Taking Control of Your User Accounts
Identity Management Basics

DUSTIN PURYEAR
PURYEAR IT, LLC

Who are we?

Puryear IT, LLC
Baton Rouge, LA – 225-706-8414
http://www.puryear-it.com/

Managed Services for Networks, Security, Identity Management

Contact us for a free consultation
contact-us@puryear-it.com

Is Identity and Access Management Important?

“Breaches of identity and access management (IAM) lead to billions of dollars of losses each year, both reported and unreported.”

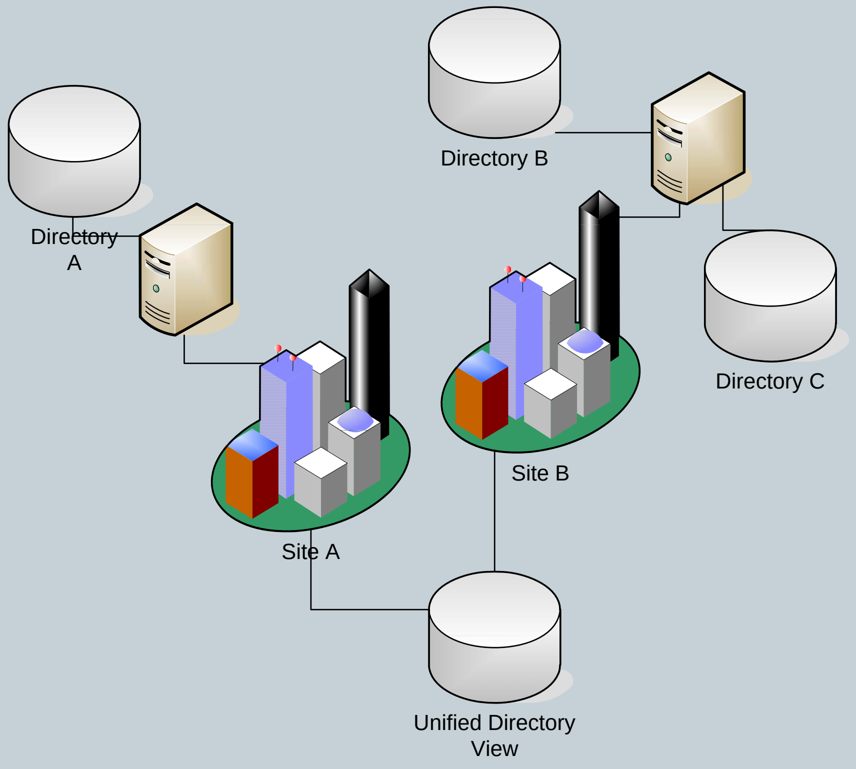
- Gartner

Forrester Research states that the average help desk labor cost for a single password reset is roughly $70.

But does it impact me?

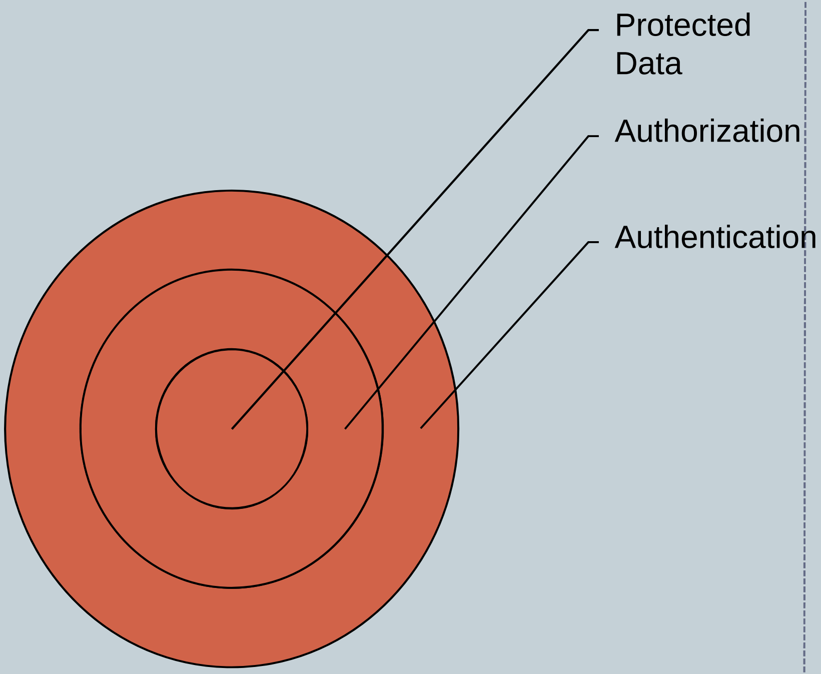
YOU BET IT DOES!

Directory Services



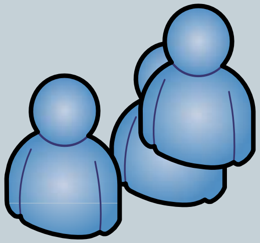
- Directories are a critical infrastructure component
  - Identity repositories
  - Metadata replication/synchronization services
  - Directory virtualization

Access Control



- Role-based Access Control
- Enterprise Single Sign On (ESSO)
- Web Single Sign On (WebSSO)
- Reduced Sign On
- Federation

Separation of Duties



Separation
Of Duties

- Critical for internal controls
- Implements checks and balances on individuals
- Reduces danger/risk of individual actions
- Can be difficult and expensive to implement
- Separate or Compensate
- Bread and butter of audit/compliance

Developing an Identity Management Roadmap

- Several steps involved:
  - Needs Analysis
  - Management Involvement
  - Team Involvement
  - Selecting Best Solution
  - Technical Design Decisions
  - Roll Out
  - Monitor/ROI

Needs Analysis

- Map existing processes into a set of business problems
- Map business problems into requirements
- Map requirements into technical specification
- Map technical specification into:
  - Technical selection
  - Implementation design

Issue: New Hires

- Business Problem
  - New hires require new accounts
  - Accounts must get proper access rights
  - How do we maintain SoD?
  - New hires must wait for process to complete!
- Business Solution
  - Automate on-boarding that relies on business rules and workflow/approvals
- Technical Solution
  - Define HR system as System of Record (SoR)
  - Creation of "minimum privileged" accounts based on HR data
  - Use of workflow to increase privileges

Issue: Costly User Administration

- Business Problem
  - Each application is a silo
  - Helpdesk can't easily change passwords
  - Lacks consistent audit trail
  - Inconsistent end-user information in databases
  - Security administrators perform user management activities
- Business Solution
  - Develop consistent user management process for administrators and helpdesk
  - Use SoR to define/update user information

- Technical Solution
  - Develop single interface to user management
  - Develop single interface for password management/changes
  - Develop automation of updates for "most critical" data
  - Identify SoD violations and eliminate!

Issue: Inconsistent Login IDs and Passwords

- Business Problem
  - Users have different Login IDs for applications
  - Users have too many passwords
  - Lack of consistency in password policy across the enterprise
- Business Solution
  - Develop enterprise Login ID convention
  - Migrate existing Login IDs to new convention
  - Develop enterprise password policy
  - Migrate existing passwords to new policy

- Technical Solution
  - Reconcile Login IDs to new convention using batch and manual methods
  - Implement consistent password policy
  - Implement password synchronization, reduced sign-on, single sign-on

Issue: Security Vulnerabilities

- Business Problem
  - Delayed terminations result in critical vulnerabilities
  - Disgruntled terminated staff
  - Unused/dormant accounts
  - Access rights increase over time
  - Access rights incorrectly granted: “Set the new guy up just like Susan in HR”
- Business Solution
  - Develop process/workflow to handle terminations
  - Periodically review/audit user access rights
  - Develop request and authorization process for increasing user access rights

- Technical Solution
  - Automate user account terminations via SoR
  - Develop automated reports for user access rights, focusing on exception reporting for elevated rights
  - Implement workflow solution for user access rights

Issue: Audit, Reporting

- Business Problem
  - Lack of audit trails within application silos
  - Many enterprise applications lack administrative logging
  - For those that have it, those applications don’t have a consistent log format
  - Difficult to monitor and enforce SoD policies
- Business Solution
  - Require enterprise-wide logging of accounts changes and use
  - Develop process to use account change and use logging for SoD reporting

- Technical Solution
  - Replace manual account management with software solutions that include logging capabilities
  - Enable SoD rules within user management solution to require workflow for SoD-sensitive positions

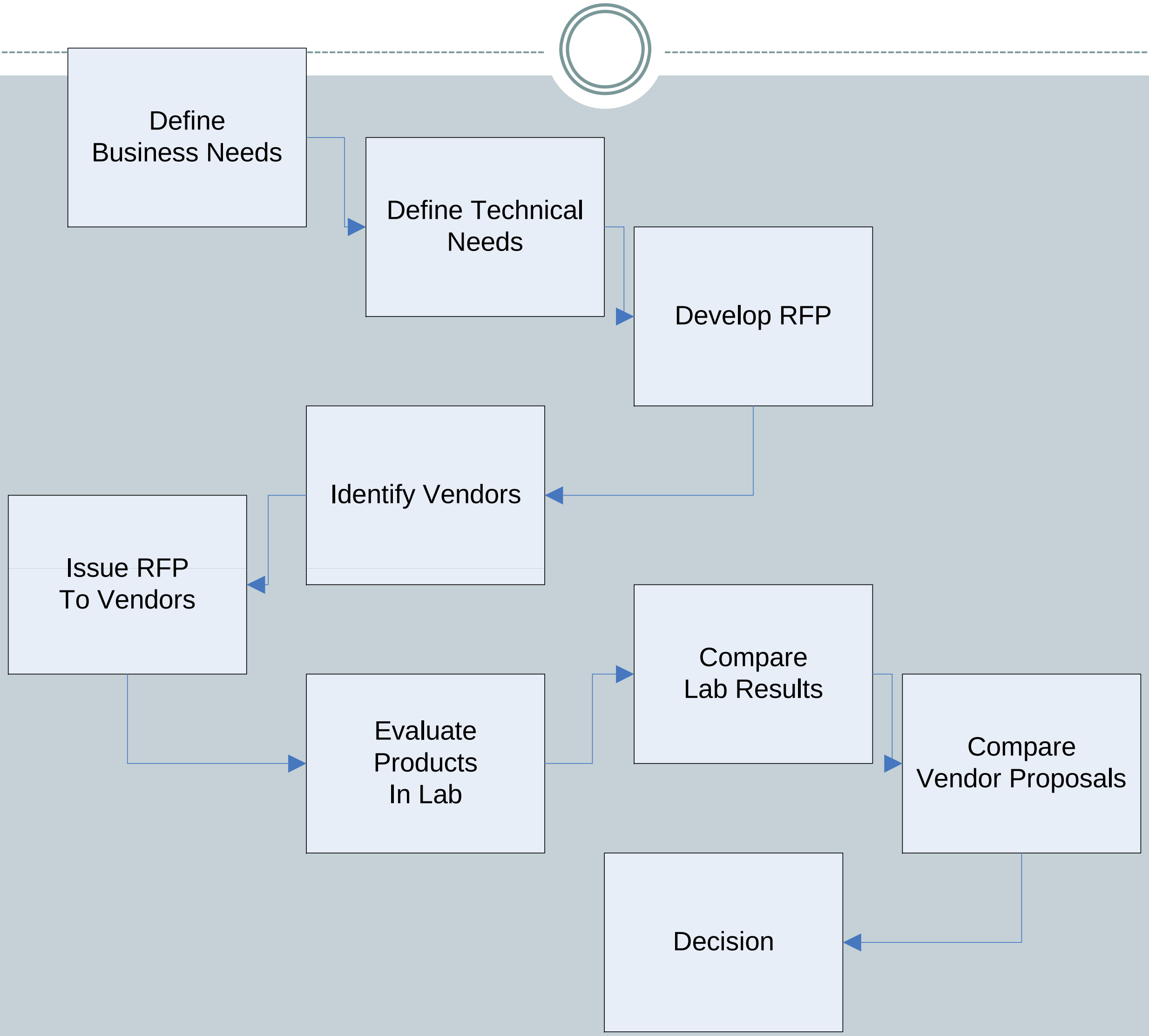
Management Involvement

- A mandate is crucial!
  - Develop a clear mandate
  - Outline likely issues/problems
- Budget
  - Software license
  - Support
  - Training
  - Hardware and support software
  - Professional Services
  - Internal Resources

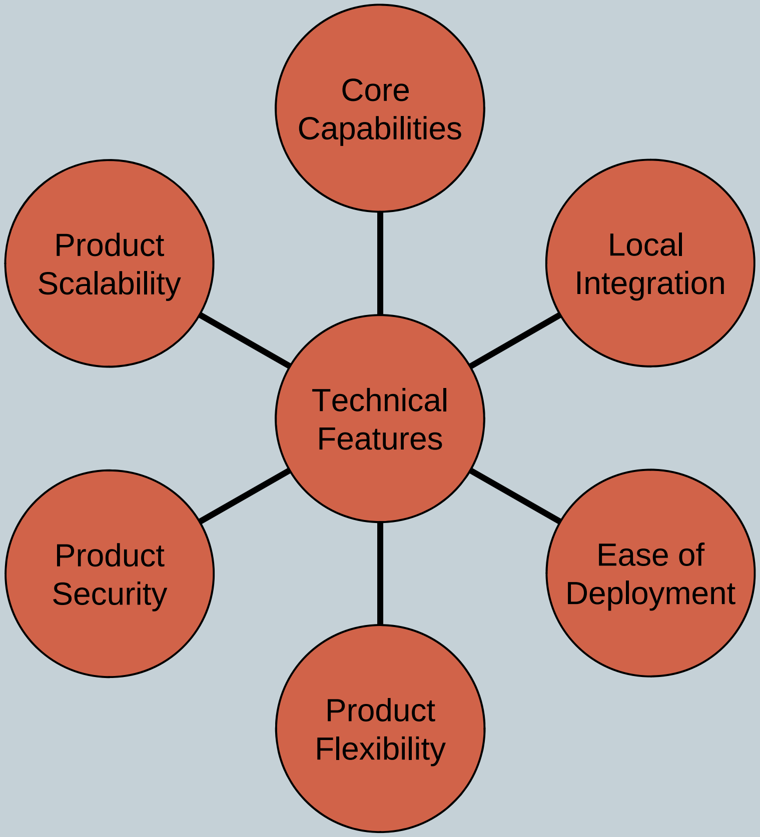
Team Involvement

- Security Administrators
- Security Managers
- Audit/Compliance
- Systems Administrators
- Human Resources

Selecting Best Solution



Identify Feature Requirements


Technical Features

Core Capabilities

Local Integration

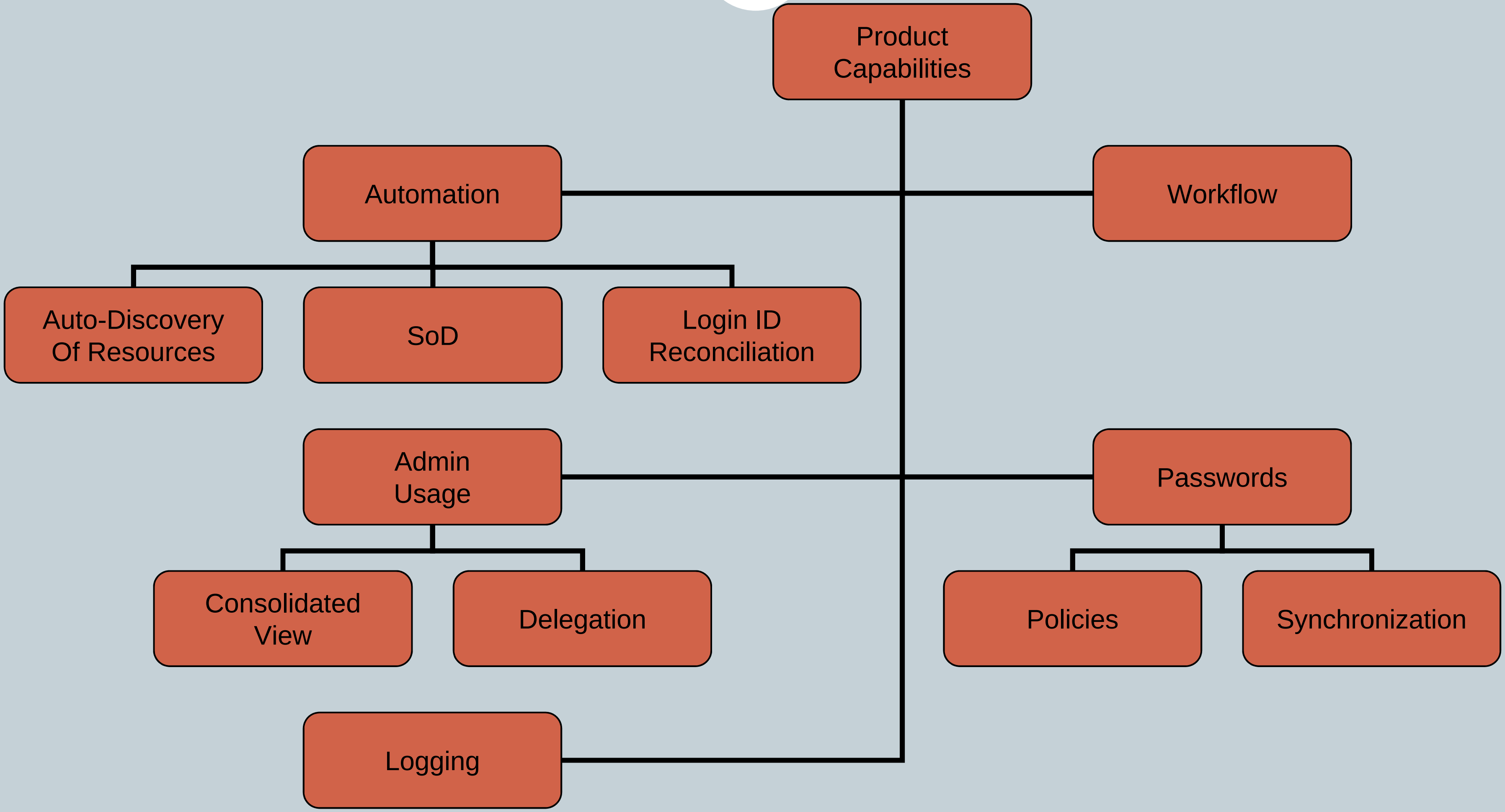
Ease of Deployment

Product Flexibility

Product Security

Product Scalability

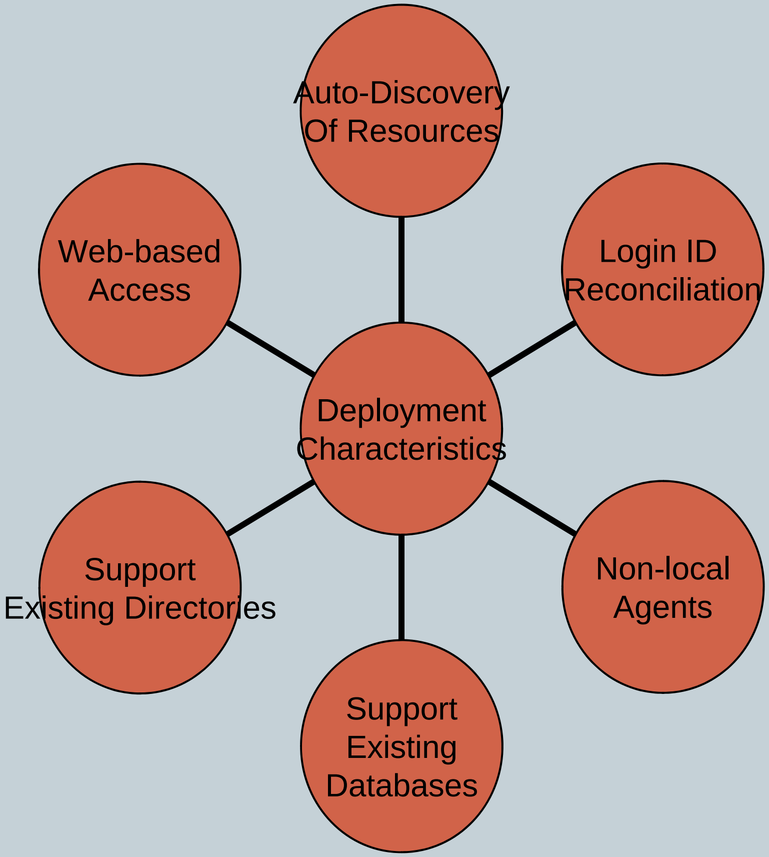
Core Capabilities



Local Integration

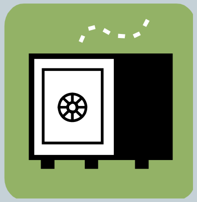
- *Localization is key to end-user acceptance!*
- Local language support
- Logo
- Corporate look&feel
- Customization of request forms
- Integration into helpdesk
- Ability to send emails
- Accessible for performance & availability monitoring
- Support for local network and application, e.g., AD, RSA

Ease of Deployment


Auto-Discovery Of Resources
Web-based Access
Login ID Reconciliation
Deployment Characteristics
Support Existing Directories
Non-local Agents
Support Existing Databases

- Deployment is the stumbling block for many organizations.
- Be sure to map your needs to the technical capabilities of the product!

Product Security



- Encryption
  - Local data
  - Remote access
- Authentication
  - Admin users
  - End-users/SSPR
  - Web Services
- Accountability
  - Logging
  - Reporting

Product Scalability

- Can it handle your current organization?
- Can your organization handle it?
- Can it handle your organization in the future?
- Calculating scalability requirements
  - Servers
  - Service layer
  - Network
  - Target systems

Product Flexibility

- Organization specific data elements
  - HR#
  - Student#
  - Job code
  - Facility
- Handle wide-range of applications
  - Network OS (NOS): AD, Novell, Linux/UNIX
  - Applications: Exchange, GroupWise, Mainframe apps
- Handle custom applications
  - Many enterprises have more custom applications than COTS applications

Octopus = Flexible

Get it?

Customization for Custom Applications

- Pre-built agents for common applications
- SDK for new custom agents
  - C++, Java is most common
  - Java: Oracle, Sun, CA
  - C#: Microsoft
- Developer documentation
- SDK should be free or low-cost
- ODBC Wizard!

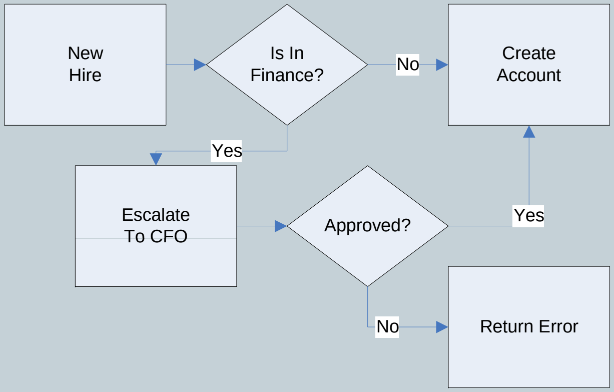
Password Management

- Deserves its own slide!
- Must support your password policies
  - Password complexity
  - Password expiration
- Think about password synchronization
- WebSSO, SSO, reduced sign-on!

Roll Out/Deployment

- Design and pilot stages are critical
  - Pilot stage will identify internal technical weaknesses
  - Failure to do a pilot can kill the project
- Pilot stage can help determine
  - Features to enable
  - User population that will access IdM solution
  - Security policies
    - Password policies
    - Authentication
    - Account configuration policies
  - Types of roles needed
- Develop SoR and IdM integration
- Develop request and workflow rules
- Helpdesk integration
  - Email only
  - Application-level integration

Request & Workflow Rules



- This is where the power really is!
  - What can be requested
  - What data must be included in request
  - Request validation
  - Request authorization
  - Request escalation

Training

- Update users about changes
  - Angry users translate to non-conforming users
- Train HR staff on SoR updates
  - The SoR is critical to accuracy
  - Bad data in the SoR may trigger inappropriate workflow rules
- Train Security Administrators
  - Local app management should be a no-no
  - Only available in “break-the-glass” situation
- Train Security Officers and Auditors
  - Develop consistent reporting procedures
  - Automate reports

Monitor and ROI

- Track helpdesk time before and after deployment
  - Without hard numbers, how do you justify?
- Track audit time before and after deployment
  - Typically a fast return
  - Easy win!
- Integrate into app deployment process
  - They will leave you behind
  - Create a standing meeting every six months or more
- Don’t become a new silo!

Q&A

Puryear IT, LLC
Baton Rouge, LA – 225-706-8414
http://www.puryear-it.com/

Managed Services for Networks, Security, Identity Management

Contact us for a free consultation
contact-us@puryear-it.com