Information Security Decisions

TechTarget

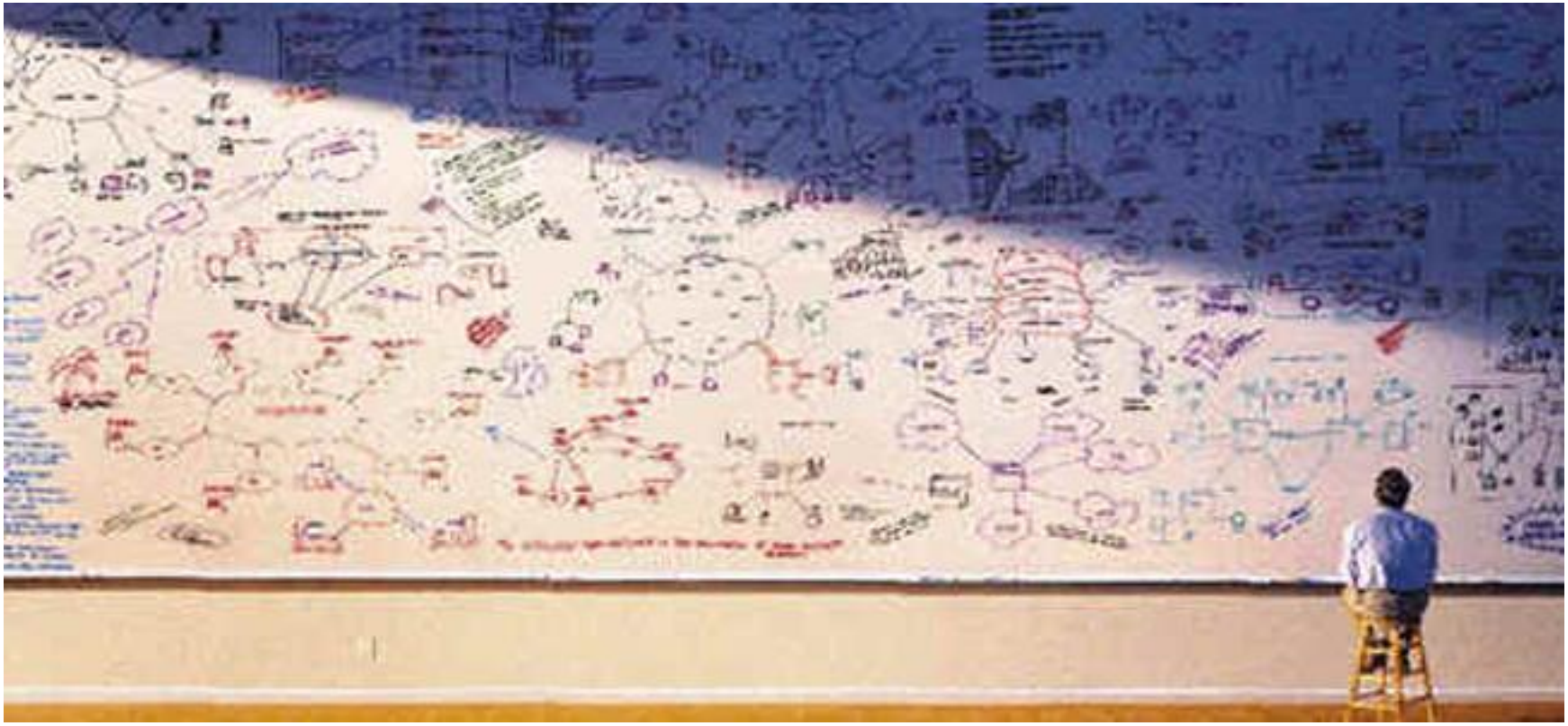
An Identity and Access Management Odyssey:

A step-by-step approach to building a global capability for managing access

John R. Schramm
Chief Information Risk Officer (CIRO)
Manulife Financial

events.techtarget.com

IAM…A Complex Problem

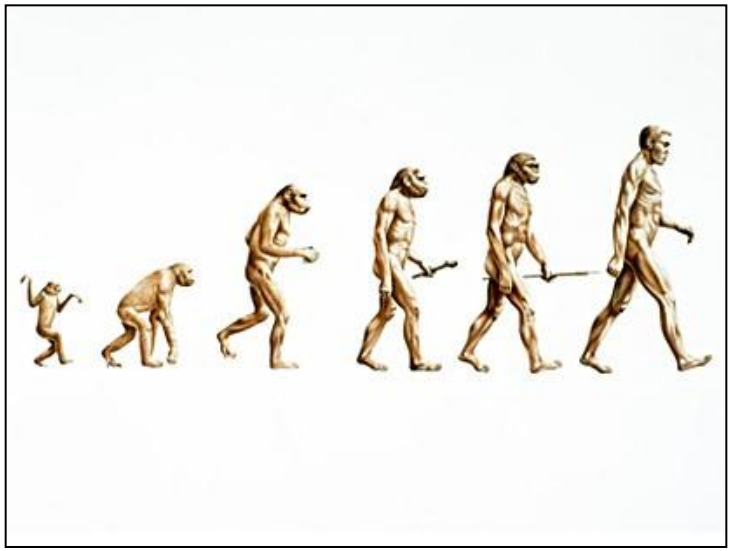


Spectrum of IAM Strategies

"Big Bang"

Big Bang ⟷ **Evolutionary**

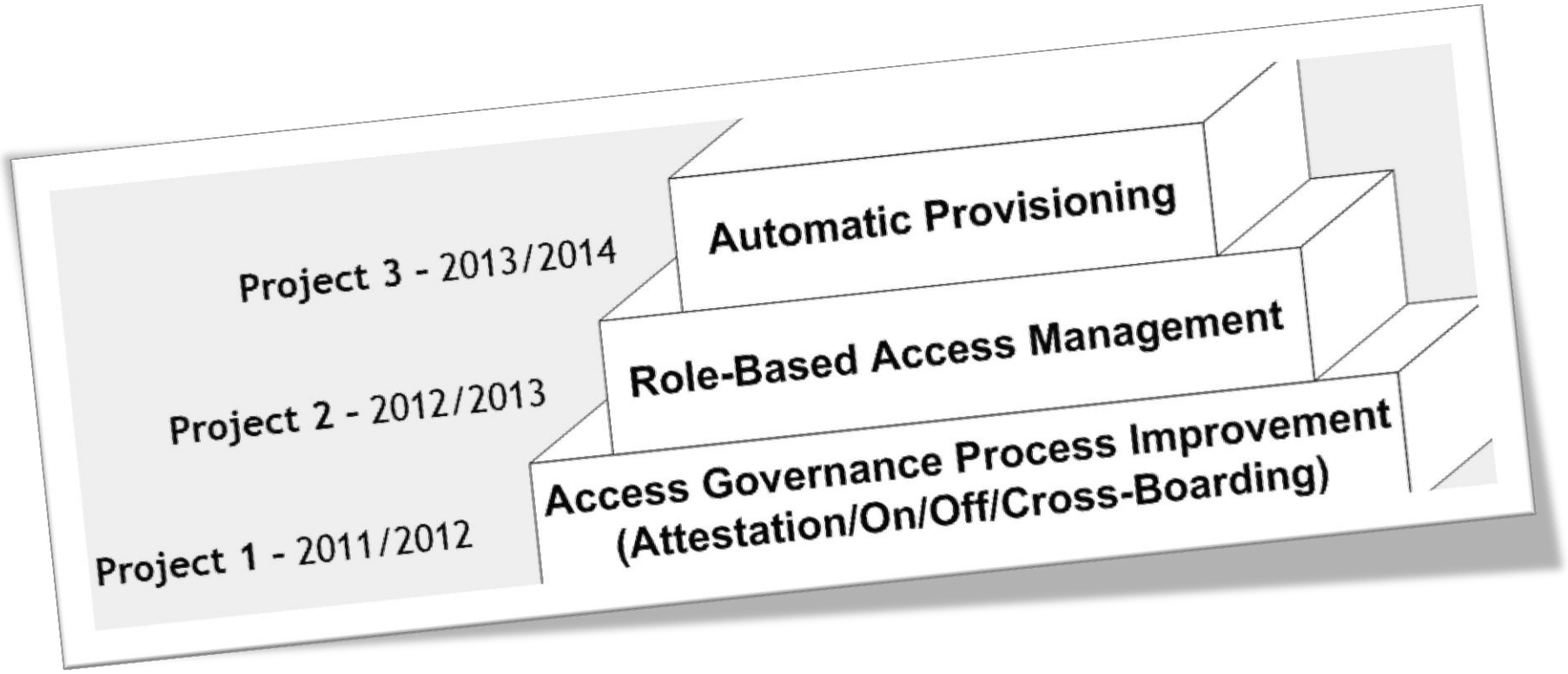
Ginsu Approach



Step-by-Step Approach

A Simple Approach…

Three primary steps with independent business cases…



<u>Required</u>: Strong sponsorship and program leadership

Access Governance: Before

Access Certification

- Manual data aggregation
- Manual (or semi-automated) review workflow
- Manual compilation of results

Termination

- Termination report sent to ID team: Daily term report sent to ID Management team for manual review
- Service management tickets reviewed: Identify all the access privileges held by an out-bound worker, the ID team calls up all tickets ever associated with the individual
- Manual compilation of provisioning requests: Closed tickets related to provisioning requests are cut-and-pasted into a new ticket/email
- De-provisioning: The aggregated access requests are sent to a “term team”; team manually identifies entitlements in target systems and de-provisions the entitlements
- Ticket closed: closure of the de-provisioning ticket indicates that terminated worker’s access privileges have been removed

Access Governance: After

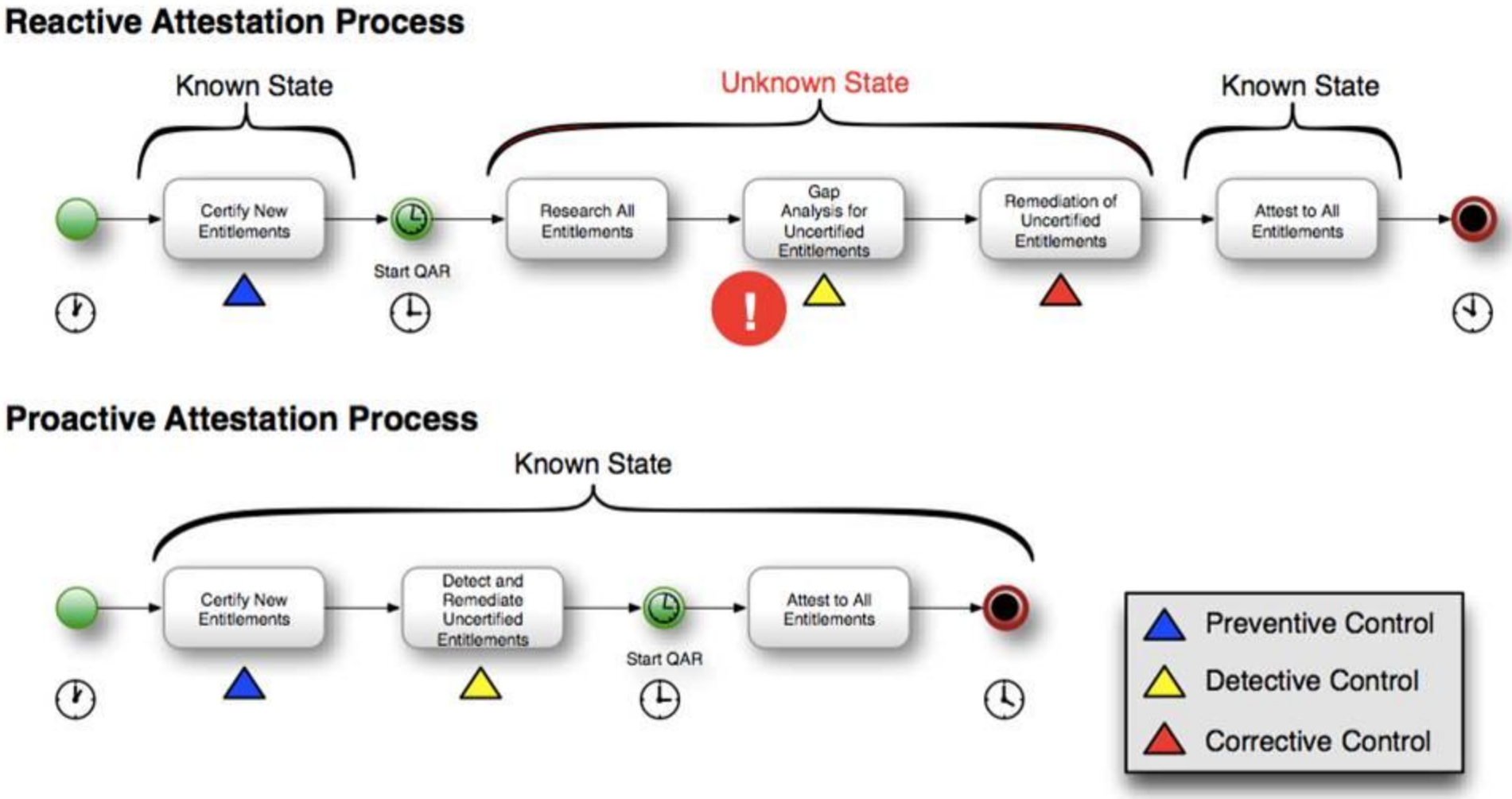
Access Certification

- Person and account data aggregated daily: IAM tool keeps track of identity data and access entitlements for integrated applications
- Certification initiation: Certification launched directly from the IAM tool; automated workflows notify reviewers by email of certification requirement
- Review process: Certifiers are presented with “business-friendly” display of entitlements for their direct reports, with simple point-and-click interface
- Certification results: IAM tool records reviewer decisions and logs certification results for audit evidence

Terminations

- Termination identified in change feed: IAM tool identifies impending worker termination from automatic daily feed of HR systems of record data
- “Off-boarding” workflow automatically initiated: The identified termination sets off workflow to person’s manager or security team, to initiate removal of associated access entitlements
- All relavant access privileges are identified: The de-provisioning process captures all necessary revocations
- Closed-loop process: If manual de-provisioning not completed the IAM tool monitors daily access feeds and notifies if de-provisioning is not completed

Process Innovation…



Challenges

- Different maturity levels within organization
- Resistance to change
- Identity correlation
- Data “cleanliness”
- Resource constraints

Lessons Learned

- Incorporate data clean-up/validation in plan
- Drive for enterprise-wide processes and single roll-out methodology
- Engage Human Resources Business Process and Data personnel as project team members, early in the process
- Engage business executives and gain their support
- Hire a strong Program Manager

Thank You!