Security Assessment and Authorization - CA

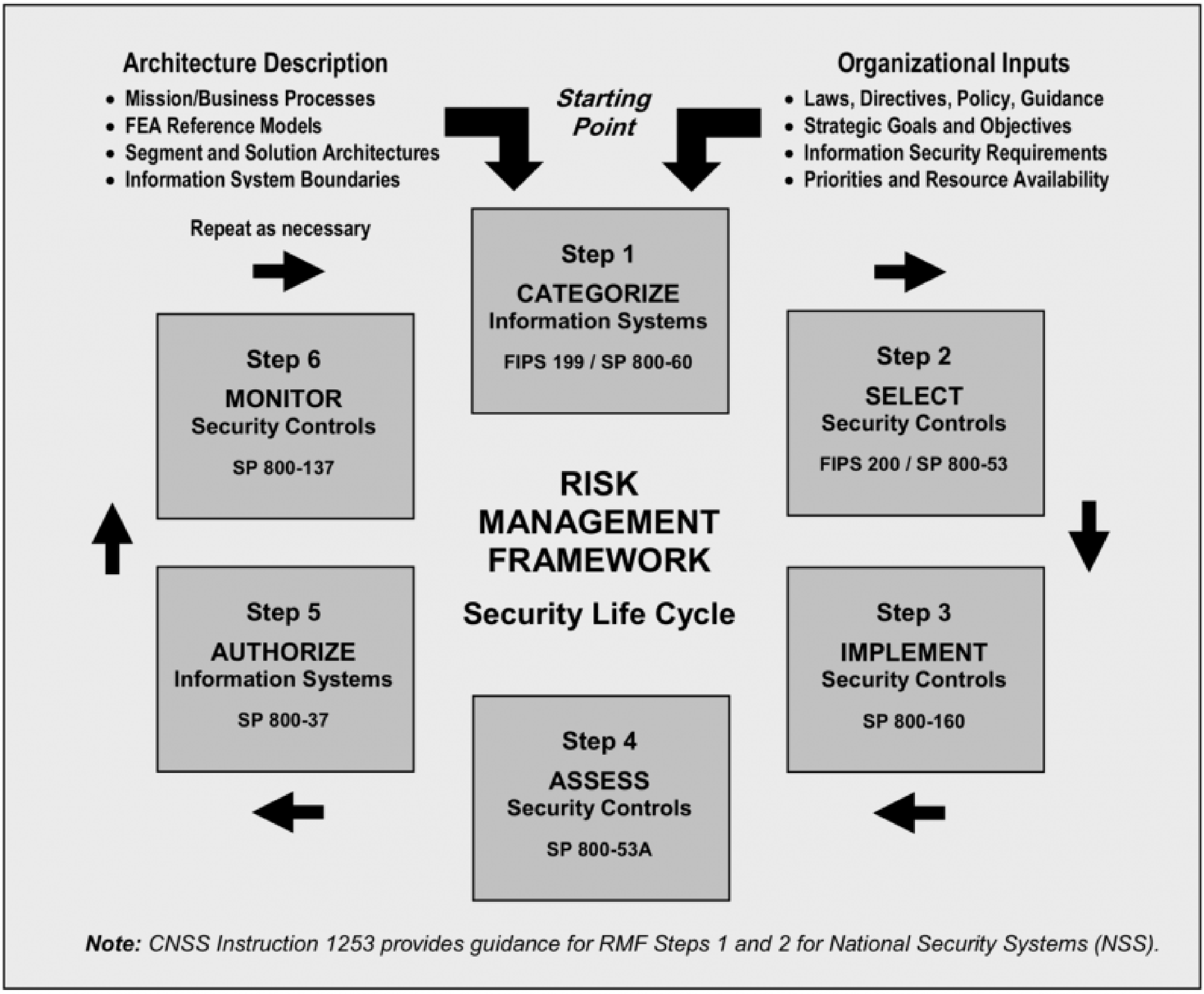
Table 1 - Control Satisfaction

Standard	NIST Category	Controls Satisfied	Audit Controls
NIST 800-53rev4	CA	aa##	IS-1

Table 2 - Major Document History

Date	Comment	Who
5/1/2019	Initial Doc	Tharp
6/03/2019	Edited Format, linked to Control Objectives Risk Assessment	Tharp

Risk Management Framework


Architecture Description
• Mission/Business Processes
• FEA Reference Models
• Segment and Solution Architectures
• Information System Boundaries
Starting Point
Organizational Inputs
• Laws, Directives, Policy, Guidance
• Strategic Goals and Objectives
• Information Security Requirements
• Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORIZE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

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.
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.

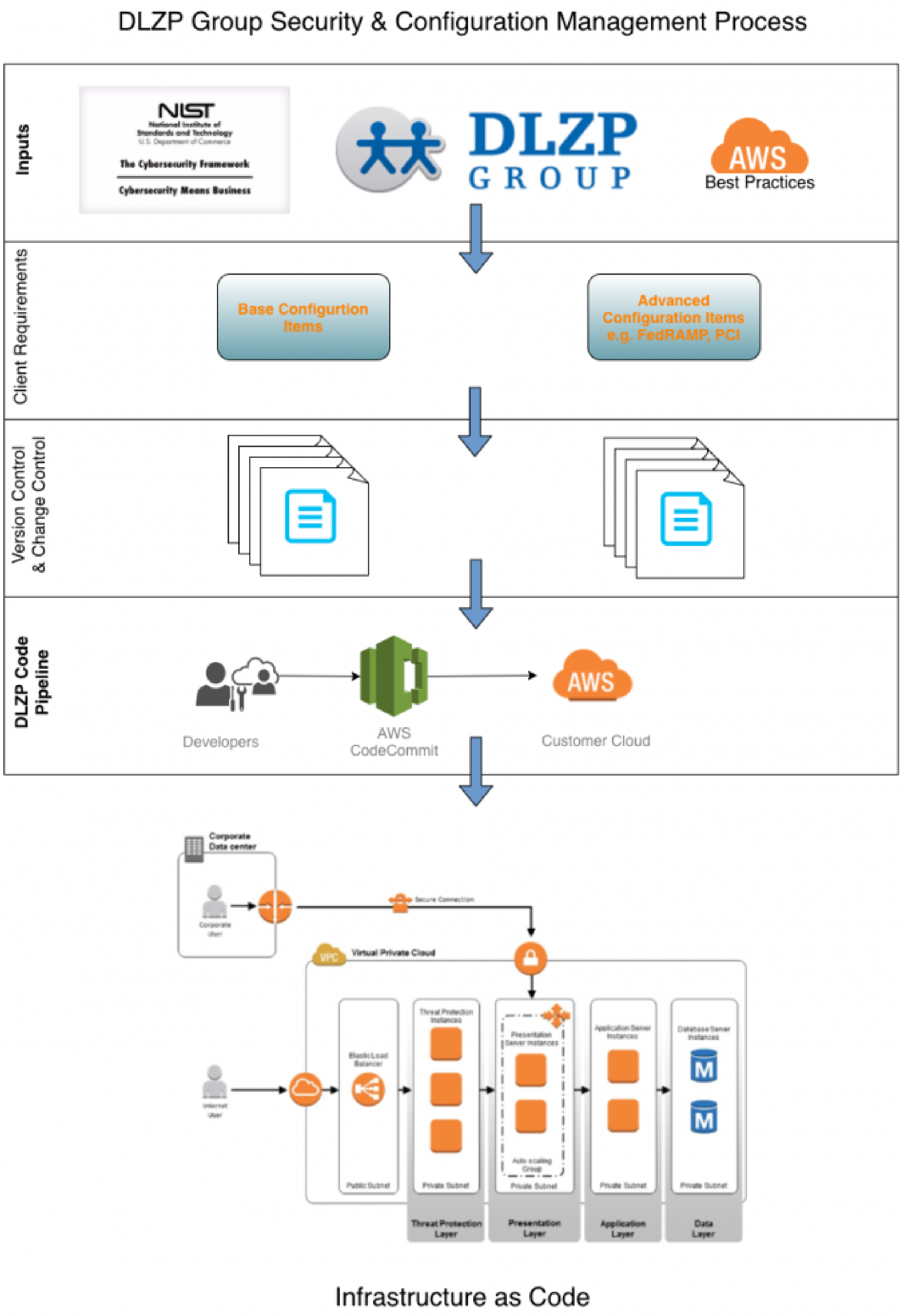
Step 2 - Select Security Controls

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

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

From:
https://wiki.cloud.dlzpgroup.com/ -

Permanent link:
https://wiki.cloud.dlzpgroup.com/doku.php?id=security:rmf

Last update: **2019/12/20 16:08**