Description of document:	Peace Corps Information Technology (IT) Project Risk Management Plan, 2016 and Intranet Modernization project, 2017
Requested date:	July 2017
Release date:	21-December-2017
Posted date:	07-January-2019
Source of document:	Freedom of Information Act Request FOIA Officer U.S. Peace Corps 1111 20th Street, NW Washington D.C. 20526

Since 1961.

December 21, 2017

RE: FOIA Request No. 17-0145

This is in response to your Freedom of Information Act (FOIA) request, which consists of two points. Both appear below, and each point is followed by our response in bold-type.

"I request a copy of the risk assessment strategy for new IT projects."

We have material which is responsive. Attached, please find a copy of "Risk Management Plan" (9 pages) with "Appendix A" (3 pages). No information has been withheld.

"I also request a copy of the plan for modernization of the Peace Corps INTRANET (internal employee website)."

We have material which is responsive. Attached, please find a copy of "2017 Intranet Modernization" (9 slides). We note that certain information has been withheld pursuant to 5 U.S.C. §§ 552 (b)(5). Exemption 5 protects records with information that is deliberative and pre-decisional; it is input to a future round of project design.

If you are not satisfied with this response, you may administratively appeal within 90 business days of your receipt of this letter. The appeal should be addressed to William L. Stoppel, Acting Associate Director – Management, Peace Corps, 1111 20th Street NW, Washington, DC 20526. Your appeal must include the FOIA request number and a statement explaining what you are appealing. It is possible to submit the appeal by U.S. mail (see above) or fax or email. Note that our fax number is 202-692-1385 and email is foia@peacecorps.gov. Also, however you submit the appeal, "Freedom of Information Act Appeal" should be clearly marked on the appeal letter and envelope, or the email subject line, or the fax cover sheet.

If you have any questions regarding this response, please contact Candice Allgaier, FOIA/Privacy Act Specialist, at 202-692-1904 or foia@peacecorps.gov.

Sincerely,

Denora Miller
FOIA/PA Officer

Attachments

Peace Corps

Risk Management Plan

Portfolio Management Office
Office of the Chief Information Officer
November 2016

Document Information

Identifier	Information
Document ID	PMO – Risk Management Plan
Document Owner(s)	Lisa Glufling

Document History

Version	Issue Date	Description
1.0	2016-11-29	First publication
0.5	2016-10-13	Initial draft

Table of Contents

1. Summary

This document describes the roles and responsibilities, risk domain, risk management processes, and reporting rules that will be used to manage risks and issues for Information Technology (IT) projects developed by the Peace Corps' Office of the Chief Information Officer (OCIO). This plan is principally based upon and guided by industry standard approaches to risk management as established in the Project Management Body of Knowledge (PMBOK), National Institutes of Standards and Technology (NIST) Special Publication 800-30, the International Organization for Standardization (ISO) ISO 31000 – Risk Management standard, and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework. This document is intended to be an operational tool to help identify, analyze, respond to, and monitor risks at the project level throughout the software development lifecycle.

2. Risk Definition

"The effect of uncertainty on objectives." –ISO 31000 definition of risk

Risk is an inherent characteristic of any project or initiative. Risks can impact various aspects of a project including cost, schedule, quality, technical stability, security, customer satisfaction, and resources. While risk themselves are neither intrinsically negative nor positive, the issues resulting from them can yield negative consequence or positive benefits (positive risks are frequently referred to as "opportunities") to a project. Risks are scored across two dimensions; probability and impact. The probability of risks are scored based on subjective analysis by the project team and substantiated by past experience or historical data. The impact of risks are graded on a determinative scale based its effect on the project.

By way of classification, internal risks are those under the control or influence of the project team, such as the level of quality of the deliverables and self-imposed timelines. External risks are those outside the control or influence of the project team, such as market influences, governmental legislation, or Peace Corps policy constraints.

Implicit in this definition is the time-bound nature of risks – they have not yet occurred. In contrast with risks, *issues* are former risks that have been actualized and are no longer a probability, but currently impacting project performance. Risk management attempts to reduce the likelihood and volume of issues, but the approaches defined in this plan can continue to be used to control for risks than evolve into issues.

3. Roles and Responsibilities

Key risk management activities are carried out by existing Integrated Project Team (IPT) members assuming roles that are responsible for executing on assigned activities. The below table identifies which team member(s) or groups perform the various risk management roles. The number of team members assuming these roles depends on the size of the projects and resource availability. When necessary, any one individual may assume multiple roles.

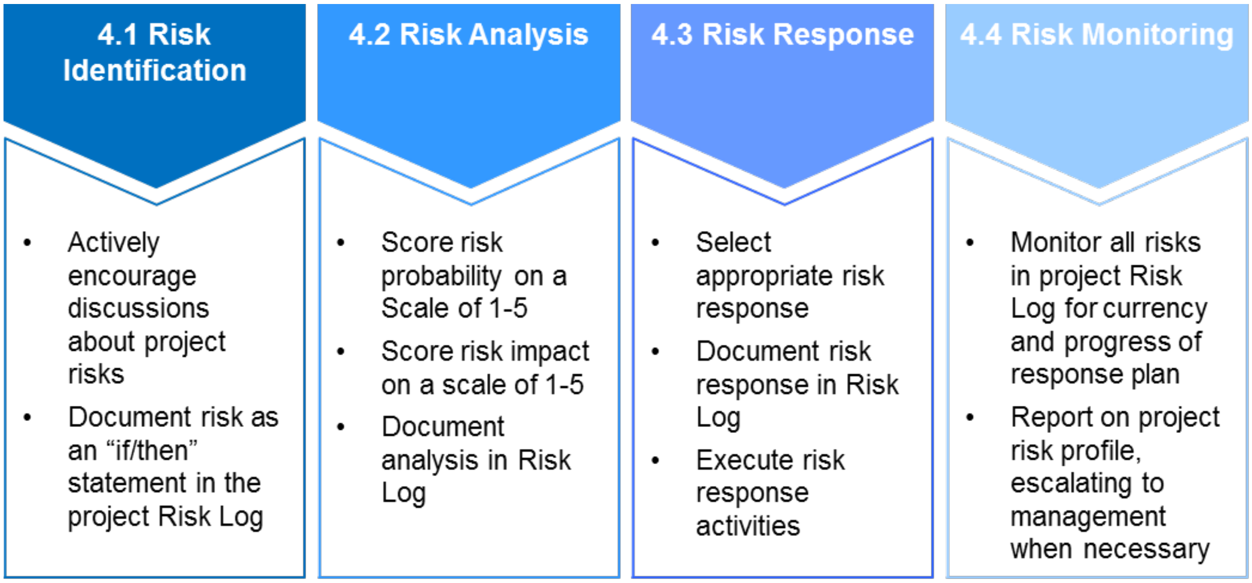
Role	Summary of Activities	Individuals/Names

Role	Summary of Activities	Individuals/Names
Risk Manager	• Manages risks by executing policy, procedures and plans. • Ensures risk sub-process activities are executed. • Periodically reviews all risks, identifies additional risks, and assesses documented risk strategies. • Escalates risks, as appropriate.	Project Manager or designee
Risk Owner	• Takes responsibility for appropriate planning and execution of the risk response. • Accepts ownership for risks in other risk domains when needed. • Ensures that Risk Management functions are performed.	Any member of the IPT in OCIO, Business Office, or contractor Development Team. On occasion, the owner can be external to the project.
Risk Identifier	• Identifies and reports any potential risk. • Identifies the trigger event and approximates a trigger date. • Participates in risk planning, mitigation and plan execution.	Any member of the IPT in OCIO, Business Office, or contractor Development Team.
Risk Management Analyst	• Performs risk analysis/assessment, risk response and monitoring. • Validates, classifies and assigns ownership of risks. • Performs qualitative and quantitative analysis. • Prioritizes risks. • Defines triggers and indicators. • Plans a risk response for each risk. • Assesses the effectiveness of the response executed. • Reviews the Risk Register. • Monitors triggers and indicators. • Prepares risk metrics.	Project Manager or designee
Risk Review Board	• Address and review all risks within the project/program • Review and approve or reject mitigation plans and contingency plans. • Determine whether additional mitigation and contingency plans are required. • Escalate risks to the next level based upon the severity and exposure thresholds. • Track overall program risk status based on reports from Risk Managers. • Reviews risk reports and metrics.	Led by PMO Manager and comprised by OCIO IPT members. This board will convene during regularly scheduled OCIO IPT Meetings and discuss critical risks as needed.

Role	Summary of Activities	Individuals/Names
External Stakeholder	• Informed of risks and provides input into mitigation strategy. • Uses influence to expedite risk responses and risk closure.	Senior Decision Makers

4. Risk Management Processes

The steps enumerated below provide a process guide for PMs to actively manage risks for their projects. These processes should be performed on a continuous basis throughout the project lifecycle.



4.1 Risk Identification

- Actively encourage discussions about project risks
- Document risk as an "if/then" statement in the project Risk Log

4.2 Risk Analysis

- Score risk probability on a Scale of 1-5
- Score risk impact on a scale of 1-5
- Document analysis in Risk Log

4.3 Risk Response

- Select appropriate risk response
- Document risk response in Risk Log
- Execute risk response activities

4.4 Risk Monitoring

- Monitor all risks in project Risk Log for currency and progress of response plan
- Report on project risk profile, escalating to management when necessary

4.1 Risk Identification

Active surveillance of project risks is a responsibility of all members of an IPT. The PMs should regularly encourage risk identification from project members during team meetings. When a risk has been surfaced for discussion and the PM agrees to its validity, it should be documented in the project's Risk Log in the following syntax:

```
If <Event>, then <Consequence>
```

An example risk statement using this convention is as follows, "If the development team does not receive access to the test environment by October 1, then system testing will experience a day-to-day slip in schedule." PMs should strive to articulate details in the risk statement to enable understanding of both the conditions and consequences of the risk. Generic risk statements are of reduced utility as they do not assist in developing an adequate response. Including specificity as it relates to the constraints of schedule, cost, and scope helps facilitate Risk Analysis, the next step of this process.

4.2 Risk Analysis

Once the risk statement has been finalized and entered into the Risk Log, the IPT should evaluate it across dimensions of probability and impact. The purpose of risk analysis is to refine the risk definition to provide key decision making information.

In order to determine probability, the IPT scores each risk on a 1-5 scale, based on the guidelines below.

Risk Probability Score	Likelihood of Event
5 Very High	> 80% – Risk event expected to occur
4 High	60-80% – Risk event more likely to occur
3 Moderate	40-60% – Risk event may or may not occur
2 Low	20-40% – Risk event less likely to occur
1 Very Low	< 20% – Risk event not expected

This estimation is a subjective analysis and requires knowledge of the activity and depends on the collective experience of the IPT or reference to historical data. This factor also includes the likely timeframe in which the risk might occur and the potential frequency of the risk (if applicable).

In concert with Risk Probability, each risk should be defined with a corresponding impact. Again, the evaluation of this score is dependent on the collective analysis of the IPT. The below table provides the criteria by which IPTs should define the impact factor of each risk.

Impact Score	Type of Impact		
	Change to Cost or Schedule	**Scope or Quality**	**Reliability**
5 Very High	> 20%	End product fails to meet customer needs or legislation requirements resulting in Congressional inquiries or punitive damages.	Software defects cause unpredictable problems for end-users.
4 High	10 – 20%	Reduction in functionality or usability unacceptable to customer.	Software contains major defects that require extensive workarounds.
3 Moderate	5 – 10%	Major impact in functionality or usability requiring customer approval.	Software contains defects that interrupt business operations sporadically and not for any sustained period of time.
2 Low	< 5%	Relatively minor impact in functionality or usability.	Software contains known defects that do not interrupt business operations.
1 Very Low	No or negligible variance	Very minor impact in functionality or usability.	Software contains minor defects – such as spelling or help – but have

			no implications to IT or business operations; can wait until another release to address.

The result of Risk Analysis is a snapshot in time, describing the risk context of a project. This may change significantly during the project as risks occur and are responded to and new risks are discovered. Risk Analysis must be performed periodically to ensure that the analysis remains current.

4.3 Risk Response

Upon scoring each risk across probability and impact factors, IPTs shall then determine an appropriate response. This entails identifying and documenting the appropriate treatment to modify or respond to the risk. The responses include:

- **Acceptance** – An informed decision to tolerate or take on the risk
- **Avoidance** – The decision to withdraw from the activity that exposes the project to the risk
- **Mitigation** – Pursuing actions to reduce the probability of a risk or minimize its impact
- **Transference** – Involving another party to share or wholly assume the risk

For each risk under management, identified personnel will execute the response plan documented in the Risk Log for that risk. The containment strategy can be one time, periodic or continuously active, but must be appropriate to the scale of the risk. Progress made against the response plan is also recorded in the Risk Log as that progress is realized.

4.4 Risk Monitoring

Monitoring risks is a continuous activity necessary to track the state of identified risks, ensure execution of risk response plans, identify new risks resulting from responses, ensure accurate, relevant and timely risk-related data is collected, compiled and analyzed, and use the analysis to take appropriate action. Monitoring can begin when a risk has been identified and may continue throughout the lifecycle of the project or until the risk is resolved. A risk can be considered resolved when its threat has been neutralized.

In order to report on the risks monitored by each project, the IPT shall collect, update, compile risk data, and report on risk trends to determine whether particular risks are decreasing, staying the same, or increasing in severity over time. A dashboard view of a project risks as seen in the sample matrix below can provide an at-a-glance view of the overall risk profile of the project.

Impact	5 Very High	🟨	🟨	🟥	🟥	🟥
	4 High	🟨	🟨	🟨	🟥	🟥
	3 Moderate	🟩	🟨	🟨	🟨	🟥
	2 Low	🟩	🟩	🟨	🟨	🟨

	1 Very Low	🟩	🟩	🟩	🟨	🟨
		1 Very Low	2 Low	3 Moderate	4 High	5 Very High
		Probability				

Appendix A: Risk Log Template

Risk Log
Template.xlsx

[Project Name] Risk Log

Risk ID	Status	Risk Statement	OMB Risk Category	Probability	Impact	Response	Response Plan	Risk Owner	Date Identified
R001	Open	If <EVENT>, then <CONSEQUENCE>	Strategic	5	5	Accept			
R002	Open	If <EVENT>, then <CONSEQUENCE>	Technical Obsolescence	4	4	Avoid			
R003	Open	If <EVENT>, then <CONSEQUENCE>	Reliability of Systems	3	3	Mitigate			
R004	Open	If <EVENT>, then <CONSEQUENCE>	Dependencies and Interoperability between this Investement and others	2	2	Transfer			
R005	Open	If <EVENT>, then <CONSEQUENCE>	Data/Info	1	1	Accept			

Closed Risks

Risk ID	Status	Risk Statement	OMB Risk Category	Probability	Impact	Response	Response Plan	Risk Owner	Date Identified
R001	Open	If <EVENT>, then <CONSEQUENCE>	Strategic	5	5	Accept			
R002	Open	If <EVENT>, then <CONSEQUENCE>		4	4	Avoid			
R003	Open	If <EVENT>, then <CONSEQUENCE>		3	3	Mitigate			
R004	Open	If <EVENT>, then <CONSEQUENCE>		2	2	Transfer			
R005	Open	If <EVENT>, then <CONSEQUENCE>		1	1	Accept			

OMB	Response
Schedule	Accept
Initial Cost	Avoid
Life-cycle (	Mitigate
Technical (	Transfer
Feasibility	
Reliability of Systems	
Dependencies and Interoperability between this Investement and others	
Surety (Asset Protection) Considerations	
Risk of Creating Monopoly for Future Procurements	
Capability of Agency to Manage this Investment	
Overall Risk of Investment Failure	
Organizational and Change Management	
Business	
Data/Info	
Technology	
Strategic	
Security	
Privacy	
Project Resources	

Current State: Overview

Project Summary

The Intranet Modernization project identifies the functional owner of the intranet, develops a content management strategy and requirements, including support for migrating current intranet content and an approach for maintaining currency and accuracy of content, develops a User Interface (UI) strategy and requirements, and completes any outstanding transitions from legacy platforms. Additionally, this project will define and implement a communication strategy, roles and responsibilities, support plan, data architecture, governance, and Intranet and workspace use policy.

Strategic Plan Alignment
Volunteer Well-Being
Service Opportunity of Choice
Development Impact
Cross-Cultural Understanding
Continuation of Service
Diversity and Inclusion
Site Development
Train Up
High-Performing Learning Organization
Global Connectivity
Measurement for Results

Solution Delivery Framework (SDF) Milestones	
Request	February 2016
Initiation	October 2016
Planning & Requirements	**March 2017**
Design	June 2017 (Phase 1)
Development	June 2017 (Phase 1)
Integration & Test	June 2017 (Phase 1)
Deployment	September 2017 (Phase 1)
Closeout	---

Current State: Platform Structure

SharePoint Platform 2013

Intranet

Purpose: Provides access to current events, leadership plans, office information and resources, libraries, staff directory, HR, navigation to other key internal applications.

Design: Templated office pages. Limited design on landing pages.

Team: EBSS

Security: Staff access only (on agency network).

Workspace

Purpose: Serves as a community collaboration hub for sharing content and information amongst groups and offices globally.

Design: Open canvas for customization based on business needs.

Team: PO&I

Security: Staff access only (on agency network).

Posts

Purpose: Allows content sharing between Post staff and volunteers across Post locations. Provides personnel with easy navigation to other key applications. Only rolled out to 6 of 64 Post sites to date.

Team: PO&I

Design: (b)(5) [redacted]

Security: Staff and volunteer access (separate services).

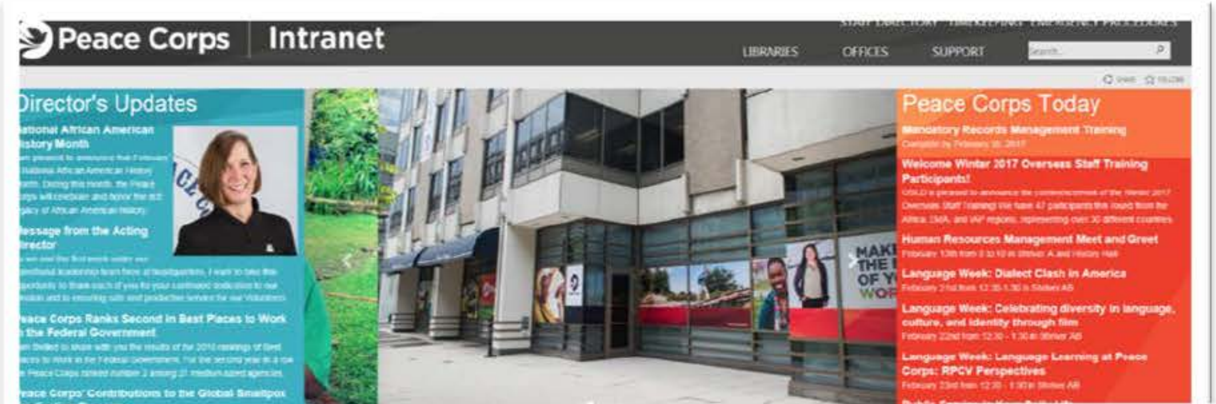
Discovery Findings: Overview

To understand the current state of internal communications and help define the project scope and direction, the team gathered information from leadership and users on goals and perceptions of the agency's "Internet" and "Workspaces" internal communications tools.

Sources included:

- Director's Internal Communications Task Force Report
  - Content inventory and survey representing diverse offices and skill sets (575 overseas; 396 HQ; 74 RROs); Focus groups from 16 offices and 75 employees
- Survey Data collected from Agency Content Administrators
  - 52 out 85 content editors/users representing 65% of offices
- Interviews with Peace Corps leaders and stakeholders

Discovery Findings: Intranet & Workspaces



Peace Corps | Intranet

STAFF DIRECTORY TIMEKEEPING EMERGENCY PROCEDURES

LIBRARIES OFFICES SUPPORT Search...

SHARE FOLLOW

Director's Updates

National African American History Month

[illegible]

Message from the Acting Director

[illegible]

Peace Corps Ranks Second in Best Places to Work in the Federal Government

[illegible]

Peace Corps' Contributions to the Global Smallpox Eradication Program

[illegible]

Peace Corps Today

Mandatory Records Management Training

[illegible]

Welcome Winter 2017 Overseas Staff Training Participants!

[illegible]

Human Resources Management Meet and Greet

February 13th [illegible]

Language Week: Dialect Clash in America

February 21st [illegible]

Language Week: Celebrating diversity in language, culture, and identity through film

February 22nd [illegible]

Language Week: Language Learning at Peace Corps: RPCV Perspectives

February 23rd [illegible]

Public S[illegible]

AGENCY TOOLS

OR HQ
Hyperion
Odyssey
OdyWeb
Ilum
Sunflower
PCUniversity
[illegible]
Lynda.com Agency Login
T&E Resources

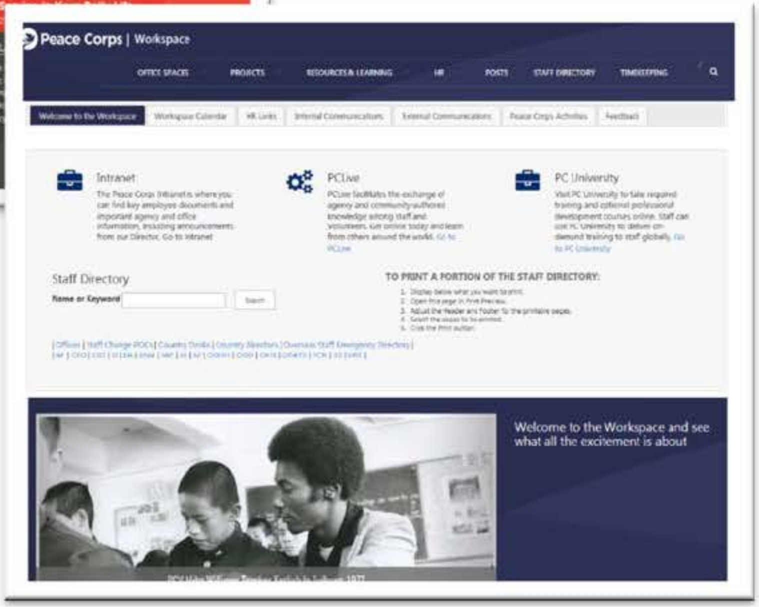
NON-AGENCY SITES

CITIBANK Login
Purchase/Travel Card Training
Per Diem Rates

IT RESOURCES

Conference Room Reservation Quick Guide
Outlook Web Access
Remote Access Connectivity Guide
Track-It
Using Skype for Business
HQ Wi-Fi
Secure File Transfer Protocol (SFTP) Quick Guide

MISCELL[illegible]



Peace Corps | Workspace

OFFICE SPACES PROJECTS RESOURCES & LEARNING HR POSTS STAFF DIRECTORY TIMEKEEPING

Welcome to the Workspace | Workspace Calendar | HR Links | Internal Communications | External Communications | Peace Corps Activities | Feedback

Intranet

The Peace Corps Intranet is where you can find key employee documents and important agency and office information, including announcements from our Director. Go to Intranet

PCLive

PCLive facilitates the exchange of agency and community-authored knowledge among staff and volunteers. Get online today and learn from others around the world. Go to PCLive

PC University

Visit PC University to take required training and optional professional development courses online. Staff can use PC University to deliver on-demand training to staff globally. Go to PC University

Staff Directory

Name or Keyword Search

TO PRINT A PORTION OF THE STAFF DIRECTORY:

1. Display below what you want to print.
2. Open this page in Print Preview.
3. Adjust the header and footer to the printable pages.
4. Select the pages to be printed.
5. Click the Print button.

| Offices | Staff Change POCs | Country Desks | Country Directors | Overseas Staff Emergency Directory |

[illegible]

Welcome to the Workspace and see what all the excitement is about

Areas for Improvement:

User Design

- (b)(5)
- (b)(5)
- (b)(5)
- (b)(5)

Support Services

- (b)(5)
- (b)(5)
- (b)(5)

Discovery Findings: Challenges

- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]

Future Direction: Recommendations Overview

1

(b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]

2

(b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]

3

(b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]

1

Recommendation: (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]
- (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]
  - (b)(5) [redacted]

2 Recommendation: (b)(5) [redacted]

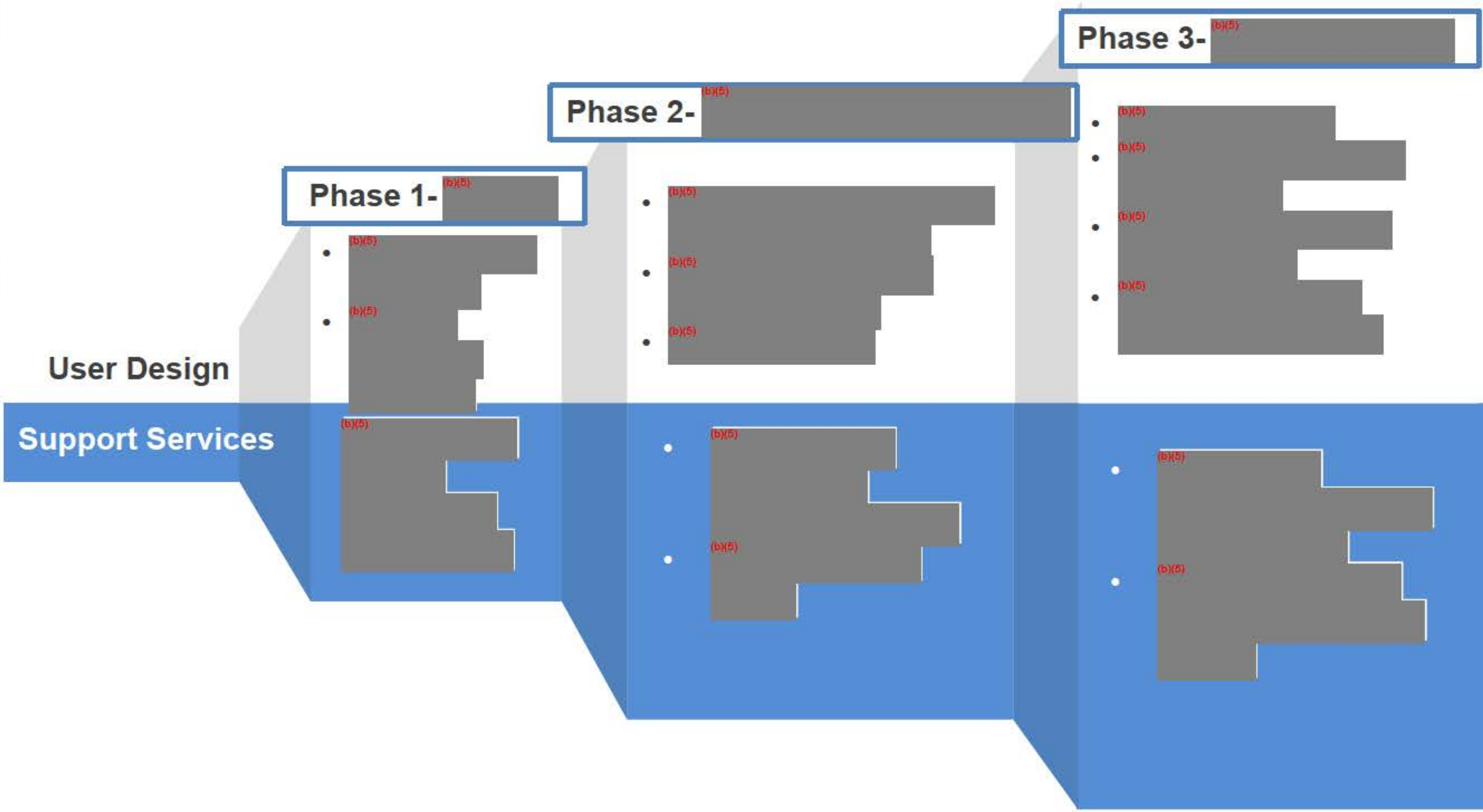
(b)(5) [redacted]

(b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]

3

Recommendation: (b)(5) [redacted]



User Design

Support Services

Phase 1- (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]

(b)(5) [redacted]

Phase 2- (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]

Phase 3- (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]
- (b)(5) [redacted]

- (b)(5) [redacted]
- (b)(5) [redacted]