Security Assessment and Authorization - CA

Policy Page Template

Control Satisfaction Matrix

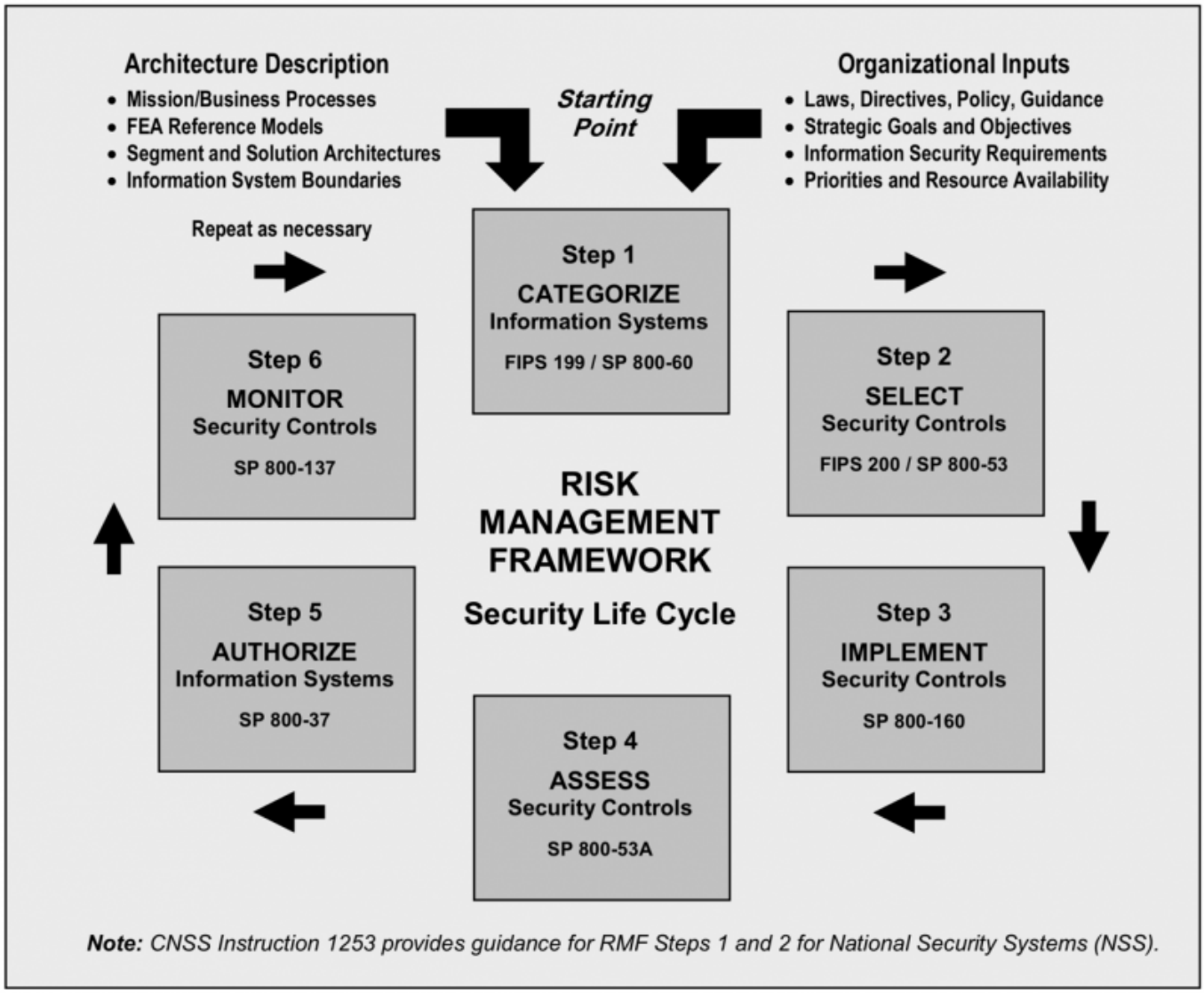
Framework Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST Standard	Various	Various	Various	N/A	N/A

Major Document History

Date	Comment	Who
5/1/2019	Initial Doc	Tharp
6/03/2019	Edited Format, linked to Control Objectives Risk Assessment	Tharp
8/16/2019	Moved RMF to Org. Governance Topic	Tharp
8/29/2019	Copied Content For IS-1 SOC submission	Tharp
9/27/2019	Added Risk Assessment Example	Tharp
10/6/2021	Policy's Reviewed for Audit	Tharp

Risk Management Framework

Figure 1



Step 1 - Categorize

FIPS 199

FIPS 199 Sets the Standards for Security Categorization of Federal Information and Information System and SP 800-60 guides the application of those standards. The table below summarizes the Security Objective vs. Potential Impact.

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability - Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

DLZP Group Security Standard

```
DLZP Group shall treat all client data and environments as **Confidential-
High**
```

Therefore, all systems built and maintained by DLZP in the AWS cloud shall meet this standard. This is achievable in the AWS cloud environment at no extra cost to the client. Furthermore, by adopting a single standard DLZP limits the possibility of exposing data due to accidental mis-classification.

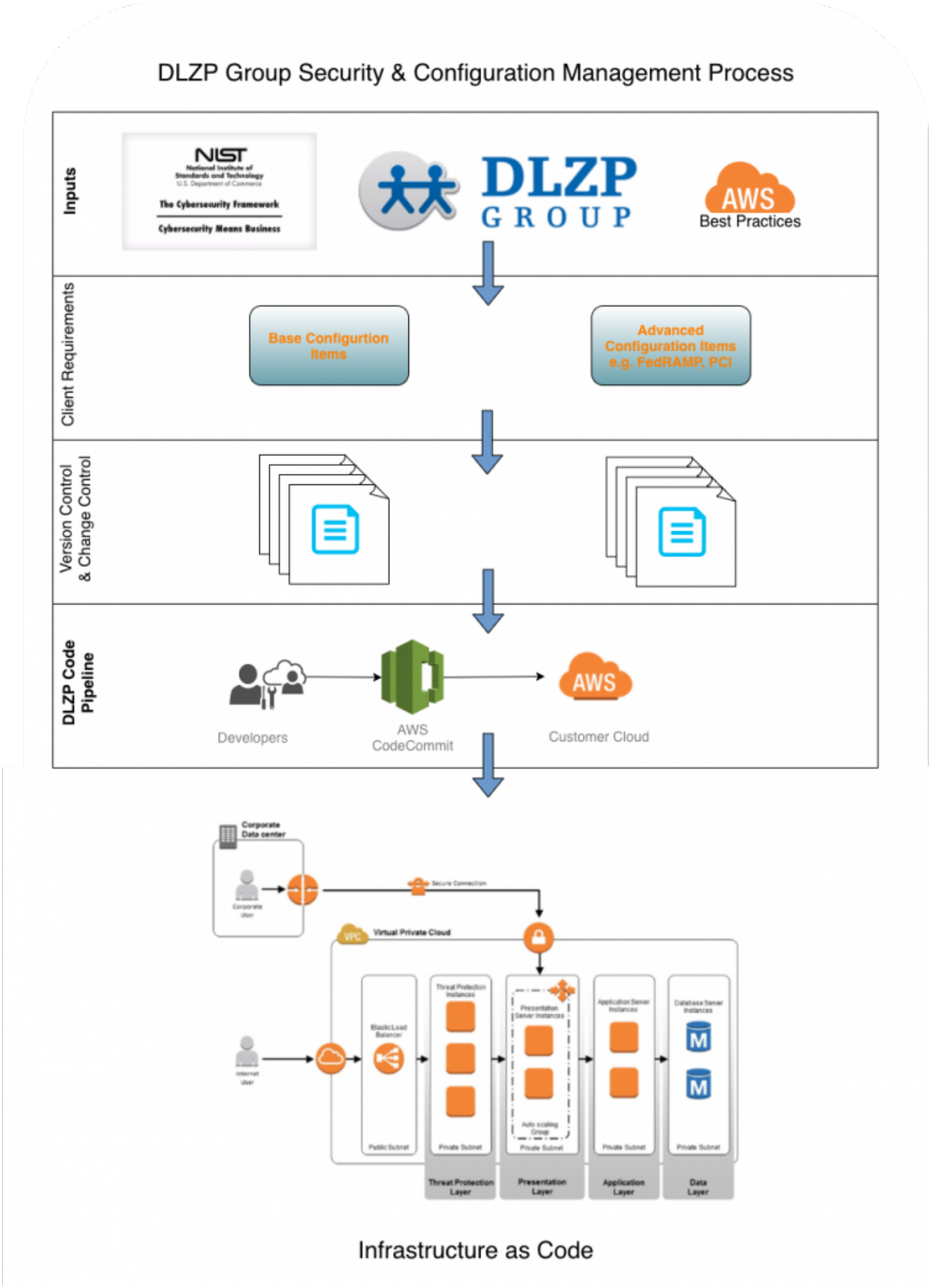
Step 2 - Select Security Controls

FIPS 200 sets the minimum security requirements for Federal Information Systems. And, **NIST 800-53 rev.4** provides a library of controls configuration items (CI's) and policies that provides the operating environment framework that must be met to maintain compliance with FedRAMP standards. To meet the **DLZP Group Security Standard of Confidential-High**, DLZP will maintain appropriate 800-53 controls throughout its business and data processing practices.

DLZP Group Security Standard

```
All systems BASE CI's will meet relevant NIST 800-53 Confidential-High
security objectives.
DLZP Group offers clients the choice of a Compliance Framework (Advanced
CI's) to match their business requirements.
```

This ensure our client's have the most secure environment and matches the cost associated with their Compliance Standards e.g. FedRAMP, HIPAA, PCI, FERPA to the regulatory environment of the customers business model and entity needs.



Steps 3 - 6

Referencing Figure 1. **Steps 3 thru 6** cover data processing and governance business practices that will we covered within their own wiki chapters.

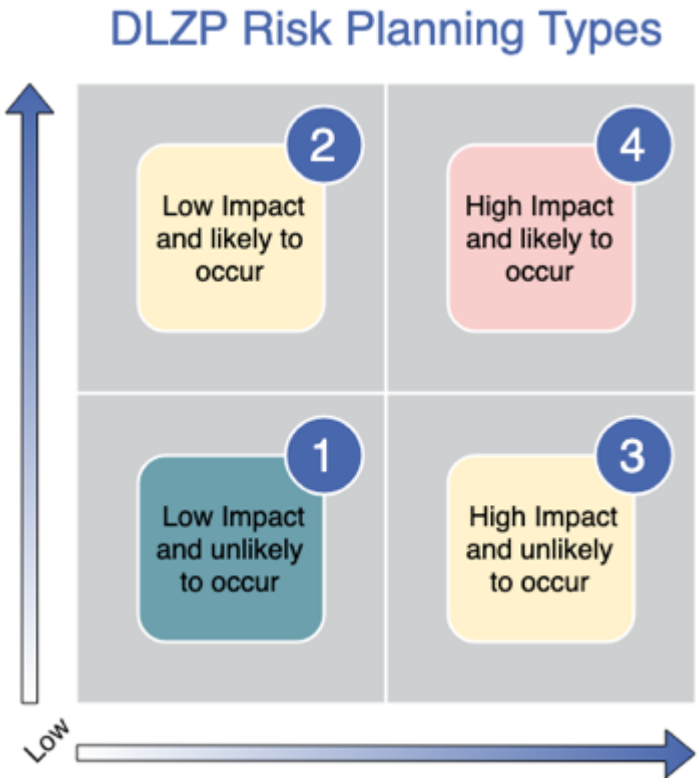
Risk Assessment Example

Risk Planning

For projects of the scope and complexity of the CLC's PeopleSoft Upgrade and cloud hosting, an AWS Cloud implementation reduces or eliminates many sources of technical, performance, and capacity risks associated with IT systems. DLZP Group's 8+ years of AWS experience makes us fully aware of its services and their programing and deployment.

Performance issues may be mitigated rapidly in the AWS virtual environment with systems' scale up. And capacity limitations are non-existent in the AWS cloud for projects of this scale.

Therefore, our leading risks are limited to personnel resource availability and the potential change in requirements from design due diligence, data conversion and 3rd Party Integration reference. Review Table for risk mitigation steps.



Phase	Risk by Phase	Risk Type	DLZP Mitigation
Scope			
	Project Start Is Delayed by client	1; 2	Outside DLZP Control
	Project Scope is Changed by client	1; 2	Outside DLZP Control
	CLC Requirements Change	1; 2	Outside DLZP Control

Phase	Risk by Phase	Risk Type	DLZP Mitigation
Scope			
Design			
	Project Phase Is Delayed by client	2; 3	Outside DLZP Control
	Project Scope is Changed by client	1; 2	Outside DLZP Control
	CLC Requirements Change	1; 2	Outside DLZP Control
	CLC Resource Availability	2; 3	Schedule Around Resource Constraints
	DLZP Group Resource Availability	1	DLZP Team Approach Mitigates
	Unknown Requirement Discovered	2; 3	DLZP Design Interview Process Mitigates
Build			
	Project Phase Is Delayed by client	2; 3	Outside DLZP Control
	Project Scope is Changed by client	2; 3	Outside DLZP Control
	CLC Requirements Change	2; 3	Outside DLZP Control
	CLC Resource Availability	1; 2	Schedule Around Resource Constraints
	DLZP Group Resource Availability	1	DLZP Team Approach Mitigates
	Data Conversion	1; 3	DLZP Automation and Approach Mitigates
	3rd Party Integration	2; 3	DLZP Experience and Cloud Microservices Mitigates
Deploy			
	Project Phase Is Delayed by client	2; 3	Outside DLZP Control
	Project Scope is Changed by client	2; 3	Outside DLZP Control
	CLC Requirements Change	2; 3	Outside DLZP Control
	CLC Resource Availability	2; 3	Schedule Around Resource Constraints
	DLZP Group Resource Availability	1	DLZP Team Approach Mitigates
Operate			
	CLC Requirements Change	2; 3	Upgrade/Maintenance Support
	CLC Resource Availability	1; 2	Schedule Around Resource Constraints
	DLZP Group Resource Availability	1; 3	DLZP Team Approach Mitigates