

## Application Recovery Scenarios

A supporting framework needed for comprehensive application recovery planning is available online (Team 4, 2021d). ACME IT staff and senior leadership must understand expectations and requirements for restoring ERP solution service quickly. The following high level event scenario descriptions define both the boundaries of the plan as well as incident response capability assessment candidates.

|  |  |  |
| --- | --- | --- |
| **SID** | **Scenario Name** | **Scenario Enablers** |
| A1 | Web server failure beyond incident management | * *Human factor (malicious or accidental)* * *Extensive on premises hardware failure* * *Denial of service (malicious, accidental, or environmental)* * *Ransomware infection* |
| A2 | Application server failure beyond incident management | * *Human factor (malicious or accidental)* * *Extensive on premises hardware failure* * *Denial of service (malicious, accidental, or environmental)* * *Ransomware infection* |
| A3 | Database server failure beyond incident management | * *Human factor (malicious or accidental)* * *Extensive on premises hardware failure* * *Denial of service (malicious, accidental, or environmental)* * *Ransomware infection* |
| A4 | Data loss/corruption beyond incident management | * *Human factor (malicious or accidental)* * *Ransomware infection* |

# References

Belanger, S. & Casemore, B. (2019). Exploring the Impact of Infrastructure Virtualization on Digital Transformation Strategies and Carbon Emissions. Available from: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/company/vmware-exploring-impact-of-infrastructure-virtualization-on-digital-transformation-strategies-and-carbon-emissions-whitepaper.pdf [Accessed 13 September 2021].

Biscoe, C. (2017). Top 10 threats to include in an ISO 27001 risk assessment. 27 June 2017. *IT Governance*. Available from: https://www.itgovernance.co.uk/blog/top-10-threats-to-include-in-an-iso-27001-risk-assessment [Accessed 28 August 2021].

CompTIA (2021). *Cyberstates 2021*. Downers Grove, Il: CompTIA. Available from: https://www.cyberstates.org/pdf/CompTIA\_Cyberstates\_2021.pdf [Accessed 14 September 2021].

Dell (2021). PowerEdge R740 Rack Server. Available from: https://www.dell.com/en-us/work/shop/servers-storage-and-networking/poweredge-r740-rack-server/spd/poweredge-r740/pe\_r740\_12248a\_vi\_vp?configurationid=cf3134a9-cdd6-4021-8568-489959668799 [Accessed 4 September 2021].

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].

ISACA (2018). *Cobit 2019 Framework Introduction and Methodology*. 1st ed. Schaumburg, Il: ISACA.

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

Jafari, S. M. (2014). Strategic Cost-Cutting in Information Technology: toward a Framework for Enhancing the Business Value of IT. *Iranian Journal of Management Studies* 7(1), pp. 21-39. Available from: https://doi.org/10.22059/IJMS.2014.36201 [Accessed 16 September 2021].

Microsoft (2021) Pricing calculator. Configure and estimate the costs for Azure products. Available from: https://azure.microsoft.com/en-us/pricing/calculator/ [Accessed 19 September 2021].

National Cyber Security Center (n.d). Penetration Testing. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 5 July 2021].

NIST (2021). An Introduction to the Components of the Framework. Available from: https://www.nist.gov/cyberframework/online-learning/components-framework [Accessed 16 September 2021].

Paloalto Networks (2021). *Use Case: Apply Network Segmentation to a Traditional Data Center.* Available from: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\_US/resources/whitepapers/apply-network-segmentation-traditional-data-center [Accessed 12 September 2021].

Schmoller, D. (2020). Pros and Cons of the FAIR Framework. Available from: https://reciprocity.com/pros-and-cons-of-the-fair-framework/ [Accessed 18 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].

Sutton, D. (2014). *Information Risk Management: A practitioner’s guide*. Swindon: BCS, The Chartered Institute for IT.

Team4 (2021a). ACME Cost Benefit Analysis. Available from: https://irmteam4.github.io//Cost\_Benefit\_Analysis-scoring-presentation.xlsx [Accessed 19 September 2021].

Team4 (2021b). Project Status Report, Acme Manufacturing IRM. Available from: https://irmteam4.github.io/ACME\_IRM\_Project\_Status\_Report.pdf [Accessed 19 September 2021].

Team4 (2021c). ACME ERM Risk Summary. Available from: https://irmteam4.github.io/ACME\_ERM\_Risk\_Summary.xlsx [Accessed 19 September 2021].

Team4 (2021d). Application Recovery Plan. Available from: https://irmteam4.github.io/IRM\_GRP4\_ApplicationRecoveryPlan.pdf [Accessed 19 September 2021].

The Open Group (2020). *The Open Group Standard Risk Taxonomy (O-RT), Version 3.0*, Berkshire: The Open Group. Available from: https://www.opengroup.org/forum/security/riskanalysis [Accessed 19 September 2021].

University of Cambridge Institute for Manufacturing (n.d). Porter's Generic Competitive Strategies (ways of competing). Available from: https://www.ifm.eng.cam.ac.uk/research/dstools/porters-generic-competitive-strategies/ [Accessed 14 September 2021].