# The Anatomy of a Contextual and Dynamic Access Policy

*A Foundation in Identity Governance Controls*

**Frank Briguglio, CISSP**

**Federal CTO, SailPoint**

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

# Contextual and Dynamic Access Policies

**Definition**

A contextual and dynamic access policy adapts access decisions based on real-time signals, such as user identity, behavior, location, device security, and environmental risks. It ensures that access is granted based on the current context rather than static attributes, reducing the risk of over-provisioning or unauthorized access.

**Core Elements**

1. **Contextual Awareness:**
    - Access is granted based on real-time context, such as:
        - User behavior (e.g., login time, frequency).
        - Device posture (e.g., OS version, encryption status).
        - Location (e.g., IP address, geofencing).
        - Environmental signals (e.g., time of day, threat intelligence).
2. **Dynamic Decision-Making:**
    - Policies enforce least privilege dynamically by assessing context and risks.
    - Incorporates risk-based authentication (e.g., MFA triggered only for high-risk scenarios).
3. **Integration with Identity Governance:**
    - Enforces access policies through a foundation of identity governance, ensuring that users are only granted access aligned with their roles, responsibilities, and compliance requirements.

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

## Identity Governance Controls

Identity governance controls are the foundation for establishing a secure and compliant access ecosystem. They provide the structure and policies necessary to support dynamic decision-making.

**Key Components of Identity Governance**

1. **Role-Based Access Control (RBAC):**
    - Defines roles and associated entitlements to ensure consistent access management.
    - Helps minimize excessive or inappropriate access.
2. **Access Reviews:**
    - Periodic validation of user access rights to ensure continued alignment with business needs and compliance.
3. **Separation of Duties (SoD):**
    - Prevents conflicts of interest by ensuring no individual has excessive control over critical processes.
4. **Lifecycle Management:**
    - Automates the provisioning, modification, and de-provisioning of access based on changes in user roles or statuses.
5. **Policy Framework:**
    - Establishes baselines for access policies (e.g., who can access what, when, and under what conditions).

## Runtime Evaluation vs. Governance Controls

**Runtime Evaluation**

- **Definition:** Access decisions made dynamically in real-time, based on the current context.
- **Purpose:** Focuses on immediate risk mitigation and situational awareness.
- **Characteristics:**
    - Continuous monitoring and evaluation of access requests.

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

    - Incorporates real-time signals like device posture, user behavior, and location.
    - Examples:
        - Triggering MFA if a login request is from an untrusted device.
        - Denying access to sensitive data outside office hours.

- **Benefits:**
    - Enhance security by responding to evolving threats.
    - Reduces the attack surface by enforcing least privilege dynamically.

**Governance Controls**

- **Definition:** Predefined policies and frameworks that govern access over time.
- **Purpose:** Provides structure, consistency, and compliance for access management.
- **Characteristics:**
    - Policy-driven and role-based.
    - Focus on defining long-term access requirements and compliance.
    - Examples:
        - Role assignments for employees based on their job function.
        - Regular access reviews to ensure continued compliance with governance policies.
- **Benefits:**
    - Promotes accountability through structured access management.
    - Ensures compliance with regulatory requirements.

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

**Integration of Governance Controls with Runtime Evaluation**

The true strength of contextual and dynamic access policies lies in their integration with identity governance controls. Together, they create a layered, adaptive approach to access management:

1. **Baseline Governance:**
    - Establishes the foundational "who should have access to what" through role-based policies and lifecycle management.
2. **Dynamic Contextualization:**
    - Enhances governance with real-time decision-making, ensuring that access aligns with the current context and risk level.
3. **Feedback Loops:**
    - Runtime evaluations inform governance by providing insights into user behavior and anomalies, which can refine future policies.

**Challenges and Considerations**

1. **Balancing Security and Usability:**
    - Overly stringent runtime policies can hinder productivity, while weak policies can expose vulnerabilities.
2. **Scalability:**
    - Dynamic policies must scale effectively across complex, hybrid environments.
3. **Compliance Alignment:**
    - Policies must ensure compliance with industry standards and regulations, such as DoD instructions, DHS CISA Guidance, and NIST Frameworks and Special Publications (see the special section below *Compliance and Alignment with Standards and Guidance*)

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

**Wrapping Up**

Contextual and dynamic access policies, underpinned by robust identity governance controls, represent a significant advancement in access management. While governance controls provide a structured foundation, runtime evaluation offers the flexibility and responsiveness needed in today's dynamic threat landscape. Together, they ensure secure, compliant, and user-friendly access to critical resources.

By integrating governance controls and runtime evaluation, organizations can protect assets, mitigate risks, and empower users, aligning security objectives with business needs.

## Compliance and Alignment with Standards and Guidance

Contextual and dynamic access policies, supported by identity governance controls, align with several key frameworks and standards to ensure security, compliance, and operational resilience.

**Key Benefits of Standards Alignment**

1. **Enhanced Security Posture:**
    - Standards and frameworks emphasize best practices for secure and compliant access management, which dynamic policies inherently support.
2. **Operational Efficiency:**
    - Automating compliance checks and runtime evaluation reduces administrative overhead and enhances response times.
3. **Regulatory Compliance:**
    - Adherence to frameworks ensures that organizations meet legal and regulatory obligations, avoiding penalties and reputational damage.

This section explores how these policies adhere to and support compliance with the following frameworks and guidance:

**NIST Special Publication 800-207 (Zero Trust Architecture)**

- **Alignment:**
    - **Dynamic Policy Enforcement:** NIST SP 800-207 emphasizes the need for real-time access decisions based on contextual factors, such as user

identity, device health, and environmental risk, aligning closely with dynamic access policies.

- **Least Privilege Access:** Dynamic policies enforce least privilege by continuously evaluating access against real-time signals, a core tenet of zero trust.
- **Continuous Verification:** Runtime evaluation supports the zero trust principle of ongoing verification rather than static, one-time authentication.

- **Implementation Examples:**
  - Using runtime evaluation to grant access only to devices that meet security posture requirements (e.g., encryption enabled, updated antivirus).
  - Dynamically restricting access to critical assets based on real-time risk assessments.

**NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations)**

- **Alignment:**
  - **Access Control (AC):** Dynamic access policies align with the AC family of controls, particularly AC-2 (Account Management), AC-3 (Access Enforcement), and AC-5 (Separation of Duties).
  - **Risk Assessment (RA):** Policies integrate real-time risk assessments to enforce conditional access.
  - **System and Communications Protection (SC):** Continuous monitoring of communication channels aligns with SC-7 (Boundary Protection) and SC-12 (Cryptographic Key Establishment).
- **Implementation Examples:**
  - Automating user access reviews (AC-2) and dynamically modifying privileges based on user behavior and context (AC-6).
  - Enforcing multi-factor authentication (MFA) dynamically for sensitive systems (IA-2).

**NIST Cybersecurity Framework (CSF)**

- **Alignment:**

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

  - **Identify:** Identity governance provides a foundation for identifying roles, entitlements, and responsibilities.
  - **Protect:** Contextual and dynamic access policies protect assets by enforcing real-time access controls.
  - **Detect:** Runtime evaluation enhances anomaly detection and provides insights into potential security incidents.
  - **Respond and Recover:** Feedback from runtime evaluations can inform incident response and refine governance policies.

- **Implementation Examples:**
  - Using dynamic policies to automatically detect and respond to high-risk login attempts.
  - Regularly updating governance controls to reflect insights from runtime evaluation data.

**DHS CISA Recommendations**

- **Alignment:**
  - **Zero Trust Maturity Model:** Dynamic access policies support CISA's focus on zero trust principles, particularly continuous validation of users and devices.
  - **Cybersecurity Incident Response:** Policies enhance resilience by dynamically mitigating risks in real time, reducing the potential impact of incidents.
  - **Critical Infrastructure Security:** Identity governance and dynamic policies ensure compliance with sector-specific cybersecurity requirements.
- **Implementation Examples:**
  - Limiting access to critical infrastructure components based on device and location context.
  - Enforcing additional authentication steps for high-value systems during suspected cyber events.

**DoD 8520.04 (Identity Authentication for Information Systems)**

- **Alignment:**

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

  - **Authentication and Identity Management:** DoD 8520.04 emphasizes the importance of strong identity verification, which is a core component of both identity governance and contextual access policies.
  - **PKI Integration:** Dynamic policies can leverage DoD Public Key Infrastructure (PKI) for secure, context-aware authentication.
  - **Access Control Policy (ACP):** Runtime evaluation ensures compliance with ACP requirements by dynamically adjusting access rights based on the current context.

- **Implementation Examples:**
  - Integrating CAC/PIV cards with contextual access policies for high-assurance environments.
  - Applying runtime risk assessment for access to classified systems, limiting exposure in case of a compromise.

**Other Relevant Standards and Guidance**

1. **ISO/IEC 27001 and 27002 (Information Security Management):**
   - Aligns with Annex A controls, particularly A.9 (Access Control) and A.12 (Operations Security).
   - Ensures policies are continuously evaluated against security risks and updated to meet compliance.
2. **GDPR (General Data Protection Regulation):**
   - Dynamic policies support GDPR by ensuring data access is limited to authorized individuals and only when necessary.
   - Identity governance ensures compliance with principles of data minimization and accountability.
3. **HIPAA (Health Insurance Portability and Accountability Act):**
   - Contextual access policies align with HIPAA Security Rules by safeguarding electronic protected health information (ePHI) through real-time access controls.

**The Anatomy of a Contextual and Dynamic Access Policy:**
**A Foundation in Identity Governance Controls**

## Conclusion

Dynamic and contextual access policies, when built on a foundation of identity governance, align effectively with NIST SP 800-207, 800-53, CSF, DHS CISA recommendations, and DoD 8520.04. This alignment ensures robust security, operational resilience, and compliance across diverse organizational and regulatory environments. By continuously evolving these policies in accordance with guidance and industry standards, organizations can achieve a proactive, adaptive, and compliant cybersecurity posture.