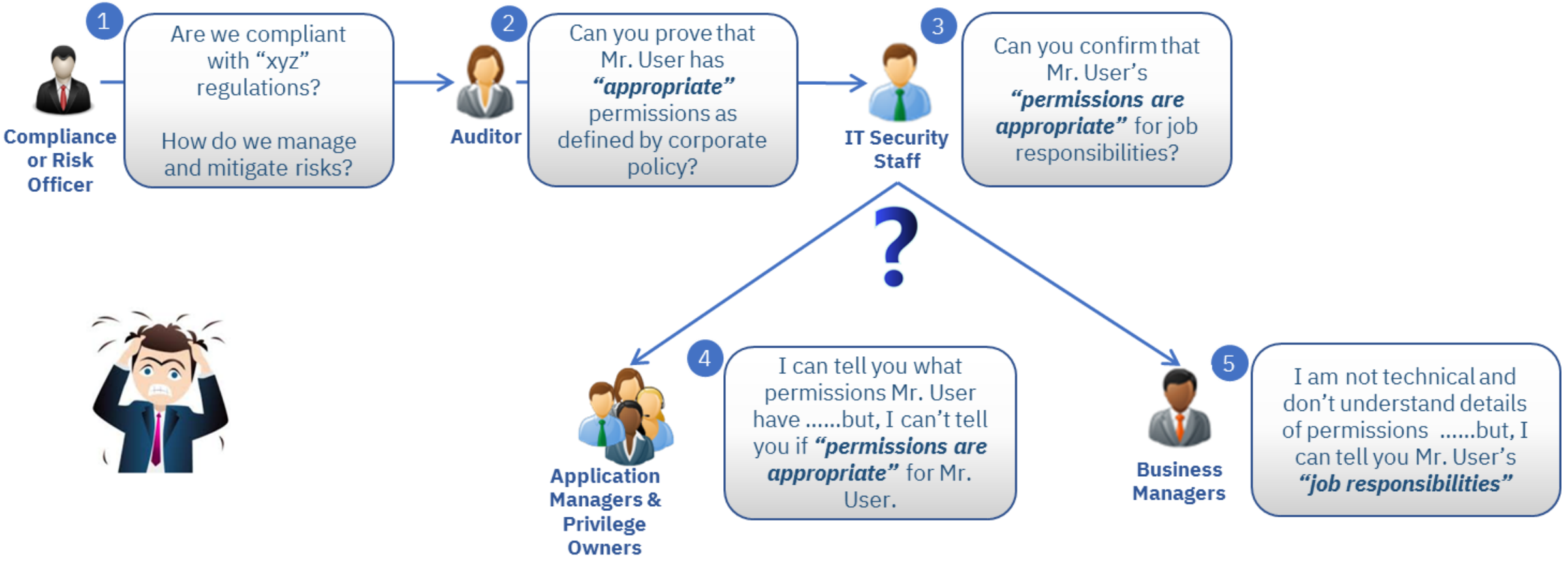
Access Governance

The Security Compliance Pain Chain



Traditional, silo-based approach to identity and access management leaves too many loose ends and engenders "compliance pain"

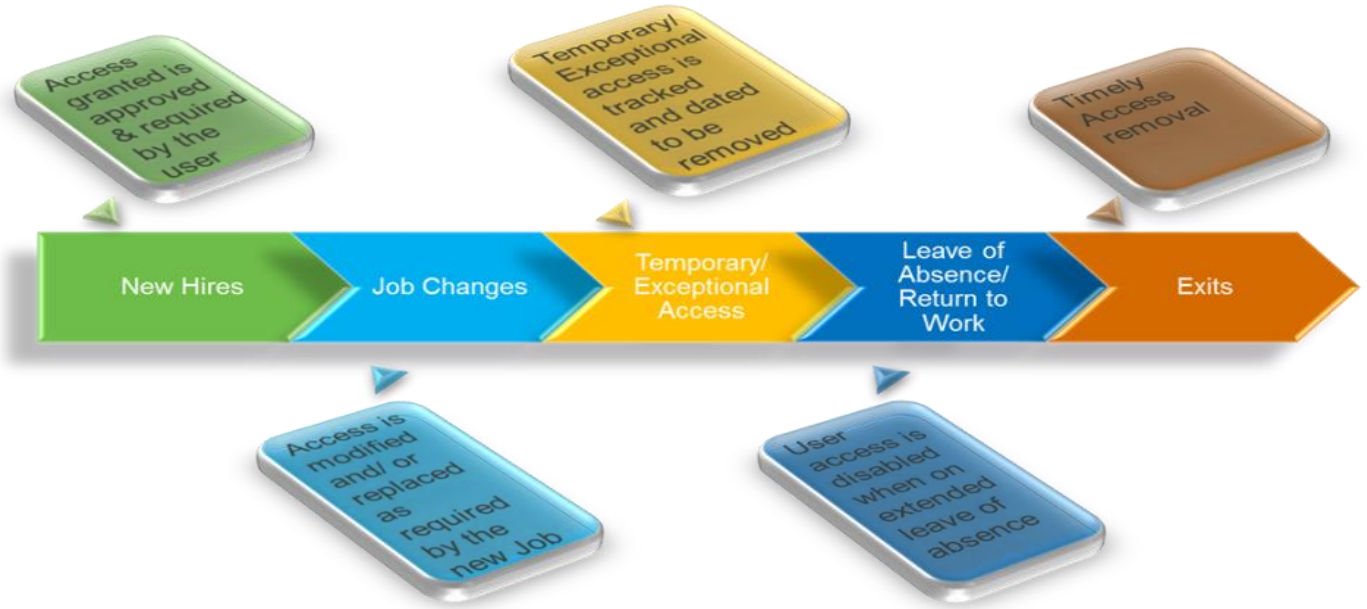
Identity Governance - Business Challenges

- Inefficient on-boarding, transfer and off-boarding processes of employees
  - Typically upward of 2 weeks
  - Large IT support staff to manage identity life cycle

- Ability to ensure the principle of least privilege.
  - Business managers cannot understand the entitlement details
  - Potential Segregation of duties (SoD) conflicts lead to security vulnerabilities
  - Management, IT, the end user and the Auditor all waste time

- Access Certifications don't get done well enough and often enough.
  - Lack of standard templates to provide business language to the entitlement
  - Large IT support staff to manage Certification
  - Lack of automated compliance report

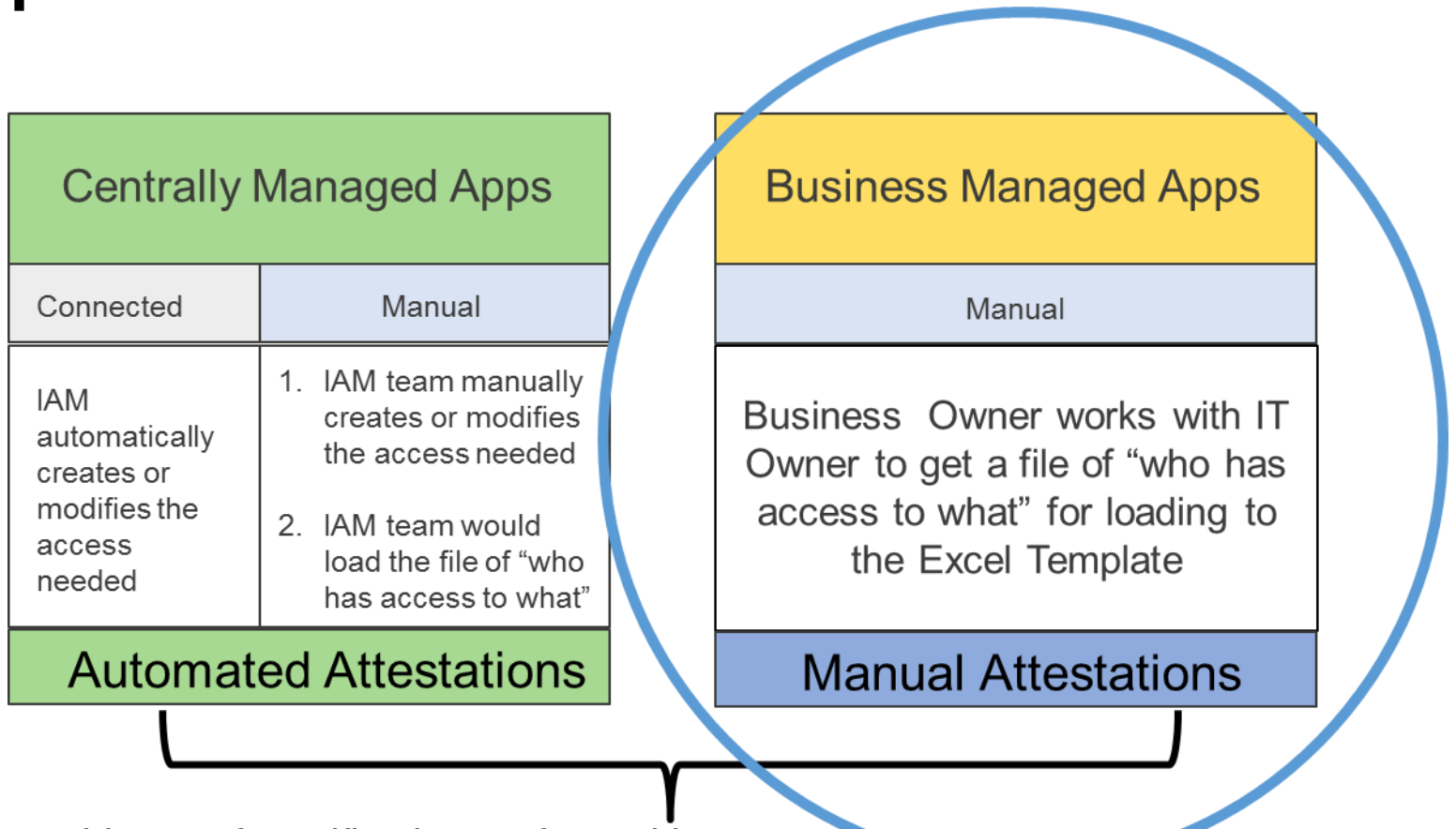
Importance of User access reviews & attestations



User Access Management is an On-going Process throughout the entire User's lifecycle

4

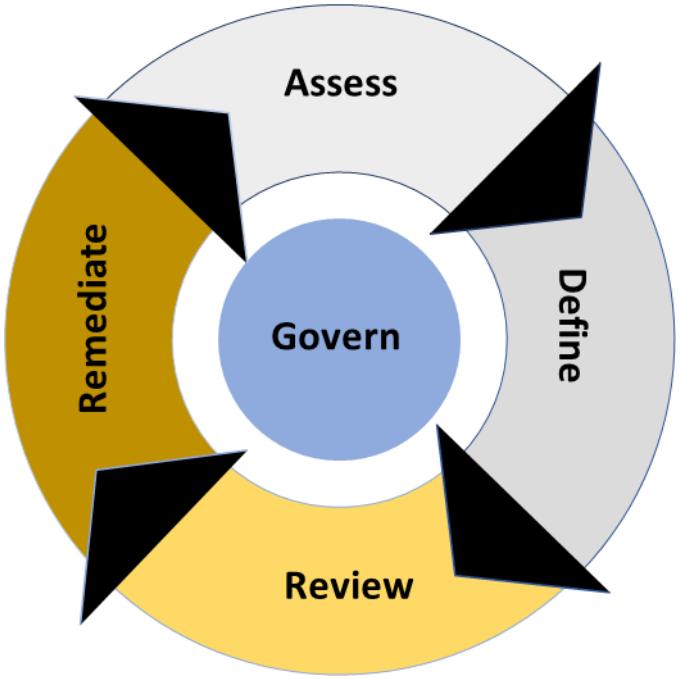
Attestation Landscape – How do we determine “who has access to what” in an application ?



- Evidence of Certification performed by Manager
- Metrics: Revocations vs. Keeps, Time to Revoke, Time to Complete, etc.
- Must complete process – only acceptable bar is 100% completion, every time

5

IAM Attestations: The Attestation Lifecycle



Govern

- Establish enterprise standards/principles
- Requirements & Controls for review
- Set Roles & Responsibilities for access review
- Perform Quality Assurance / Spot Checking
- Secure Sign-off's from IT and Business Owners

Assess

- Certification Type & Scope: Regular, or targeted sub-group
- Frequency: SOX/PCI and Privileged Access = Quarterly, all others Annually

Define

- Retrieve access information into Attestation Templates
- Educate on Review & Remediation
- Provide Training; Kick-off review cycle

Review

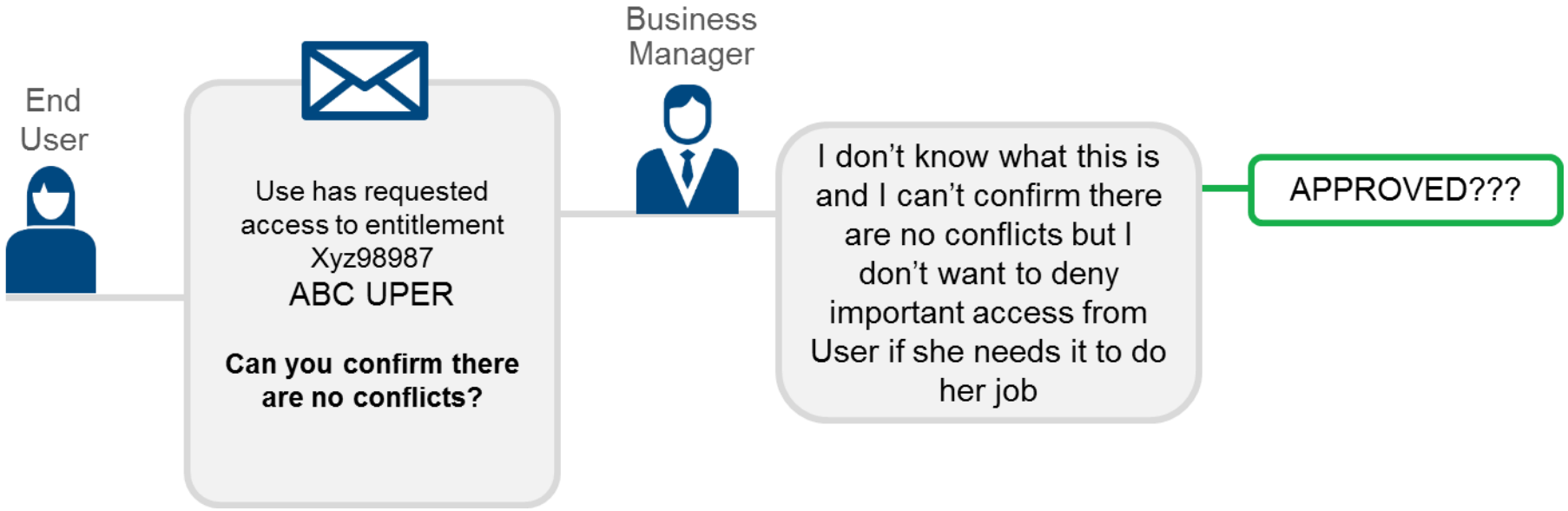
- Conduct user access reviews: **Manager-based**
- Continuous Progress Reports weekly
- Support & assistance to Business where needed

Remediate

- Remediate user access as within 48 hours after closure of review
- Ticket/Closure or Evidence of remediation required for Audit
- Additional access pulls might be required to provide evidence of removals

6

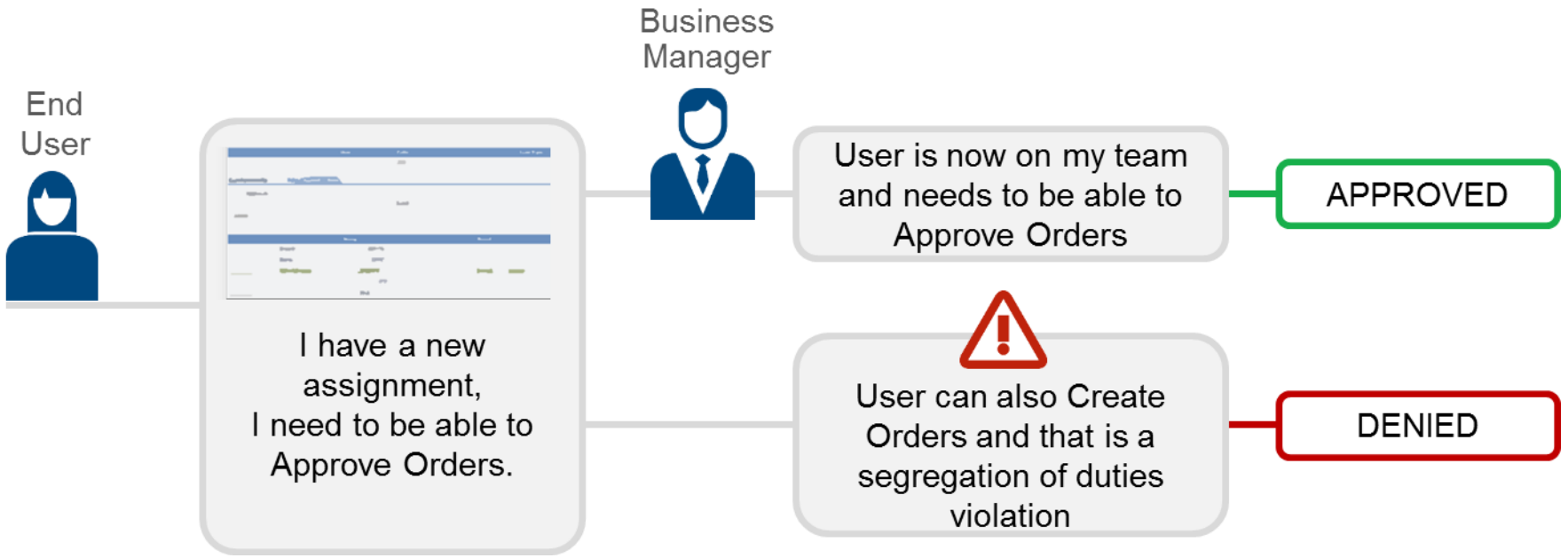
The old way – Process-driven access request management



- Business managers cannot understand the entitlement details
- Leads to overentitled users and noncompliance
- Potential Segregation of duties (SoD) conflicts lead to security vulnerabilities
- Management, IT, the end user and the Auditor all waste time

The new business centric way - Access request management

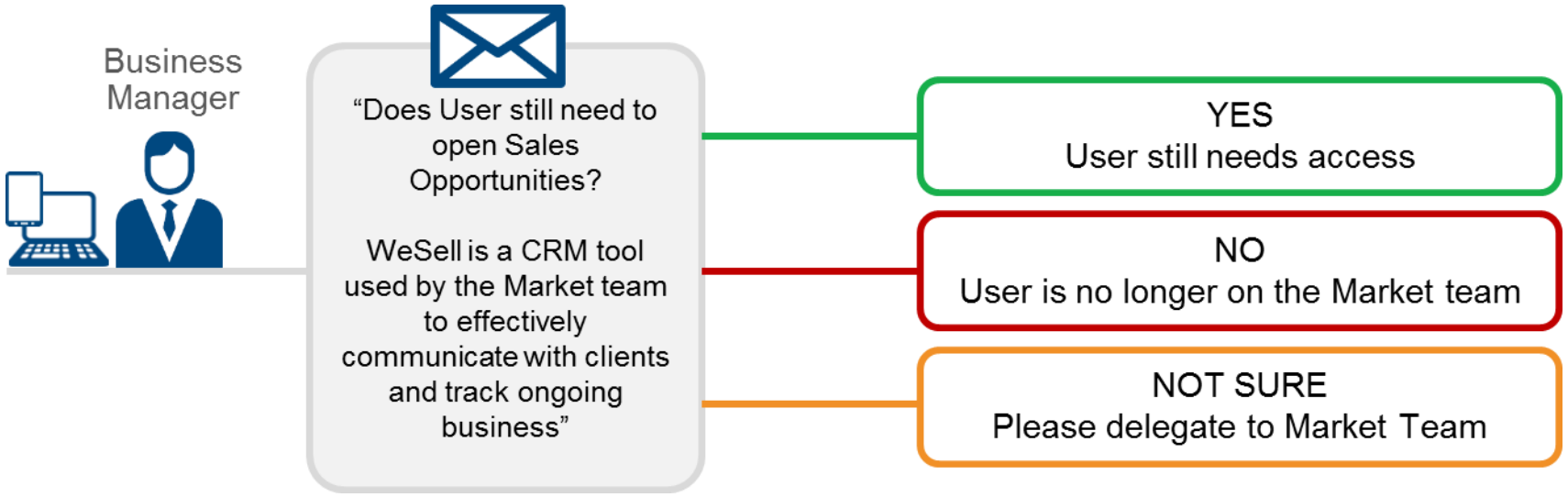
Simplify self-service access request for managers and employees



- Self-service, shopping cart interface
- “Speaks” business language but also understands the IT and application roles
- Automatically detects segregation of duties (SoD) conflicts
- Saves time, while ensuring proper and compliant user access

Business centric access certification

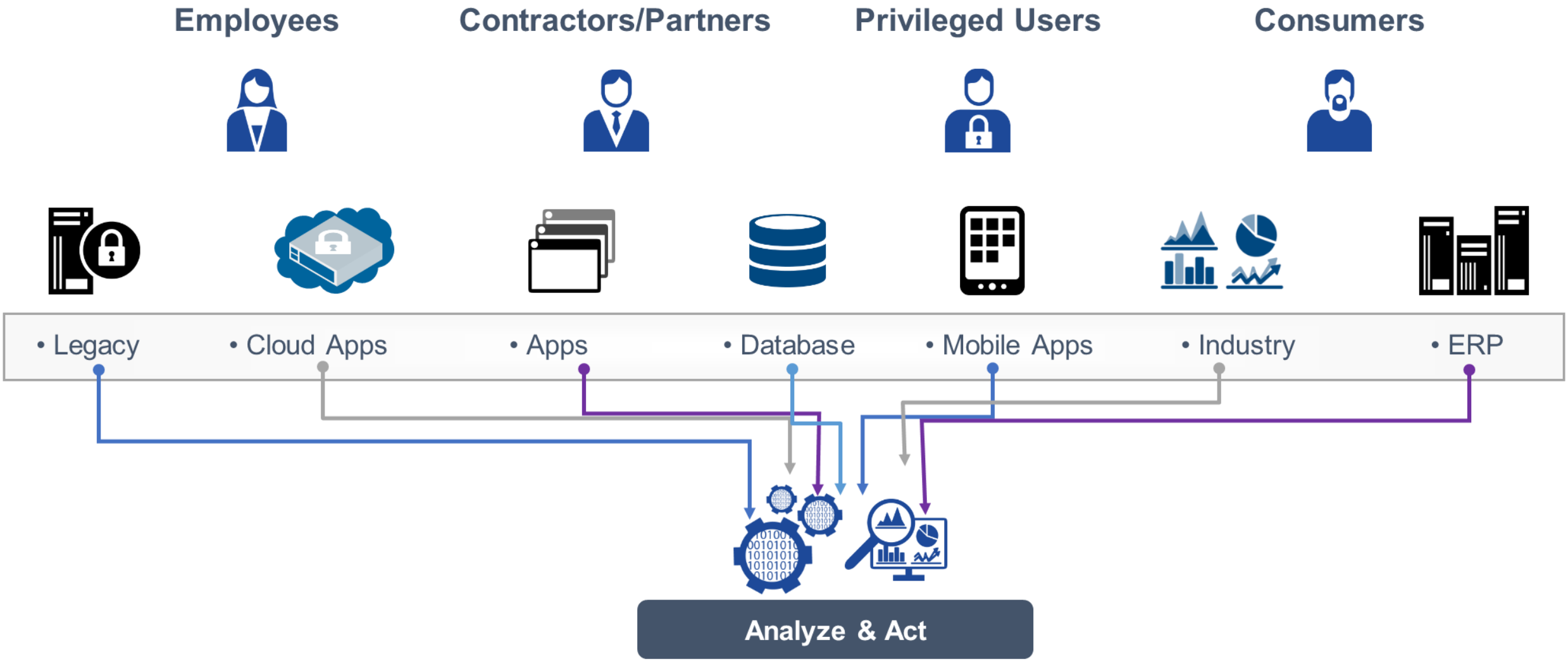
Enables business managers to quickly review employee access and take action



- Focused, risk-driven campaigns
- Managers can understand exactly what access they are certifying and why
- Same simple look and feel regardless of role within the organization
- Ability to execute multi-step approval workflows

User access and entitlement information is everywhere

How do we use it to automate processes? To mitigate risk? To remain compliant? To take action?



Identity Governance tools delivers key identity lifecycle and compliance controls

Seamless User Access Experience

- Simplify self-service user access management
- Automate user and identity lifecycle processes

Intelligent Analytics

- Identify and prioritize risky access or users
- Personalized, actionable dashboards

Continuous Compliance

- Visualize and certify user entitlements
- Provide insight into user risks
- Verify access visibility and context

Organizations are seeking a business-driven approach to Identity Governance and Intelligence

Identity and Governance Evolution

1 Administration

- Cost savings
- Automation
- User lifecycle
- Key on premise applications and employees

2 Governance

- Role management
- Access certification
- Extended enterprise and business partners
- On and off-premise applications

3 Analytics

- Application usage
- Privileged activity
- Risk-based control
- Baseline normal behavior
- Employees, partners, consumers – anywhere

Focus on identity intelligence: *Collect and analyze identity data*

Improve visibility into how access is being utilized

Prioritize compliance actions with risk-based insights

Make better decisions with clear actionable intelligence

Thank You