Critical Thinking Module 3: Webpage Deployment Scope Management

Alexander Ricciardi

Colorado State University Global

CSC501: Management for the Computer Science Professional

Dr. Brian Holbert

November 30, 2025

Critical Thinking Module 3: Webpage Deployment Scope Management

The organization has decided to deploy a new customer-facing webpage to showcase our new 3D printers, as well as filament and spool products. This necessitates the development of an e-commerce platform, whose success relies not only on the timely completion of the development project but also on the quality, robustness, integrity, and security established within a defined project scope. Therefore, managing the project scope is crucial for the success of the project. This document discusses the development process of the project's Management Scope plan, explains the inputs, tools, techniques, and outputs that will be part of the webpage deployment, and discusses a project lifecycle plan, development approach, and some of the tools and techniques that may be utilized in the deployment process. It also discusses possible security issues with the site, hardware, and configuration.

Designing the Scope Management Plan

Scope Management is the process of managing a project scope by defining the boundaries of the project, by defining what is included, and what is excluded (Ucertify, n.d.). On the other hand, designing a Scope Management Plan (SMP) is the process of creating a plan that defines and manages what is included in a project. Consequently, if a procedure or a feature is not mentioned in the plan is not mentioned by the plan, it is excluded from the scope. Nonetheless, an effort can be made by explicitly listing specific exclusions, for instance, listing that for this project, the physical logistics for shipping and warehousing products are excluded from this project as they are exclusively managed by the Operations department, not the Marketing Department. In other words, designing the SMP involves clearly defining the project scope, the project boundaries, and its role in managing the scope, ensuring that it is and stays aligned with the project requirements. This is important for the success of the project, as without

a clear and documented understanding of a project scope, the project is at risk of uncontrolled expansion of work (Scope Creep, e.g., adding not-scheduled and not-budget features to the webpage) or additions to a feature initiated by the team (Gold-Plating, e.g., adding a feature to the webpage that was not requested) both of which can create to project delays and budget overruns jeopardizing the project deployment.

Inputs, Tools, Techniques, and Outputs (ITTOs)

The planning of the SMP is guided by a series of Inputs, Tools, Techniques, and Outputs (ITTOs). ITTOs are a set of management tools associated with the Project Management processes detailed in the Project Management Body of Knowledge (PMBOK) guide (Project Management PrepCast, n.d.).

An input is an item required by a process before that process can proceed (Project Management PrepCast, n.d.). For this project, before proceeding with the SMP, a Project Charter is needed, as it can provide a high-level description (input) of the project itself and its products (e.g., the 3D printers, filaments, and spools). Other input requirements needed to design the SMP are Enterprise Environmental Factors (EEFs), such as the Payment Card Industry Data Security Standard (PCI DSS), which are regulations dictating how to securely process transactions (payments) (PCI, 2022). For example, for filaments or printers' customer purchases. These regulatory standards are project constraints that define security features requirements. An additional useful input for designing the SMP, which is usually found in the Organizational Process Assets (OPAs), is lessons learned from previous IT deployments. It provides valuable deployment information (requirements) that prevent repeating errors.

Modern web deployment can be a very complex process; having Tools and Techniques such as templates and defined systematic procedures to design the SMP is essential for ensuring

the quality of the plan (Project Management PrepCast, n.d.). For example, having procedures such as consulting Expert Judgment guidance for cybersecurity architects, identifying potential security threats, and e-commerce experts to identify Non-Functional Requirements (NFRs) such as load capacity and transaction speed. Furthermore, having Data Analysis tools, specifically Alternatives Analysis, is useful for defining the viability of different deployment scopes; for example, evaluating whether the project needs to build a custom backend or customize an off-the-shelf platform (e.g., Shopify or Magento) (MyQuests, n.d.).

Outputs are the results or services generated by a process (Project Management PrepCast, n.d.). The outputs are typically integrated into the design process of SMP itself, as the SMP dictates the protocol used for processing scope changes (the expected outputs from processes). In addition, a Requirements Management Plan can help define how requirements and their outputs will be prioritized and tracked throughout the project lifecycle. For example, the Requirements Traceability Matrix (RTM) is an output document that tracks requirements from their origins and follows them throughout the project life cycle (Ucertify, n.d.).

Project Lifecycle and Development Approach

A Hybrid Adaptive Life Cycle model is the best-suited approach for deploying this project, as a purely predictive (Waterfall) model is too rigid for the fast-paced changes that often occur in web design, such as gathering User Experience (UX) requirements changes, and a purely Agile model prioritizing change over security, lacking the tools to appropriate manage the financial regulations and web security implementations. Therefore, this hybrid strategy requires that the backend infrastructure and security layers deployment be orchestrated using a Predictive approach, utilizing tools such as Work Breakdown Structure (WBS). WBS can manage tasks such as server hardening, database schema design, and PCI audit preparation. This approach is

necessary, for instance, when implementing security features that need to adhere to PCI DSS rigid mandates, which leave no room for ambiguity. On the other hand, for the frontend deployment, especially for UX development, the hybrid strategy requires an Adaptive (Agile) approach. This approach can use tools and techniques such as User Stories (e.g., “As a user, I want to filter filaments by material type”) and iterative sprints, allowing the deployment/developing team to rapidly prototype UX features or apply changes based on user feedback without disrupting the security infrastructure of the project.

Security Issue: Hardware and Configuration

The development of the SMP and the choice of using the Hybrid Adaptive Life Cycle model are heavily influenced by the Security feature of the project. The Security feature is a core component of the project scope. Thus, identifying and understanding the requirements associated with it and properly managing the development of it are essential for the successful deployment of the webpage. Analysis of the deployment reveals that the project scope must incorporate security across three layers, which are application, hardware, and configuration. At the application layer, the scope must include “Secure-by-Design” requirements that diminish risks such as Insecure Direct Object References (IDOR), used by attackers to manipulate URLs and access customer orders (CISA, 2023). At the hardware infrastructure layer, whether on-premise or cloud-based, requires managing distinct development work tasks for “hardening” the security of the hardware infrastructure, tasks such as disabling unnecessary ports and services to reduce the infrastructure attack surface. Finally, at the configuration layer, the SMP must implement Integrated Change Control for all configurable items to prevent configuration drift. For example, by implementing and undergoing an approval process, it ensures that any change to the payment features process, firewall settings, or server permissions is authorized and aligns with the overall

configuration of the project (MDN, n.d.). These processes will keep the webpage site secure post-deployment.

Conclusion

For a successful deployment of the new customer-facing webpage, it is essential to design an SMP that integrates clear project boundaries and prevents Scope Creep and Gold-Plating by using the standard ITTO framework provided by the Project PMBOK. Additionally, to manage the project scope and deployment, a Hybrid Adaptive Life Cycle model is best suited, as it provides a balance between the Agile approach flexibility, to manage the deployment of the frontend, and a predictive approach to manage the deployment of the backend infrastructure and security layers. Furthermore, these processes allow addressing hardware, configuration, and security issues across all infrastructure layers, ensuring the integrity, efficiency, and safety of the customer-facing webpage post-deployment.

References

CISA. (2023, July 27). *Preventing Web Application Access Control Abuse*. Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-208a

MDN. (n.d.) *Website security.* Mozilla. https://developer.mozilla.org/en-US/docs/Learn_web_development/Extensions/Server-side/First_steps/Website_security

MyQuests. (n.d.). *E-Commerce Optimisation and Conversion for eShop*. MyQuests. https://myquests.org/services/e-commerce-optimisation-and-conversion-for-eshop/

PCI. (2024, June). *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0.1.* PCI Security Standards Council, LLC. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Project Management PrepCast. (n.d.). *The Complete Guide to PMP ITTO (Advanced Guide & Review)*. OSP International LLC. https://www.project-management-prepcast.com/pmp-itto

Ucertify (n.d.). Lesson 6: Project Scope. Project Manager Professional (PMP) Based on PMBOK7. Ucertify. ISBN: 978-1-64459-415-5