THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Defending the Fortress:
New Threats Meet New Defenses

Increasing Operational Efficiency with a Governance Risk and Compliance (GRC) Framework

Sam Curry

Vice President, Product Management and Strategy,

RSA, The Security Division of EMC

Jerry Archer, CISSP

Senior Vice President and Chief Security Officer, Sallie Mae

Deloitte.

RSA
The Security Division of EMC

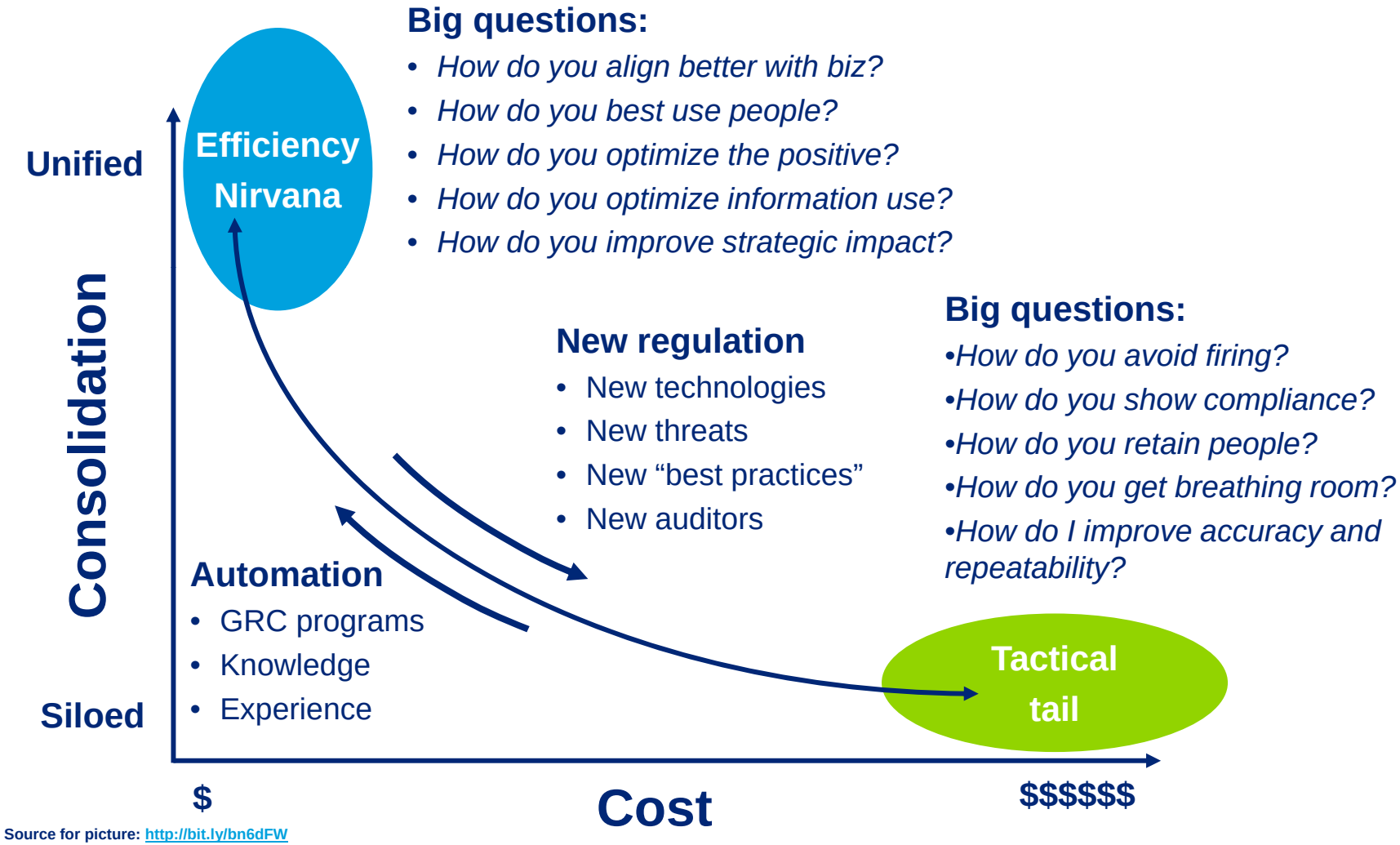
Increasing Operational Efficiency with a Governance, Risk, and Compliance (GRC) Framework.

September 13, 2010

Business first principles

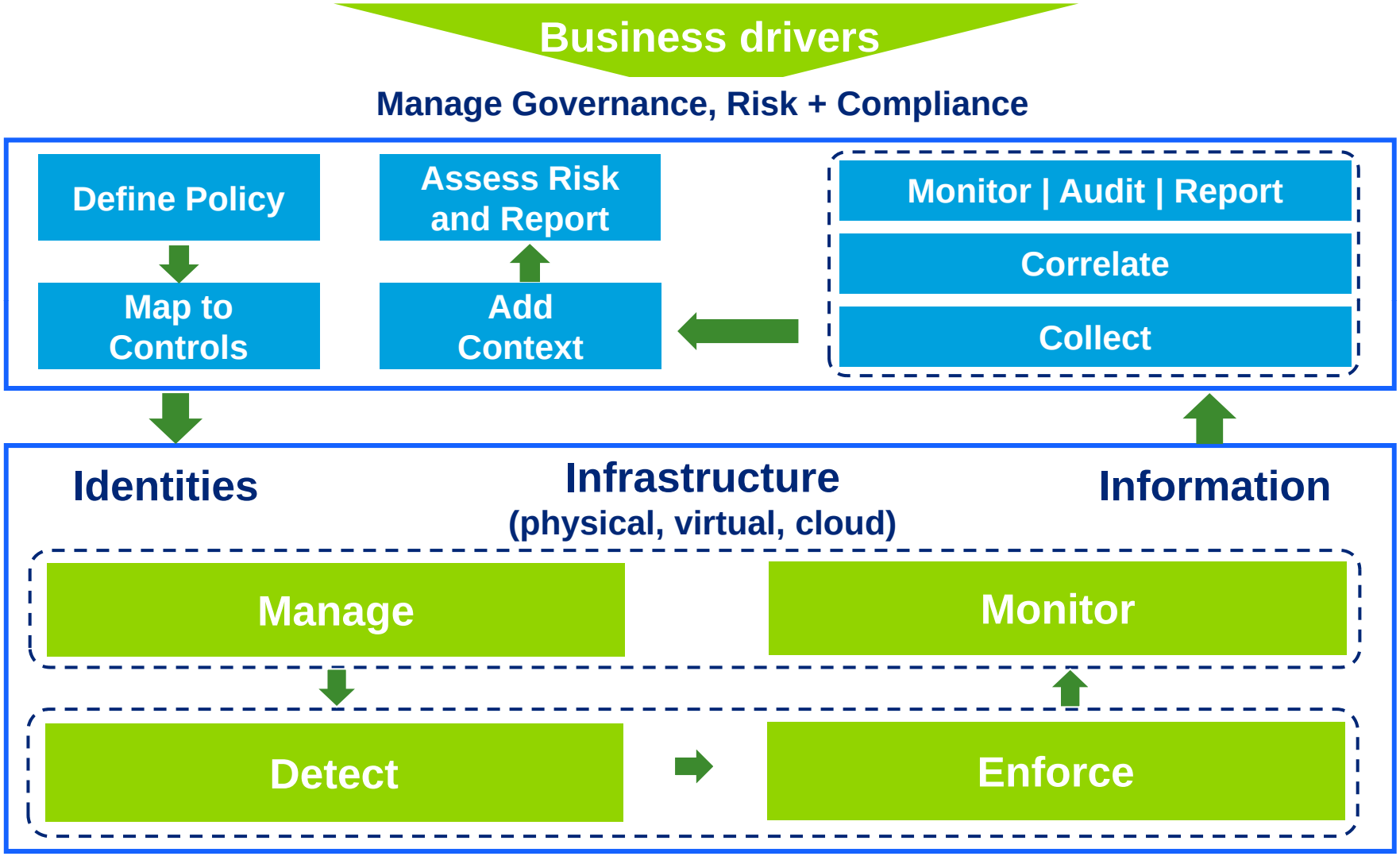
1. Business is ultimately about
   - Risk versus Reward
2. IT should be a *service* to the business
   - Transparent and easy to use
   - Flexible
   - Ubiquitous
3. It's about Confidentiality, Integrity, Availability (CIA)
4. Manage it! It's about the management (predictable, repeatable, improving) discipline…let's look at *"GRC"…*a little out of order
   - G: tell the IT infrastructure what to do and be sure it can do it
   - C: have the IT infrastructure tell you what is happening
   - R: manage the business priority and reduce risk

Moving away from the tactical

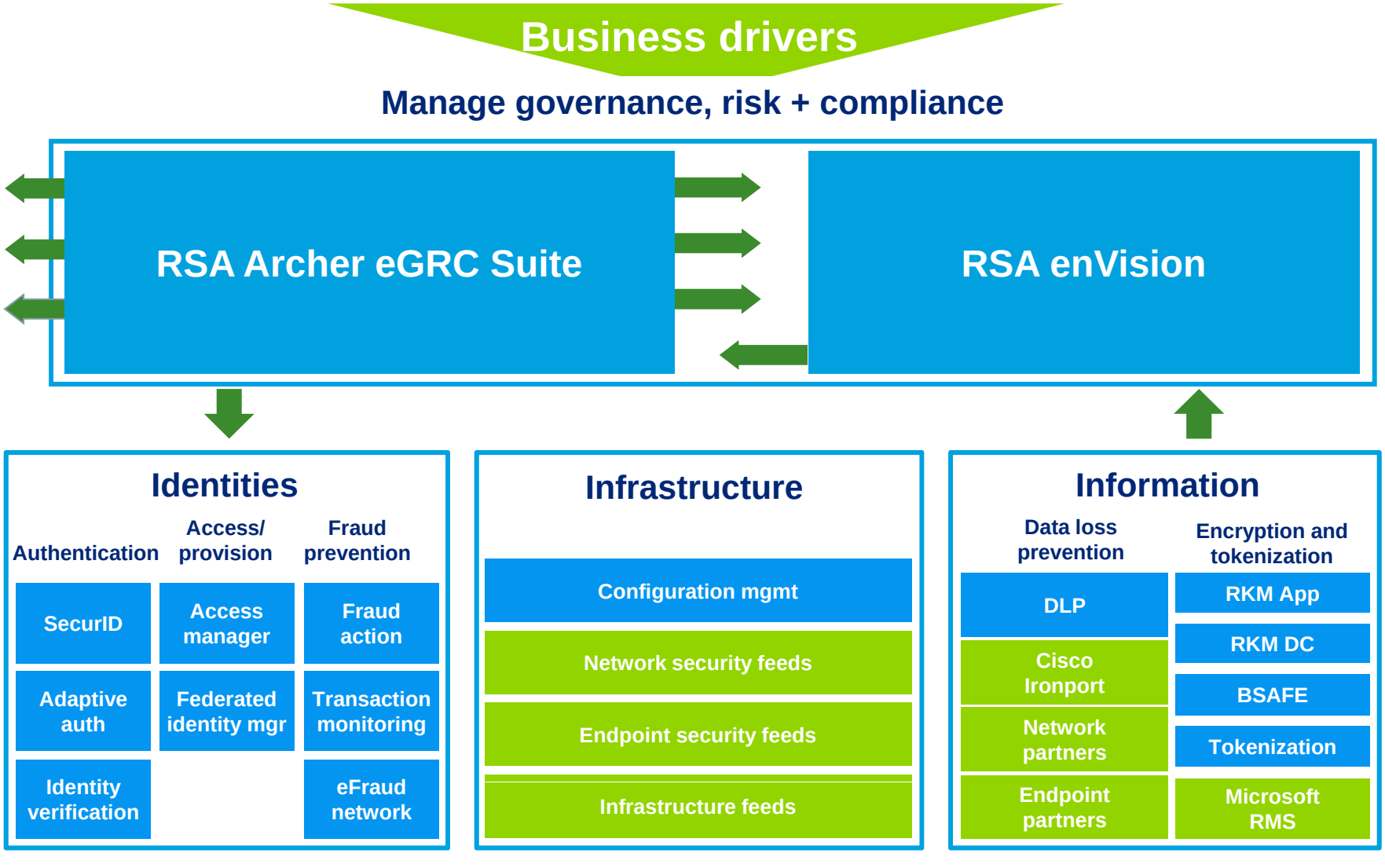


Source for picture: http://bit.ly/bn6dFW

Managing security, risk, and compliance

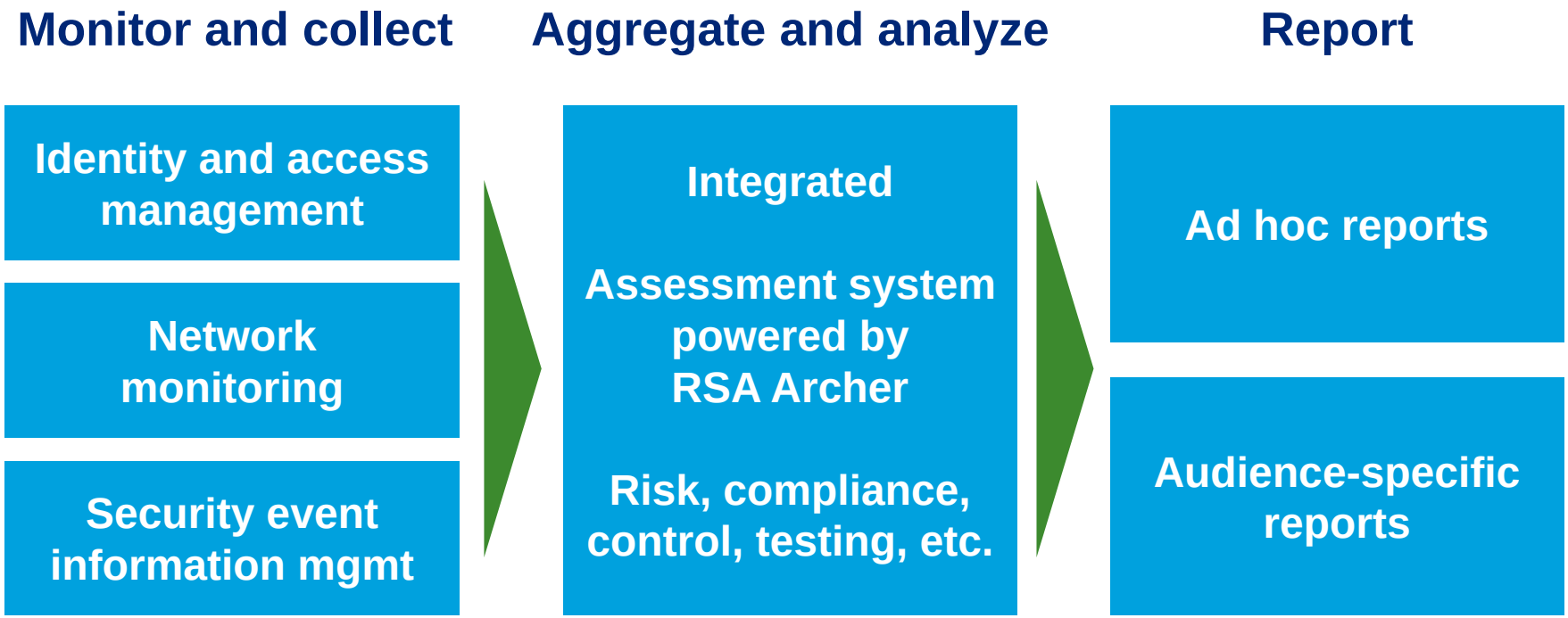


The RSA ecosystem

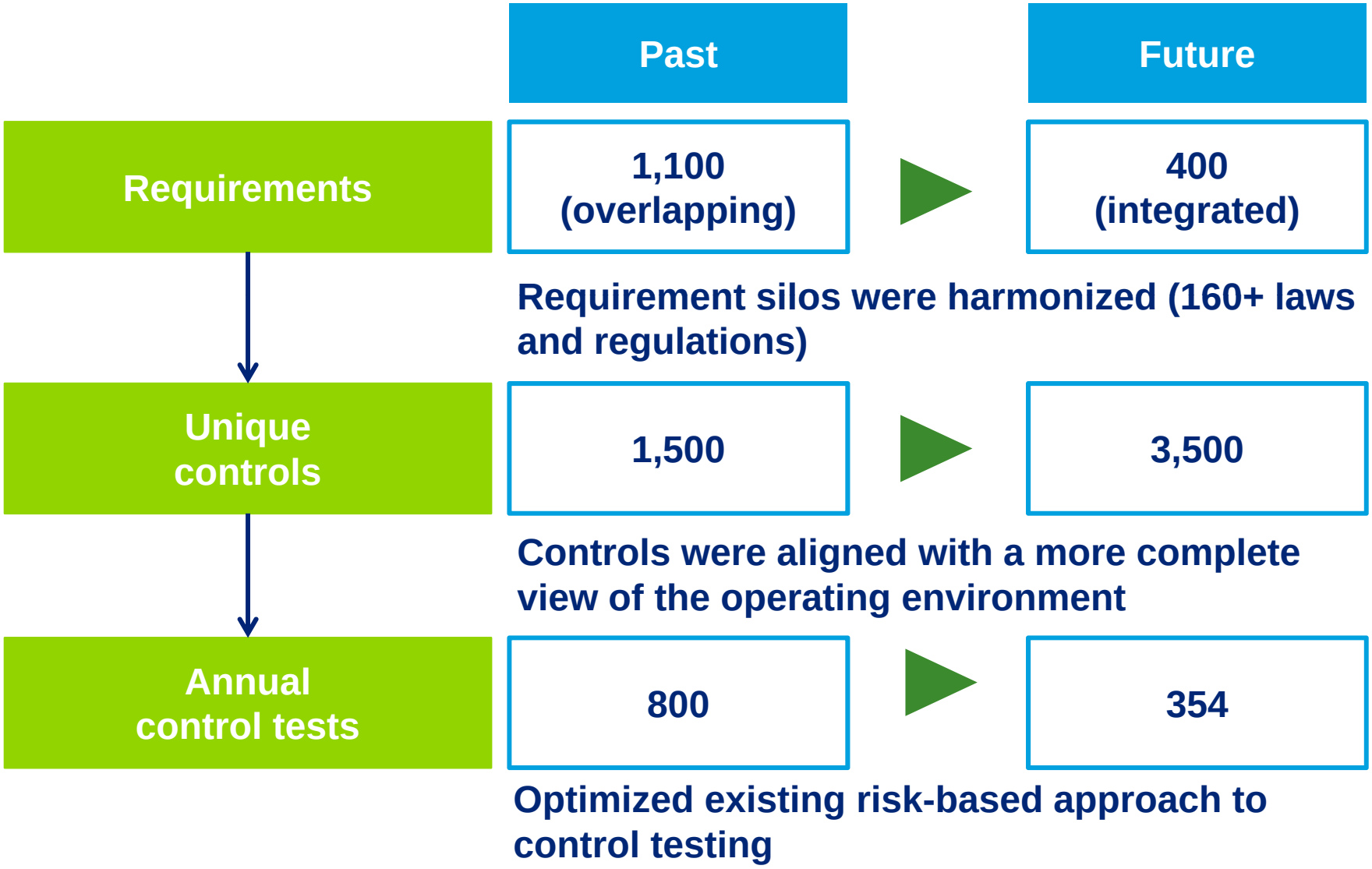


Consistent aggregation and reporting

We are using RSA Archer eGRC Platform as the common aggregation engine to accelerate risk and compliance reporting for security and information technology



Three-step approach to control testing efficiency



Operational sustainment through automation

Our approach accommodates flexibility and sustainment considerations

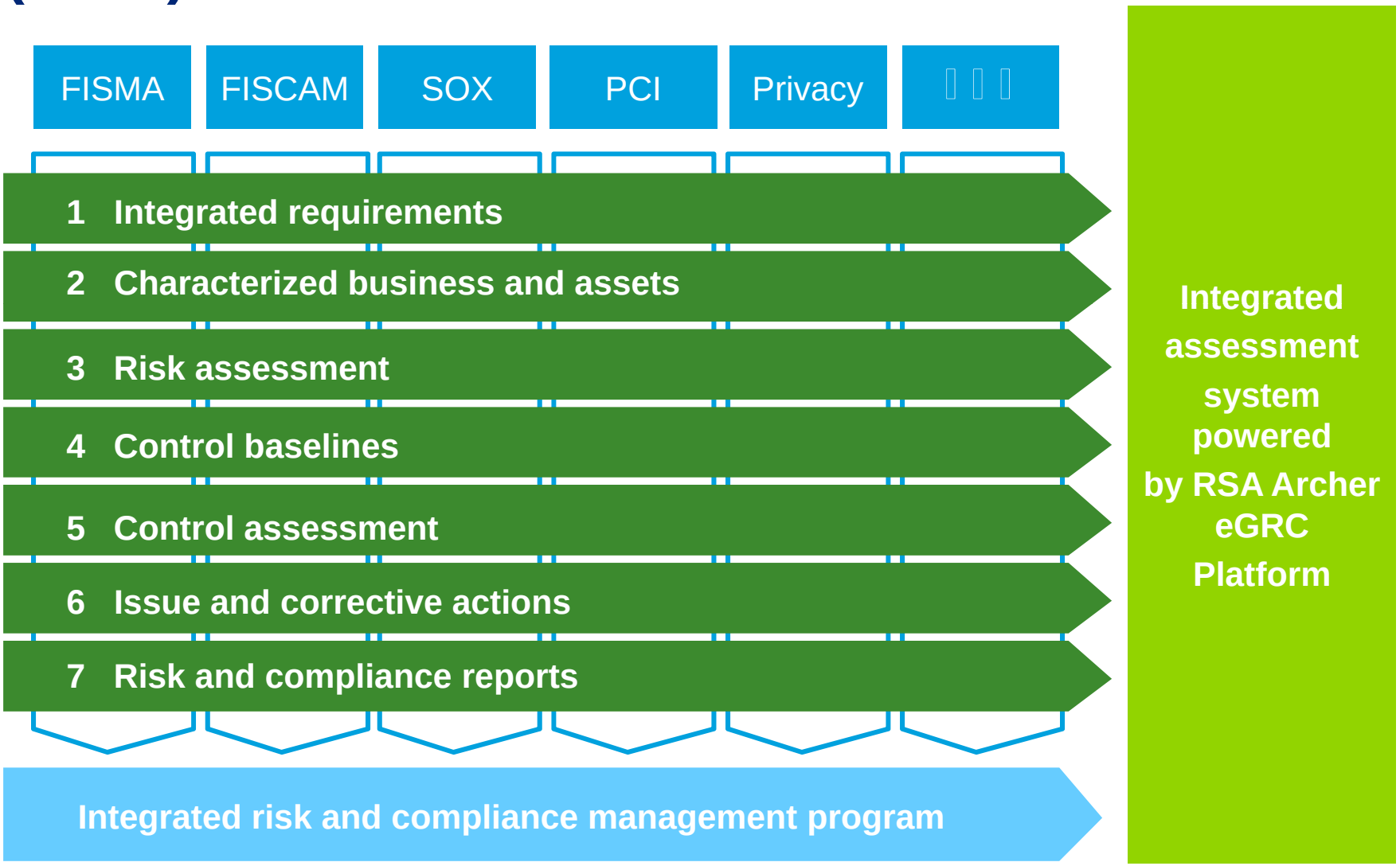
Flexibility and scalability

- Common processes and definitions for better alignment
- Integrated requirements linked to operating environment
- Defined risk and compliance monitoring criteria
- Federated operating model for business unit flexibility
- Reporting traceability for each risk/compliance area

Sustainment considerations

- Roles and responsibilities support multi-stakeholder views
- Workflow-enabled process supports issue management
- Enterprise governance model for process reliability
- Traceable QA and sign-off for assessment results
- Evidence collection, data archiving, and trending

Operational sustainment through automation (cont.)



Benefits

Incremental benefits are being achieved beginning with immediate improvements from the integrated requirements

Quality

- Full traceability between the mandate, the control, and Sallie Mae policies and standards
- Improved coverage for new mandates
- Standardization through control baselines
- Repeatable process
- Mandatory fields with drop-down options

Optimization

- One control satisfies many requirements
- Risk-based approach
- Avoid redundant testing
- Right-size controls
- Automated workflow
- Automated reporting and dashboards

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Thank You

Questions?