Business Case for Implementing Cisco ISE

Executive Summary:

Cisco Identity Services Engine (ISE) is a sophisticated network security solution designed to provide comprehensive visibility and control over who and what is accessing your network. Implementing Cisco ISE is a strategic decision that aims to enhance network security, compliance, and operational efficiency.

Key Features and Benefits:

1. **Network Visibility:**
   - **Feature:** Cisco ISE provides deep visibility into the users and devices that access your network.
   - **Benefit:** Improved security posture through enhanced monitoring and identification of potential threats.
2. **Access Control:**
   - **Feature:** Offers dynamic access control and segmentation capabilities.
   - **Benefit:** Ensures that only authorized users and devices have access to network resources, thereby reducing the risk of data breaches.
3. **Policy Enforcement:**
   - **Feature:** ISE enforces consistent security policies across the network.
   - **Benefit:** Streamlines compliance with internal and external regulations.
4. **Guest Networking:**
   - **Feature:** Provides secure and customized guest access.
   - **Benefit:** Enhances the user experience for visitors while maintaining network security.
5. **BYOD Support:**
   - **Feature:** Supports Bring Your Own Device (BYOD) policies.
   - **Benefit:** Allows employees to use their devices securely, increasing productivity and user satisfaction.
6. **Integration with Other Security Tools:**
   - **Feature:** Integrates with other Cisco and third-party security solutions.
   - **Benefit:** Creates a more robust and comprehensive security ecosystem.
7. **Automated Threat Response:**
   - **Feature:** Enables automated threat containment and response.

- **Benefit:** Reduces the time to detect and respond to threats, mitigating potential damage.

8. **Compliance Reporting:**
    - **Feature:** Offers detailed compliance reporting.
    - **Benefit:** Simplifies audit processes and ensures regulatory compliance.

Conclusion:

Implementing Cisco ISE in [Your Company Name] represents an opportunity to strengthen network security, streamline access control, and enhance compliance reporting. By leveraging ISE's advanced features, the organization can protect its critical assets more effectively while providing a flexible and user-friendly networking environment.

Cisco ISE Knowledge

Cisco Identity Services Engine (ISE) is a comprehensive network security and access control solution designed to provide visibility, authentication, authorization, and policy enforcement across wired, wireless, and VPN networks. Cisco ISE consists of various hardware, software, and components to deliver its features and functionality. Here's an overview of the major components and features of Cisco ISE:

Hardware Components:

1. **Cisco ISE Appliances**:
    - Cisco ISE typically runs on dedicated hardware appliances that serve as the core of the system. These appliances come in various models to accommodate different scale requirements, ranging from small to large deployments.
2. **Cisco Catalyst Switches and Routers**:
    - In network deployments, Cisco Catalyst switches and routers can act as Policy Service Nodes (PSNs) and RADIUS servers, extending the reach of Cisco ISE.
3. **Cisco Wireless LAN Controllers (WLCs)**:
    - Cisco ISE integrates with Cisco WLCs to provide secure wireless access control, allowing for centralized management and authentication of wireless clients.

Software Components:

1. **ISE Operating System (ISE OS)**:
    - The ISE OS is the core software that runs on Cisco ISE appliances. It provides the foundation for all other software components and services.
2. **Policy Services**:
    - Policy Services in Cisco ISE enable the creation and enforcement of access policies. They include Authentication, Authorization, and Accounting (AAA) services, as well as profiling and posture assessment.
3. **Administration and Monitoring Console**:
    - The ISE Administration and Monitoring Console provides a web-based interface for configuring, managing, and monitoring the Cisco ISE deployment.
4. **ISE Databases**:
    - Cisco ISE relies on databases to store configuration data, event logs, and user information. The primary databases used are the Policy Administration Database (PAS) and the Monitoring and Troubleshooting Database (MnT).

5. **Identity Stores**:
    - Cisco ISE integrates with identity stores such as Microsoft Active Directory, LDAP, and internal databases to authenticate and authorize users.
6. **Guest Services**:
    - Cisco ISE includes built-in guest services to provide controlled and secure guest access to the network. It allows for self-registration and sponsor-based guest access.

Key Features and Functionality:

1. **Authentication**:
    - Cisco ISE supports a wide range of authentication methods, including 802.1X, MAB (MAC Authentication Bypass), and web-based authentication, ensuring that only authorized users and devices gain network access.
2. **Authorization**:
    - ISE enforces role-based access control policies that determine what network resources users and devices can access based on their attributes and roles.
3. **Profiling**:
    - Cisco ISE can automatically profile and classify devices on the network, providing granular visibility into the types of devices connecting to the network.
4. **Posture Assessment**:
    - ISE assesses the security posture of endpoints and enforces compliance policies. Non-compliant devices can be quarantined or remediated.
5. **Guest Access**:
    - Cisco ISE offers guest access services, allowing organizations to securely onboard and manage guest users without compromising network security.
6. **BYOD (Bring Your Own Device)**:
    - ISE enables secure onboarding and management of personal devices in corporate networks while maintaining network security and compliance.
7. **Security Analytics and Threat Response**:
    - ISE provides real-time visibility into network activities, making it easier to detect and respond to security threats and anomalies.
8. **Integration with Other Cisco Technologies**:
    - Cisco ISE seamlessly integrates with other Cisco solutions such as Cisco AnyConnect VPN, Cisco TrustSec, and Cisco SecureX for enhanced security.
9. **Multi-Factor Authentication (MFA)**:

- Cisco ISE supports MFA methods like one-time passwords (OTP) and push notifications for added authentication security.

10. **Scalability**:
    - Cisco ISE can scale to accommodate the needs of small, medium, and large organizations with distributed or centralized deployment options.
11. **Compliance Reporting**:
    - ISE generates compliance reports to help organizations demonstrate adherence to security and regulatory standards.
12. **Troubleshooting and Monitoring Tools**:
    - Cisco ISE offers extensive troubleshooting and monitoring tools to diagnose and resolve network issues quickly.

Cisco ISE's combination of hardware, software, and features makes it a powerful solution for network security, access control, and compliance enforcement. Organizations can leverage Cisco ISE to enhance their network security posture and streamline access management.

Cisco ISE Knowledge

To understand the full range of features provided by Cisco Identity Services Engine (ISE) and determine which are relevant to your needs, consider the following questions. Each question corresponds to a specific feature of Cisco ISE:

1. **Do you need comprehensive visibility and control over who and what is accessing your network?**
    - Feature: **Network Visibility and Control**
2. **Is granular access control based on user identity, device type, and other factors critical for your network?**
    - Feature: **Dynamic Access Control**
3. **Are you looking to enforce consistent security policies across your wired, wireless, and VPN networks?**
    - Feature: **Policy Enforcement**
4. **Do you need to provide secure, regulated access for guests or visitors on your network?**
    - Feature: **Guest Access Management**
5. **Is managing the security for employee-owned devices (BYOD) a requirement for your organization?**
    - Feature: **BYOD Support**
6. **Do you require integration with other security solutions for a unified security stance?**
    - Feature: **Security Ecosystem Integration**
7. **Are automated threat detection and response capabilities important for your network security?**
    - Feature: **Threat Centric NAC (Network Access Control)**
8. **Do you need to ensure compliance with industry regulations and internal policies through detailed reporting?**
    - Feature: **Compliance and Reporting**
9. **Is a streamlined process for onboarding and managing devices on your network necessary?**
    - Feature: **Device Profiling and Onboarding**
10. **Do you need to segment users and devices to control access to sensitive parts of your network?**
    - Feature: **Micro-segmentation and TrustSec**
11. **Is automating routine network tasks to reduce complexity and improve efficiency a priority?**

- Feature: **Automated Policy Application**

12. **Do you require a solution to centrally manage encrypted traffic while maintaining privacy and compliance?**
    - Feature: **Encrypted Traffic Analytics**

Issues and Problems Without Cisco ISE

Security Vulnerabilities

Problem: Lack of network access control and authentication measures leaves the organization vulnerable to unauthorized access. Unauthenticated devices can easily enter the network, increasing the risk of security breaches.

Impact: Increased risk of data breaches, unauthorized access, and potential loss of sensitive information.

Compliance Challenges

Problem: Inability to enforce compliance with security policies and regulations. Without Cisco ISE, it's challenging to monitor and ensure that devices adhere to security and compliance standards.

Impact: Non-compliance with industry regulations, potential legal issues, and financial penalties.

Network Overload

Problem: Uncontrolled network access can lead to network congestion and bandwidth hogging by unmanaged devices. This affects network performance and user experience.

Impact: Slower network speeds, reduced productivity, and frustrated users.

Lack of Visibility

Problem: In the absence of Cisco ISE, there's limited visibility into who and what is accessing the network. This makes it difficult to monitor network activities and detect suspicious behavior.

Impact: Inadequate threat detection, delayed incident response, and increased exposure to cyber threats.

Manual User Management

Problem: Without Cisco ISE's automation, user management is manual and time-consuming. Adding, modifying, or removing user access requires manual intervention, leading to inefficiencies.

Impact: Slower user onboarding and offboarding processes, increased IT workload, and potential errors.

Limited Network Segmentation

Problem: Network segmentation for security and traffic management becomes challenging without Cisco ISE. Uncontrolled access across segments can lead to inter-segment threats.

Impact: Reduced network security, difficulties in isolating network issues, and higher security risks.

Inefficient Guest Access

Problem: Providing guest network access becomes cumbersome without Cisco ISE. Manual guest provisioning and access control lead to inefficiencies and potential security risks.

Impact: Delayed guest access, increased administrative overhead, and potential unauthorized access.

Difficulty in Policy Enforcement

Problem: Without Cisco ISE's policy enforcement capabilities, it's challenging to ensure that devices and users adhere to network policies consistently.

Impact: Inconsistent policy enforcement, potential policy violations, and security gaps.

Complex Authentication

Problem: Implementing complex authentication methods without Cisco ISE can be error-prone and difficult to manage, resulting in user frustration.

Impact: User authentication issues, increased IT support requests, and decreased user satisfaction.

Inadequate User Accountability

Problem: The lack of user accountability mechanisms makes it difficult to trace network activities back to individual users, hindering incident investigation.

Impact: Reduced ability to identify and address security incidents, prolonged downtime during investigations.

Cisco ISE Implementation Plan for Company ABC

Phase 1: Pre-Deployment Assessment

1.1 Define Objectives and Goals for Company ABC

Objectives and Goals:

- Modernize network infrastructure for improved scalability and agility.
- Enhance network security through segmentation and policy enforcement.
- Simplify network operations and management.
- Ensure seamless connectivity for 1000 users.

1.2 Assemble Company ABC Project Team

Project Team:

- Network Architects
- Network Engineers
- Security Experts
- IT Administrators
- User Training Specialists

1.3 Assess Current Network Environment at Company ABC

Assessment Scope:

- Review of existing network infrastructure and devices.
- Evaluation of network performance and scalability.
- Identification of security and compliance gaps.

1.4 Define Network Policies and Security Requirements for Company ABC

Network Policies and Security Requirements:

- Define access controls, specifying user roles and permissions.
- Segmentation strategies for network traffic isolation.
- Compliance standards and regulatory requirements.

Phase 2: Solution Design and Planning

2.1 Design Cisco ISE Deployment Architecture

Deployment Architecture:

- Define the architecture for Cisco ISE deployment, including server placement and redundancy.

2.2 Plan Hardware and Software Requirements

Hardware and Software Requirements:

- Specify the hardware and software components needed for Cisco ISE.
- Ensure compatibility with existing network infrastructure.

2.3 Develop Authentication and Authorization Policies

Authentication and Authorization Policies:

- Define policies for user authentication and authorization based on roles and attributes.

2.4 Create User Training and Awareness Plan

User Training and Awareness:

- Develop a plan to train end-users on new authentication methods and security practices.

Phase 3: Cisco ISE Deployment

3.1 Install and Configure Cisco ISE Appliances

Appliance Installation:

- Install Cisco ISE appliances according to the designed architecture.

3.2 Integration with Existing Network Infrastructure

Integration:

- Integrate Cisco ISE with existing network components, including switches, routers, and Active Directory.

3.3 Configure Authentication and Authorization Policies

Policy Configuration:

- Implement defined authentication and authorization policies within Cisco ISE.

3.4 Testing and Validation

Testing and Validation:

- Perform comprehensive testing to ensure proper functionality and security.
- Validate policies, authentication methods, and network segmentation.

Phase 4: User Enrollment and Training

4.1 User Enrollment

User Enrollment:

- Onboard and enroll 1000 users into the Cisco ISE system.

- Configure user profiles, roles, and permissions.

4.2 User Training and Support

Training and Support:

- Provide training and support to users for seamless network access through Cisco ISE.
- Communicate new authentication processes and security best practices.

Phase 5: Monitoring and Maintenance

5.1 Network Monitoring and Logging

Monitoring:

- Set up continuous monitoring and logging of network activities.
- Configure alerts and notifications for security incidents.

5.2 Maintenance and Updates

Maintenance and Updates:

- Perform regular system maintenance, including software updates and patches.
- Ensure the system remains secure and up-to-date.

Phase 6: Documentation and Knowledge Transfer

6.1 Documentation

Documentation:

- Create comprehensive documentation of the Cisco ISE configuration, policies, and procedures.
- Develop user guides and documentation for end-users.

6.2 Knowledge Transfer

Knowledge Transfer:

- Provide knowledge transfer sessions to the IT team for ongoing management and support.
- Ensure that the IT team is well-equipped to handle Cisco ISE operations.

Project Resources

- Cisco ISE appliances and licenses.
- IT staff with Cisco ISE expertise.
- Network administrators and security personnel.
- Project management tools and software.

Project Risks and Mitigation

- **Risk**: Network disruptions during deployment.
    - **Mitigation**: Perform deployment during non-business hours and have a rollback plan in place.
- **Risk**: User resistance to new authentication methods.
    - **Mitigation**: Provide user training and support, and communicate the benefits of the new system.
- **Risk**: Compliance and security policy misalignment.
    - **Mitigation**: Regularly review and update policies to align with changing requirements.

Project Communication

- Regular project status meetings with stakeholders.
- Updates and notifications to end-users about the Cisco ISE deployment.
- Clear and transparent communication channels for issue reporting.

Project Completion

- Successful deployment and testing of Cisco ISE.
- User onboarding and training completed.
- Documentation and knowledge transfer delivered.
- Ongoing monitoring and maintenance plan in place.

Project Sign-off

- Project Sponsor: [ABC Company Executive]
- Project Manager: [Your Name]
- Date: [Completion Date]

Test Case for Advanced Cisco ISE Implementation

Test Case ID: TC_ADV_CISCO_ISE_001

Title: Validate Advanced Cisco ISE Implementation Across Multi-Site Network

Objective: To ensure that the Cisco ISE implementation across all sites is functioning as expected, with all advanced features being tested for efficacy and reliability.

Test Environment:

- Cisco ISE deployed across 4 sites.
- Network setups including wired, wireless, and VPN access.
- Various devices representing typical user scenarios (including BYOD).
- Integration with existing network security tools.

Preconditions:

- Cisco ISE is fully deployed and configured with all intended features.
- Test accounts and scenarios are set up for different user roles and access levels.

Test Steps:

1. **User Authentication and Authorization:**
    - **Action:** Test user access across different network access methods (wired, wireless, VPN).
    - **Expected Result:** Users are authenticated and authorized according to their roles and access policies.
2. **Dynamic Access Control:**
    - **Action:** Validate dynamic access control policies for various user groups and devices.
    - **Expected Result:** Access control policies are correctly applied and enforced.
3. **Network Visibility:**
    - **Action:** Review the visibility features for monitoring user and device activity on the network.
    - **Expected Result:** Comprehensive network visibility and reporting capabilities.
4. **BYOD Policy Enforcement:**
    - **Action:** Test BYOD scenarios for compliance with organizational policies.
    - **Expected Result:** BYOD devices comply with security policies and access controls.

5. **Guest Access Management:**
    - **Action:** Verify guest networking access and restrictions.
    - **Expected Result:** Guests have appropriate access with enforced security limitations.
6. **Security Integration:**
    - **Action:** Test integration with firewalls, intrusion prevention systems, and endpoint protection.
    - **Expected Result:** Seamless integration and data sharing with other security tools.
7. **Micro-Segmentation and TrustSec:**
    - **Action:** Validate network segmentation policies and TrustSec implementation.
    - **Expected Result:** Effective segmentation and security policy enforcement.
8. **High Availability and Redundancy:**
    - **Action:** Simulate failover scenarios to test system redundancy.
    - **Expected Result:** System failover occurs smoothly with no loss of functionality.
9. **Compliance and Reporting:**
    - **Action:** Generate compliance reports and audit logs.
    - **Expected Result:** Accurate and detailed reporting meeting compliance requirements.
10. **Multi-Site Synchronization:**
    - **Action:** Ensure configurations and policies are synchronized across all sites.
    - **Expected Result:** Consistent policy enforcement and user experience across all locations.

Postconditions:

- Restore any settings changed for testing purposes.
- Ensure no residual test data poses a security risk.

Pass/Fail Criteria:

- Pass: All features function as expected, with policies and integrations correctly applied.
- Fail: Any feature does not perform as expected, or integration issues are encountered.

Remarks:

Sample Test Case for 2-Node Cisco ISE Active-Passive Deployment

Test Case ID: TC_2NODE_ISE_APP_001

Title: Validate Functionality and Failover in 2-Node Cisco ISE Active-Passive Deployment

Objective: To ensure that the Cisco ISE 2-node setup operates correctly in an active-passive configuration, with seamless failover and consistent performance.

Test Environment:

- Two Cisco ISE nodes configured in an active-passive setup.
- Network infrastructure that includes switches, routers, and end-user devices for testing authentication and policies.
- Test accounts for different access scenarios.

Preconditions:

- Both Cisco ISE nodes are installed, configured, and networked.
- Active node is handling all the authentication requests under normal operations.
- Passive node is in standby, ready to take over when the active node fails.

Test Steps:

1. **Verify Initial Configuration:**
    - **Action:** Check configurations on both active and passive ISE nodes.
    - **Expected Result:** Configurations are identical and correct on both nodes.
2. **Normal Operation Testing:**
    - **Action:** Test various authentication scenarios on the active ISE node.
    - **Expected Result:** Authentication processes work correctly with the active node.
3. **Failover Testing:**
    - **Action:** Simulate failure of the active node (e.g., network disconnection, power off).
    - **Expected Result:** The passive node automatically takes over with minimal disruption.
4. **Failback Testing:**
    - **Action:** Restore the active node and test failback operation.
    - **Expected Result:** Control is seamlessly transferred back to the original active node.
5. **Data Synchronization Check:**

- **Action:** Verify that data and configurations are synchronized post-failover and failback.
- **Expected Result:** Both nodes have synchronized configurations and data.

6. **Performance Benchmarking:**
   - **Action:** Monitor and record system performance metrics during normal operation, failover, and failback.
   - **Expected Result:** Performance remains within acceptable thresholds.
7. **Redundancy Mechanism Verification:**
   - **Action:** Check the redundancy mechanisms and configurations.
   - **Expected Result:** Redundancy settings are correctly configured as per best practices.
8. **Logging and Alert Testing:**
   - **Action:** Review system logs for failover and failback events.
   - **Expected Result:** Appropriate logs and alerts are generated during failover scenarios.
9. **User Experience Monitoring:**
   - **Action:** Test and monitor user experience during failover.
   - **Expected Result:** Users experience minimal or no disruption during the failover process.
10. **System Health Check:**
    - **Action:** Perform a comprehensive system health check post-testing.
    - **Expected Result:** Both nodes are healthy with no critical issues.

Postconditions:

- Ensure both nodes are back in their initial states (active-passive) with normal operations resumed.
- Confirm that no residual configuration or data discrepancies exist between the nodes.

Pass/Fail Criteria:

- Pass: All test steps are executed successfully; failover and failback processes are seamless with data and configuration integrity maintained.
- Fail: Any of the test steps do not meet the expected results, or issues are observed in synchronization, performance, or user experience.

Remarks:

- Document any anomalies or issues encountered for further analysis and resolution.

- This test case aims to ensure high availability and reliability of the Cisco ISE deployment in an active-passive setup.

Cisco ISE Implementation Questions with Options:

1. What is the primary objective or goal for implementing Cisco ISE in your organization?
    - a) Enhancing network security through user and device authentication.
    - b) Enforcing access control policies for compliance.
    - c) Improving visibility and monitoring of network activity.
    - d) Streamlining guest access and onboarding.
2. Can you provide an overview of your current network infrastructure and the role Cisco ISE will play within it?
    - a) We have a well-defined network infrastructure.
    - b) Our network is complex, and we need to simplify management.
    - c) We're expanding and require better scalability.
    - d) We need to enhance security and access control.
3. Do you have a documented list of the network devices that will integrate with Cisco ISE for authentication and access control?
    - a) Yes, we have a comprehensive list.
    - b) Some devices are documented, but we need help identifying others.
    - c) We don't have a list, and we need assistance with device discovery.
    - d) We have no idea which devices need integration.
4. Are there specific compliance or security standards that you need to adhere to, and how will Cisco ISE assist in meeting those requirements?
    - a) We have specific compliance standards to meet.
    - b) Security is a concern, but no specific standards are mandated.
    - c) We're unsure about compliance requirements.
    - d) Compliance is not a priority.
5. What is the estimated number of users and devices that will be managed and authenticated through Cisco ISE?
    - a) Fewer than 100 users/devices.
    - b) 100-500 users/devices.
    - c) 500-1,000 users/devices.
    - d) More than 1,000 users/devices.

6. Have you identified the authentication methods you plan to use with Cisco ISE, such as 802.1X, MAB, or web authentication?
    - a) We plan to use 802.1X exclusively.
    - b) A combination of 802.1X and MAB.
    - c) We're considering web authentication.
    - d) We're not sure about authentication methods.
7. Are there any existing identity sources, such as Active Directory or LDAP, that need to be integrated with Cisco ISE for user identity information?
    - a) Yes, we use Active Directory.
    - b) LDAP integration is needed.
    - c) No existing identity sources.
    - d) We're not sure about integration needs.
8. What network policies and access control rules do you envision implementing with Cisco ISE?
    - a) Strict policies for secure access.
    - b) Limited policies for basic control.
    - c) No specific policies defined.
    - d) We're unsure about policy requirements.
9. Do you have specific network segments or areas that require different access policies, and if so, how will these be defined in Cisco ISE?
    - a) Yes, we have defined segments.
    - b) Some segments need separate policies.
    - c) No segment policies identified.
    - d) We need guidance on segment policies.
10. Are there any guest access or guest portal requirements that Cisco ISE needs to support?
    - a) Yes, we require guest access.
    - b) Guest access is needed with limited features.
    - c) No guest access requirements.
    - d) We're uncertain about guest access.
11. What is your preferred deployment model for Cisco ISE?
    - a) On-premises deployment.

- b) Cloud-based deployment (Cisco ISE Cloud).
- c) Hybrid deployment (combination of on-premises and cloud).
- d) Not sure about the deployment model.

12. Do you have existing network access policies or configurations that need to be migrated or integrated into Cisco ISE?
    - a) Yes, we have existing policies to migrate.
    - b) Some policies need to be integrated.
    - c) No existing policies to consider.
    - d) We're unsure about policy migration.
13. What level of reporting and monitoring capabilities are essential for your organization within Cisco ISE?
    - a) Comprehensive reporting and real-time monitoring.
    - b) Basic reporting and minimal monitoring.
    - c) No specific reporting or monitoring needs.
    - d) We need guidance on reporting and monitoring.
14. Have you identified the devices or endpoints that will be subject to profiling and posture assessment using Cisco ISE?
    - a) Yes, we have a list of devices.
    - b) Some devices identified for profiling.
    - c) No device profiling planned.
    - d) We're not sure about device profiling.
15. Are there any third-party integrations or security solutions that need to work alongside Cisco ISE, such as SIEM systems or firewall solutions?
    - a) Yes, we have specific integrations.
    - b) We're considering third-party integrations.
    - c) No third-party integrations planned.
    - d) We need guidance on integrations.
16. What is your preferred method for handling authentication failures or non-compliance issues detected by Cisco ISE?
    - a) Immediate network access denial.

- b) Limited network access with remediation.
- c) No specific method defined.
- d) We're unsure about handling failures.

17. Do you require assistance with user training and onboarding for Cisco ISE?
    - a) Yes, we need user training.
    - b) Basic user onboarding required.
    - c) No user training needed.
    - d) We're uncertain about user training.
18. How critical is high availability (HA) and redundancy for Cisco ISE in your environment?
    - a) High availability is critical (24/7 operation).
    - b) HA is important, but not 24/7.
    - c) Redundancy is not a top priority.
    - d) We need guidance on HA and redundancy.
19. Are there specific compliance audits or regulatory requirements that Cisco ISE should help address?
    - a) Yes, we have compliance audits.
    - b) Some compliance requirements to consider.
    - c) No specific compliance needs identified.
    - d) We're unsure about compliance requirements.
20. What is your timeline for the Cisco ISE implementation project?
    - a) Urgent - need to start immediately.
    - b) Within the next 3-6 months.
    - c) Within the next 6-12 months.
    - d) No specific timeline defined.

21. Which identity sources do you plan to integrate with Cisco ISE for user authentication?
    - a) Active Directory (AD).
    - b) Lightweight Directory Access Protocol (LDAP).
    - c) Remote Authentication Dial-In User Service (RADIUS).

- d) Security Assertion Markup Language (SAML).
- e) Other (please specify).
- f) No specific identity source identified.

22. Are there any specific network access control (NAC) use cases you want to address with Cisco ISE? Please select all that apply:
    - a) Guest network access control.
    - b) Bring Your Own Device (BYOD) policies.
    - c) Endpoint compliance checking.
    - d) Role-based access control (RBAC).
    - e) IoT device segmentation.
    - f) Other (please specify).
    - g) No specific NAC use case identified.
23. What is your preferred method for Cisco ISE policy enforcement?
    - a) 802.1X (Port-based) enforcement.
    - b) Web Authentication (Captive Portal).
    - c) Posture Assessment (Health checks).
    - d) Security Group Tagging (SGT).
    - e) VLAN assignment.
    - f) Other (please specify).
    - g) Not sure about policy enforcement method.
24. Do you have a disaster recovery plan in place for Cisco ISE in case of system failures?
    - a) Yes, we have a documented DR plan.
    - b) DR planning in progress.
    - c) No DR plan in place.
    - d) We need guidance on DR planning.
25. How do you plan to handle software updates and patches for Cisco ISE?
    - a) Regularly apply updates and patches.
    - b) Schedule updates during maintenance windows.
    - c) No specific update strategy.

- d) We need guidance on update management.

26. Have you considered scalability requirements for Cisco ISE to accommodate potential growth in the number of users and devices?
    - a) Yes, scalability is a key consideration.
    - b) Scalability is important but not the top priority.
    - c) No specific scalability requirements identified.
    - d) We need guidance on scalability planning.
27. What level of integration with Cisco Identity Services Engine (ISE) APIs and SDKs do you envision for your organization?
    - a) Extensive use of APIs and SDKs for customization.
    - b) Some API and SDK integrations.
    - c) Limited use of APIs and SDKs.
    - d) No specific integration plans.
    - e) We need guidance on API and SDK usage.
28. Do you have a documented access control policy or security policy that will guide the configuration of Cisco ISE?
    - a) Yes, we have a documented policy.
    - b) Policy development in progress.
    - c) No specific policy in place.
    - d) We need assistance with policy development.
29. Are there specific compliance standards or frameworks (e.g., HIPAA, GDPR, NIST) that your organization must adhere to with Cisco ISE?
    - a) Yes, we must adhere to specific compliance standards.
    - b) Compliance considerations but no specific standards identified.
    - c) No specific compliance requirements.
    - d) We need guidance on compliance standards.
30. Have you designated a project lead or point of contact responsible for the Cisco ISE implementation project?
    - a) Yes, we have a designated project lead.
    - b) In the process of designating a lead.

- c) No designated project lead yet.
- d) Not sure about the project lead.