# README

## 0.1 Document Overview

This comprehensive guide, "Developing Authorization Policies Using Ping Authorize: A SABSA-Based Approach," provides a detailed framework for implementing robust API authorization strategies using Ping Authorize, grounded in the principles of the Sherwood Applied Business Security Architecture (SABSA).

## 0.2 Purpose

The primary purpose of this document is to offer organizations a structured, risk-driven methodology for creating, implementing, and managing authorization policies within their API ecosystems. It aims to bridge the gap between high-level security architecture principles and the practical implementation of API authorization policies using Ping Authorize.

## 0.3 Target Audience

This guide is designed for:

- Security Architects
- Policy Administrators
- IT Managers and CISOs
- API Developers and DevOps Teams
- Compliance Officers
- Business Stakeholders
- Identity and Access Management (IAM) Specialists
- Security Analysts and Operators

## 0.4 Document Structure

The document is organized into the following main sections:

1. Introduction
2. SABSA Framework Overview
3. Business Requirements and Security Strategy
4. Conceptual and Logical Security Architecture

Each section builds upon the previous ones, providing a comprehensive view of the API authorization lifecycle.

## 0.5 How to Use This Document

1. **Sequential Reading**: While sections can be referenced independently, the document is designed to be read in order, as each section builds on concepts introduced in previous ones.
2. **Practical Application**: Throughout the document, you'll find case studies, examples, and best practices. Apply these to your specific organizational context.
3. **Customization**: The frameworks and strategies presented are meant to be flexible. Adapt them to fit your organization's unique needs and constraints.
4. **Cross-Team Collaboration**: Share relevant sections with colleagues from different departments to foster a holistic approach to API security.
5. **Regular Review**: As your API ecosystem evolves, periodically review this document to ensure your authorization strategies remain aligned with best practices and business needs.

## 0.6 Key Concepts

- SABSA Framework and its application to API security
- API Authorization using Ping Authorize
- Risk-based approach to security architecture
- Business-driven security strategies
- Conceptual and logical security architecture for APIs

## 0.7 Document Maintenance

This document should be reviewed and updated regularly to reflect:

- Changes in the API ecosystem
- Updates to Ping Authorize features and capabilities
- Evolving security threats and best practices
- Changes in relevant regulations and compliance requirements

## 0.8 Additional Resources

- Ping Authorize Official Documentation
- SABSA Institute Resources
- Relevant API Security Standards (e.g., OWASP API Security Top 10)

## 0.9 Feedback and Contributions

We encourage feedback and contributions to improve this guide. Please submit any suggestions, corrections, or additional insights to [insert appropriate contact or process].

By using this guide, organizations can develop a robust, flexible, and business-aligned approach to API authorization using Ping Authorize. The SABSA-based methodology ensures that technical implementations are always in service of broader business objectives and risk management strategies.