Achieving GRC Maturity with LogicGate Solution Success Kits

In this informative session, Sarah and Jerry introduced LogicGate's Solution Success Kits and walked attendees through how to leverage them alongside enhanced Access Management capabilities to advance GRC program maturity. The session provided practical insights for maximizing the value of LogicGate's Risk Cloud platform—whether you're just getting started or aiming for enterprise-level integration.

Sarah Nuttall
Manager,
Customer Success
LogicGate

Jerry McElyea
Senior Technical
Account Manager
LogicGate

Key Takeaways

1 Solution Success Kits provide structured templates and resources at three levels of program maturity, including: developing, established, and integrated; empowering teams to scale GRC use cases faster and more effectively.

3 A defined maturity path for access management, from SSO implementation to audit-ready reporting, give organizations a clear blueprint to strengthen user control and compliance over time.

2 New capabilities like role-group relationships and automated user group assignments streamline record-level access control, reduce manual effort, and improve security governance across the platform.

4 With kits tailored to six major GRC areas (listed below) customers can quickly deploy best-practice workflows aligned to their most critical risk priorities.

Available Solution Success Kits

Policy and Procedure	Cyber Risk	Enterprise Risk
Regulatory Compliance	Controls Compliance	Operational Resilience

Achieving GRC Maturity with LogicGate Solution Success Kits

Access Management Architecture & Enhancements

The presenters also shared updates to Access Management, which are critical for scaling and securing enterprise-wide usage.

Four Pillars of Access Management:
- Roles: Define entitlements and control what users can do
- Permission Sets: Regulate visibility of records at each workflow step
- User Groups: Manage who sees what within individual records
- SCIM Integration: Seamlessly sync users and roles from identity providers

Current Adoption Stats:
- 75% of customers use Single Sign-On (SSO)
- ~50% use SCIM provisioning
- Far fewer utilize SCIM group sync, indicating room for optimization

New Features Introduced:
- Role-Group Relationships: Groups can now be directly tied to roles, enabling IDP-managed access at the record level and reducing manual user assignments.
- Automated Group Assignment: Users can now be automatically assigned to user groups based on field values —ensuring consistent, pre-configured access controls with no manual input.

Access Management Maturity Path

To evolve access controls alongside your GRC program, LogicGate recommends the following maturity journey:

1. Implement Single Sign-On
2. Enable SCIM provisioning
3. Consolidate roles and permission sets
4. Activate SCIM group sync
5. Configure automated user group assignments
6. Set up record-level access controls
7. Leverage audit reporting features for transparency and assurance

Your guide to configuring role-based access control in Risk Cloud from user provisioning to individual record access.