EVA Calculation

Task	Planned Effort	Actual Effort
1	15	15.8
2	17	13
3	4	6
4	22	19.3
5	12	17
6	11	19
7	13	9.6
8	10	16
9	20	24
10	23	18
11	8	
12	15	
13	19	
14	14	
15	7	

Total Task = 66, Effort Estimated= 315 Person Day

BAC = 315, ACWP = 157.7, BCWS = 210, BCWP = 147

SPI = BCWP/ BCWS = 147 / 210 = 0.7

SV = BCWP – BCWS = 147 – 210 = - 63 person- day

CPI = BCWP/ ACWP = 147 / 157.7 = 0.93

CV = BCWP- ACWP= 147 – 157.7 = -10.7 or -11 person-day

% Schedule for completion = BCWS/ BAC= 210 / 315 = 66.66%

[% of work scheduled should have been done at this time]

% complete = BCWP/ BAC = 147 / 315 = 46.66%

[% of work completed at this time]

BUILDING RISK TABLE:

Risk Description	Impact	Probability	Category	RMMM
Regulatory Compliance Issues	2	70%	PR	Mitigation: Regularly consult with legal and compliance experts. Monitoring: Conduct compliance audits at each project phase. Management: Adjust policies and procedures based on legal advice and regulatory updates.
System Downtime	2	60%	DE, TE	Mitigation: Implement redundancy and failover systems. Monitoring: Continuously monitor system performance. Management: Develop and execute a quick recovery plan to minimize downtime.
User Resistance/Training	3	80%	CU	Mitigation: Provide comprehensive user training early and often. Monitoring: Gather and act on user feedback regularly. Management: Adjust training methods and include usability enhancements based on user input.
Data Loss	2	50%	TE	Mitigation: Implement automated backups and disaster recovery plans. Monitoring: Regularly test data recovery systems. Management: Develop rapid response plans to minimize loss if data loss occurs.
Inadequate Scalability	2	60%	DE, TE	Mitigation: Design systems for scalability from the start. Monitoring: Track system performance metrics regularly. Management: Plan for scaling up infrastructure and services based on demand growth.
Data Breach/Security Compromise	1	40%	PR, DE	Mitigation: Implement robust encryption and access controls. Monitoring: Perform regular security audits and penetration tests. Management: Have an incident response plan in place in case of breach.
Unforeseen Technological Changes	3	50%	TE	Mitigation: Implement robust encryption and access controls. Monitoring: Perform regular security audits and penetration tests. Management: Have an incident

				response plan in place in case of breach.
Insider Threats	2	30%	ST	Mitigation: Implement strict access controls and monitoring for insider activity. Monitoring: Regular employee activity audits. Management: Have contingency plans for dealing with insider threats, including rapid investigation procedures.
Lack of Penetration Testing	3	70%	PR, DE	Mitigation: Schedule periodic penetration tests and vulnerability assessments. Monitoring: Track test results and address vulnerabilities. Management: Incorporate penetration testing into routine security management practices.
Technical Compatibility Issues	3	60%	DE	Mitigation: Ensure thorough testing of integrations between systems. Monitoring: Conduct regular compatibility checks. Management: Allocate additional time and resources for resolving compatibility issues.
Integration Challenges	2	70%	DE, TE, ST	Mitigation: Plan early for integration tasks and allocate adequate resources. Monitoring: Regular integration testing and reviews. Management: Adjust timelines and resources for complex integration phases.
Inaccurate Price Calculations	2	80%	TE	Mitigation: Use automated systems for price calculations and validations. Monitoring: Periodic audits of pricing algorithms and results. Management: Have backup systems in place for manual validation or correction of calculations.
Performance Degradation	3	50%	TE	Mitigation: Implement performance monitoring tools and optimizations. Monitoring: Continuously monitor system performance under varying loads. Management: Optimize infrastructure and refactor code to improve performance.
Lack of Documentation	3	40%	PR	Mitigation: Assign dedicated resources for documentation. Monitoring: Review documentation progress regularly. Management: Set documentation standards and deadlines to ensure completeness and accuracy.
Economic/Political Changes	1	40%	BU	Mitigation: Stay informed about relevant economic and political

				factors. Monitoring: Regularly assess the project's financial health and potential political impact. Management: Adjust project timelines and budget based on economic conditions.
Changing Customer Needs	2	50%	CU	Mitigation: Use agile development methods to accommodate changing requirements. Monitoring: Regular feedback loops with customers to ensure alignment. Management: Prioritize and adjust the scope based on evolving customer needs.
Vendor/Supplier Reliability	3	70%	PR, TE, ST	Mitigation: Maintain strong communication with suppliers and have backup vendors. Monitoring: Regular vendor performance reviews. Management: Develop contingency plans for supplier failures or delays.
Skill Shortages	2	60%	ST	Mitigation: Upskill current employees and have a clear hiring strategy. Monitoring: Track team skills and project needs. Management: Allocate resources for training and recruitment of required expertise.
Budget Overruns	2	80%	BU	Mitigation: Set realistic budgets and build in contingencies. Monitoring: Regular budget reviews and expense tracking. Management: Reprioritize project tasks or secure additional funding if necessary.

Impact values:

1 - Catastrophic
2 - Critical
3 - Marginal
4 – Negligible

Allocation:

Project Management:

Project Manager: Oversees the entire project, ensuring proper planning, coordination, stakeholder communication, and risk management strategies are applied.

Legal Compliance Officer: Ensures that the project complies with regulatory requirements and that legal concerns are addressed throughout the project lifecycle.

Development Team:

System Architect: Designs the scalable system architecture to ensure it can handle anticipated load and accommodate future growth.

Backend Developer: Develops the backend systems, including database interactions and API integrations.

Frontend Developer: Implements user interfaces for the web and mobile platforms, ensuring they are user-friendly and intuitive.

Database Administrator: Manages the system's database, ensuring data integrity, security, and scalability.

Mobile App Developer: Develops the mobile application for end-users to access system functionalities.

Security Specialist: Implements robust security measures to mitigate risks such as data breaches and insider threats, ensuring compliance with best practices and regulations.

Integration Specialist: Manages the technical integration between various system components to ensure compatibility and smooth functioning.

Testing and Quality Assurance:

QA Lead: Manages all quality assurance activities, ensuring the system meets functional, security, and scalability requirements.

Test Analyst: Develops and executes test plans for functional, security, and integration testing.

QA Engineers: Assist in functional, security, performance, and penetration testing, ensuring thorough coverage of potential vulnerabilities.

Deployment and Maintenance:

Deployment Manager: Oversees the deployment process, ensuring that scalability and downtime risks are mitigated, and coordinates with system administrators.

System Administrators: Manage the infrastructure, ensuring uptime, security, and system performance. They monitor for hardware failures and execute timely replacements.

Deployment Engineers: Assist in rolling out updates and patches to the system while ensuring minimal downtime and maintaining data integrity.

Customer Support and Training:

Training Specialist: Provides training resources and guides to ensure that both end-users and internal teams are properly trained, mitigating risks of user resistance.

Support Engineers: Provide technical support, address user feedback, and resolve system issues. They also ensure that customer needs and requirements are met and help maintain high user satisfaction.

Security and Compliance:

Compliance Officer: Ensures that all legal and regulatory requirements are adhered to, conducts regular audits, and coordinates with development teams for compliance adjustments.

Incident Response Team: Dedicated team for addressing security breaches and data loss, responsible for mitigating any immediate damage and communicating with stakeholders.

This structure emphasizes proper risk handling for scalability, security, compliance, and user support.