Role Based Access Controls Revisited

- Identity Access Management Challenges
- Moving From Challenged to Valued
  - Defining A New Approach
  - Implementing RBAC with Value
  - Maintaining Your RBAC Catalog
IAM Challenges - What We All Know

Cyber Matters: Skills Shortage Will Force Cybersecurity Rethink
Posted on January 31, 2017

Cybersecurity Professionals Wanted: Study Shows Teams Are Overworked, Undertrained
Posted on January 25, 2017

Pressured App Developers More Likely to Forget Security
Posted on January 12, 2017

SEC Could Take Action Against a Public Company That Fails to Disclose a Major Hacking
Posted on February 9, 2017
There are practical approaches to designing information security programs that align and support an enterprise objectives.

- A good technology architecture requires an ongoing management review process and continuous effort; it is not a blueprint or diagram on a shelf that will enable security programs.

- One size does not fit all when it comes to the real-life operation of an entity’s information security and data protection efforts.

- Skills needed are not just training and certifications but, also real-life experiences along with proven communication and leadership skills.

- Quality Information lies at the heart of the teams’ decision making processes. Decision protocols should also include authority, accountability, and privilege.
Underserved security areas cannot be improved when over-burdened staff are expected to simultaneously develop new skills and processes while maintaining on-going operations.

Specific focus is needed on developing these underserved security pillars and their touch-points within the business:

- Identity
- Compliance
- Operations
- Skills/Structure

The goal is to tie the business drivers to these areas to help prioritize your investment efforts.
By scoping work efforts (project-to-enterprise) to meet prioritized objectives with assessments and iterative methodologies, long drawn-out projects are a thing of the past.

- Use an iterative (Agile) and transferable approach that assesses and builds on the current IT architecture and security management functions

- For your unique environment:
  - Identify capabilities of your people, practices, and technology
  - Classify static and dynamic capabilities
  - Identify and prioritize opportunities for improvement within the context of your current capabilities
  - Build a practical-tailored program that offers the best returns on service for your IT security management and data protection programs
Implementing – An Agile Approach

Agile Sprint Based Role Build

Step 1 - Define Scope
- Prioritize and select Capabilities for Sprint.
- Notify Stakeholders of their role in the Sprint.

Step 2 - Build User Stories
- Define actors, actions, and objectives for User Stories.
- Align services, capabilities, applications, tools, and databases to User Stories.
- Identify technical resources.
- Define preliminary Role Testing Plan.
- Group and distribute User Stories with Stakeholder questionnaires.

Step 3 - Validate User Stories
- Confirm User Stories with Stakeholders.
- Group User Stories into preliminary Roles.
- Finalize Role Testing Plan.
- Confirm technical resources with Application Development team.

Step 4 - Build and Install Role
- Confirm Role design with Stakeholders.
- Enter Role into Registry
- Complete Role testing in the Training environment.
- Coordinate with Security Administrator to upload Roles.
- Publish Role Registry.

Differentiators:
Adaptive, Lean, Responsive & Scalable

- Not dependent on a defined population of Users to model.
- Provides requirements in a common business language that is meaningful to all Stakeholders.
- Limits technical resource discussions outside of the IT area.
- Minimizes slack time in the build.
- Allows for clearly defined Role testing criteria.
- Integrates well with any Identity Lifecycle (IDL) process.
- Versatile enough for handling customization requests, performing role maintenance, new system implementations, and application migrations.
- Preserves a baseline registry that aligns to Business Lines.
Maintaining – Role Management

The reality is multi-directional activities and impacts with significant dependencies.

The goal is harmonious execution.
Implementing – Taking The “Value” Hill

Complexity and communication have been barriers to modeling and executing larger security goals, however, there are effective ways to take valuable ground.

- Identity and Trust Assessment
  - RBAC/ABAC Readiness
  - Network/Architecture Rapid Readout

- Run/Maintain Process & Procedures Enhancements
  - Skills Review
  - Compliance Considerations
  - Responsiveness Readiness

- Management Reporting Requirements
  - Key Monitoring Controls
  - Control Certification (Design & Testing Preparation)

- Execution Capabilities
  - Delivery to the Organization
  - Ability to Adapt to Agile Methodologies
  - Cost to Execute
# New Approaches Yield Real Wins

<table>
<thead>
<tr>
<th>The Hill</th>
<th>The Climb</th>
<th>The Prize Recognizable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forecasting Measurable Security Operations Outcomes</td>
<td>Increasing Operational Visibility</td>
<td>Flexible and Rapid Response to Change</td>
</tr>
<tr>
<td>Detailing Actionable &amp; Affordable Approaches</td>
<td>Reducing Costs to Protect</td>
<td>Better Alignment with Stakeholders</td>
</tr>
<tr>
<td>Developing Execution Strategies that Leverage Cross-functional Skillsets</td>
<td>Communicating Consistently both Vertically and Horizontally</td>
<td>Recognized Business Relevance to Stakeholders</td>
</tr>
<tr>
<td>Gaining/Maintaining Organizational Support</td>
<td>Demonstrating Returns on Service</td>
<td>Increased Organizational Awareness and Confidence</td>
</tr>
</tbody>
</table>
Advances – Transforming Theory Into Reality

Static SOD

Role Hierarchy (RH)

User Assignment (UA)

Permission Assignment (PA)

Users

Roles

Operations

Objects

User

Sessions

Roles

1

2

Dynamic SOD

Permission

Objects
Advances - No Shortage of Solutions
Thank You

April 21, 2017
Who We Are

Who We Are

Chris Bowler
Chris@puzzleboxgroup.com

Dow Smith
Dow.Smith@puzzleboxgroup.com

Formed in 2013, PuzzleBox Group, LLC is focused on helping organizations get the most out of their information technology investments.

We specialize in delivering effective solutions around IT identity, threat, trust, and risk management that are based on Agile methodologies that provide a value-added client experience.

Our team is a group of diverse professionals who have over 100 years of combined experience. This includes senior management positions in Big 4 assurance and advisory firms and industry leading corporate entities.

Our subject matter specialists that focus on IT risk management; IT operations; regulatory compliance, UX design/web development; and process improvement.