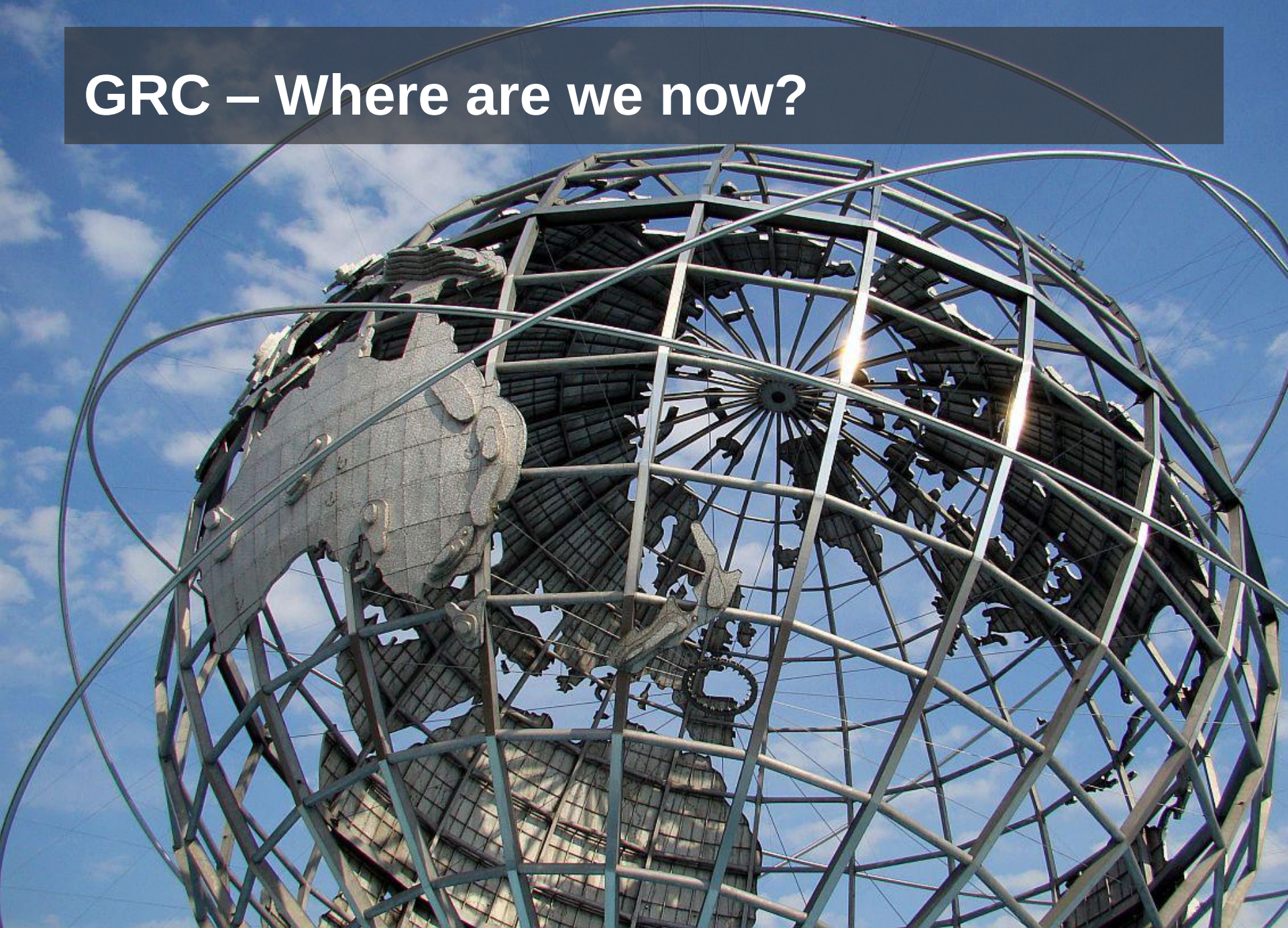
Assessing the Maturity of your Risk and Compliance Program

Chris McClean, Principal Analyst, Research Director

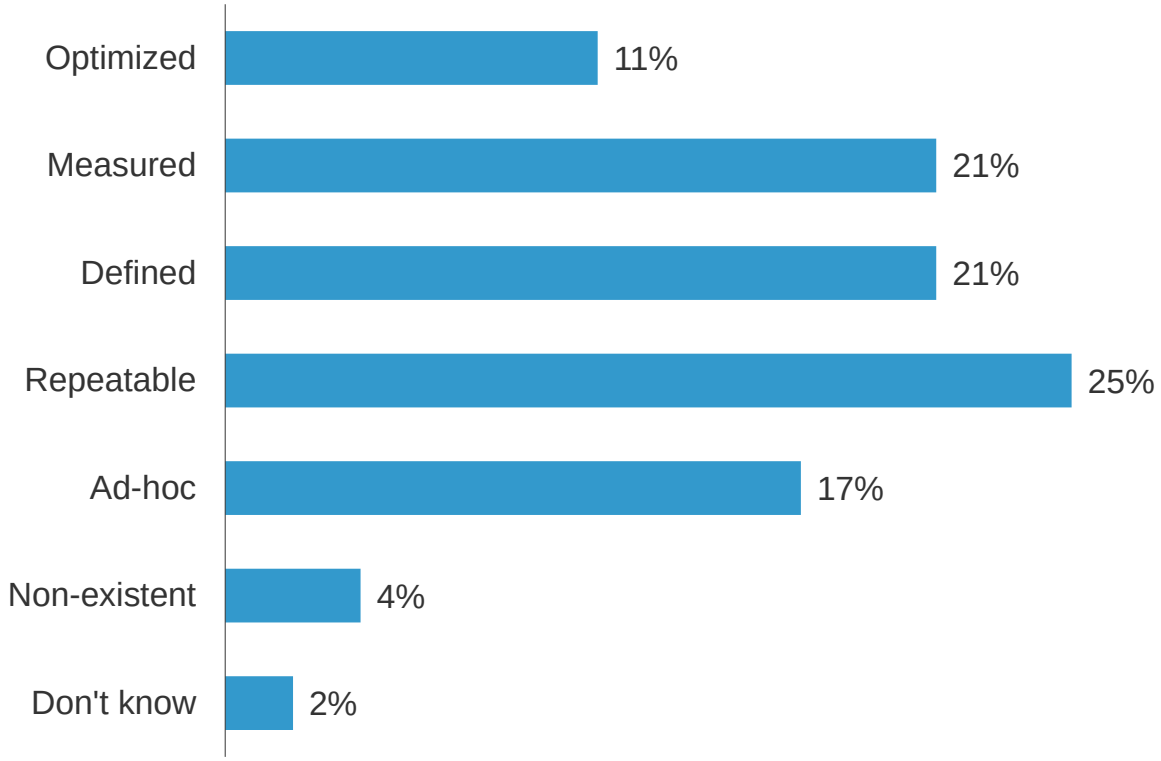
April 30, 2013

GRC – Where are we now?



Are We Fooling Ourselves?

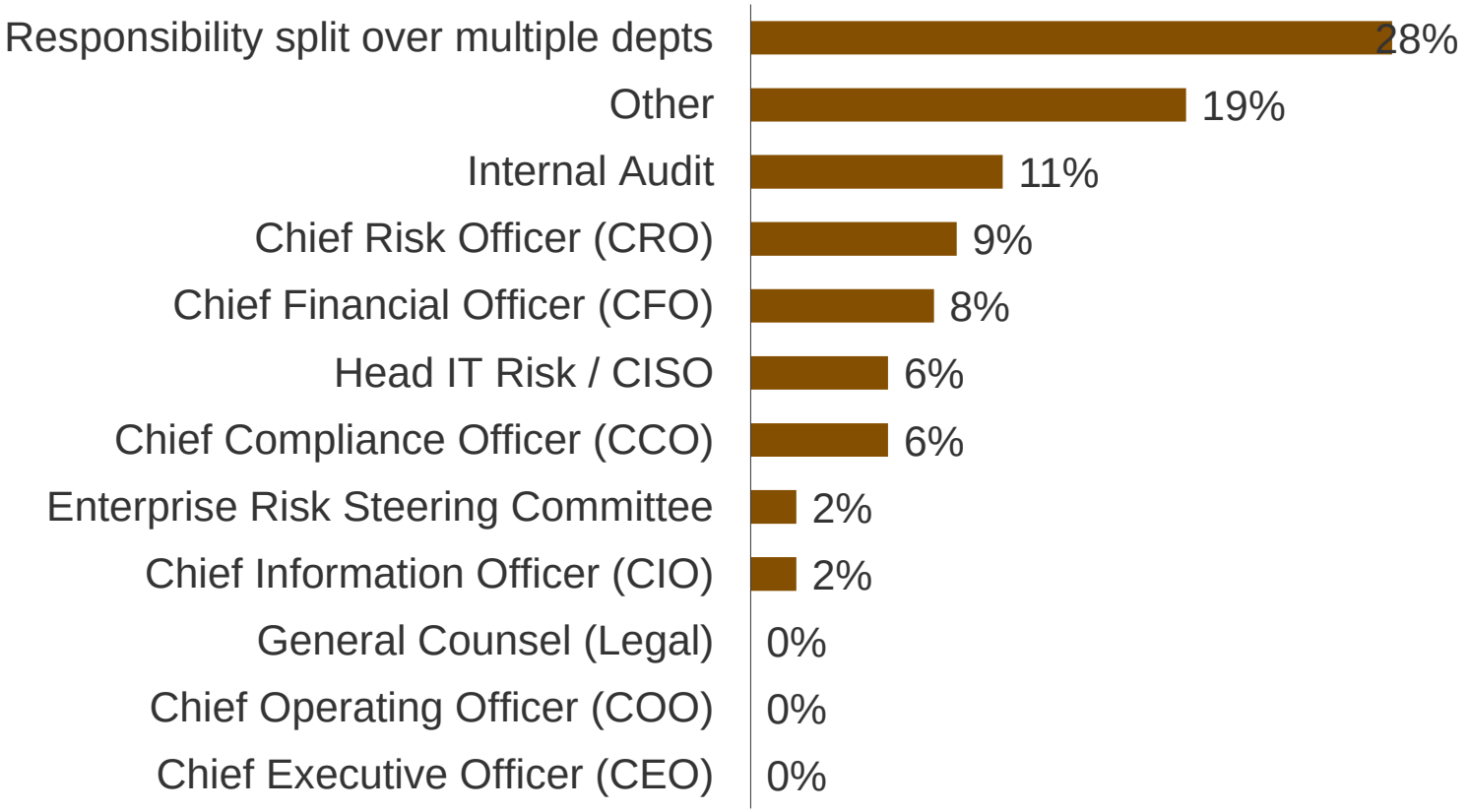
How would you characterize the maturity of your overall GRC program and processes?



Base: 53 global GRC decision-makers

GRC spans across many teams

Who is responsible for the day-to-day coordination of your GRC program?

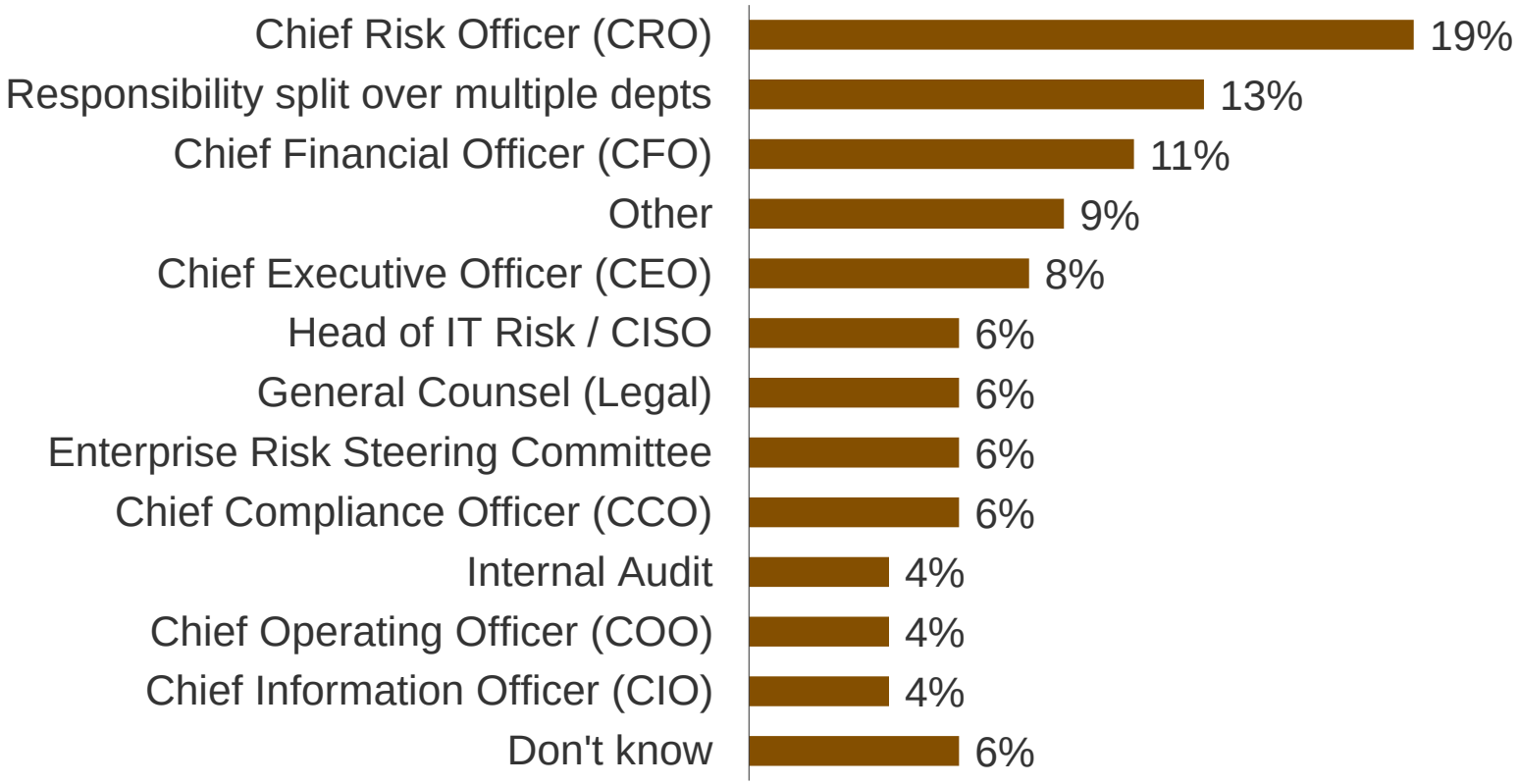


Base: 53 global GRC decision-makers

Source: Forrester's Online GRC TechRadar Customer Reference Survey, Q3 2012

GRC involves many stakeholders

Who is responsible for the overall success of your GRC program?



Base: 53 global GRC decision-makers

Source: Forrester's Online GRC TechRadar Customer Reference Survey, Q3 2012

Customer use cases are diverse…

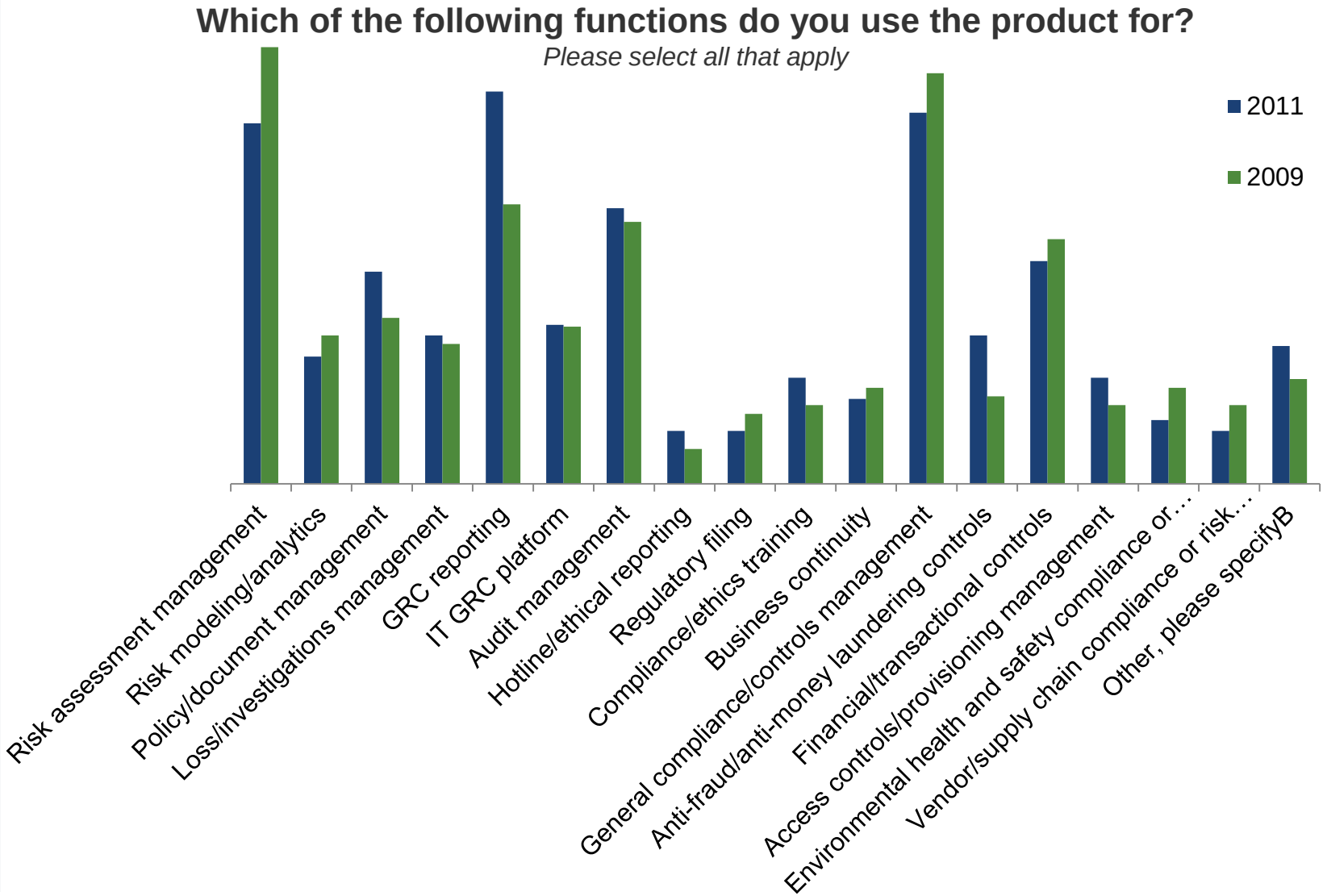
Which of the following functions do you use the product for?

Please select all that apply

Base: 121 Customer references for the Enterprise and IT GRC Platforms Waves, Q4 2011

Source: Forrester's Q2 2011 Global Governance, Risk, And Compliance Platforms Wave Customer Reference Online Survey

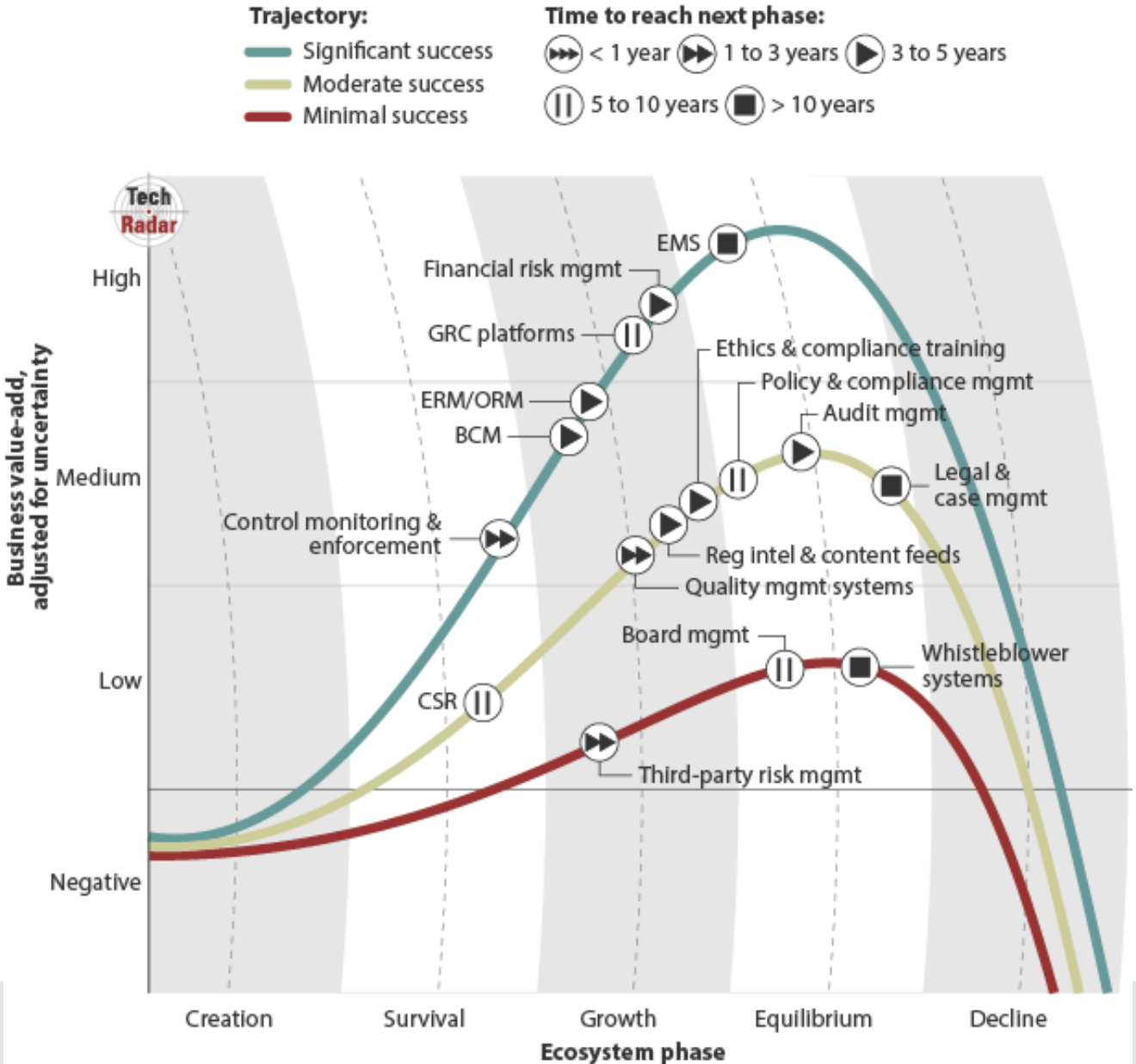
…but they haven't changed much.



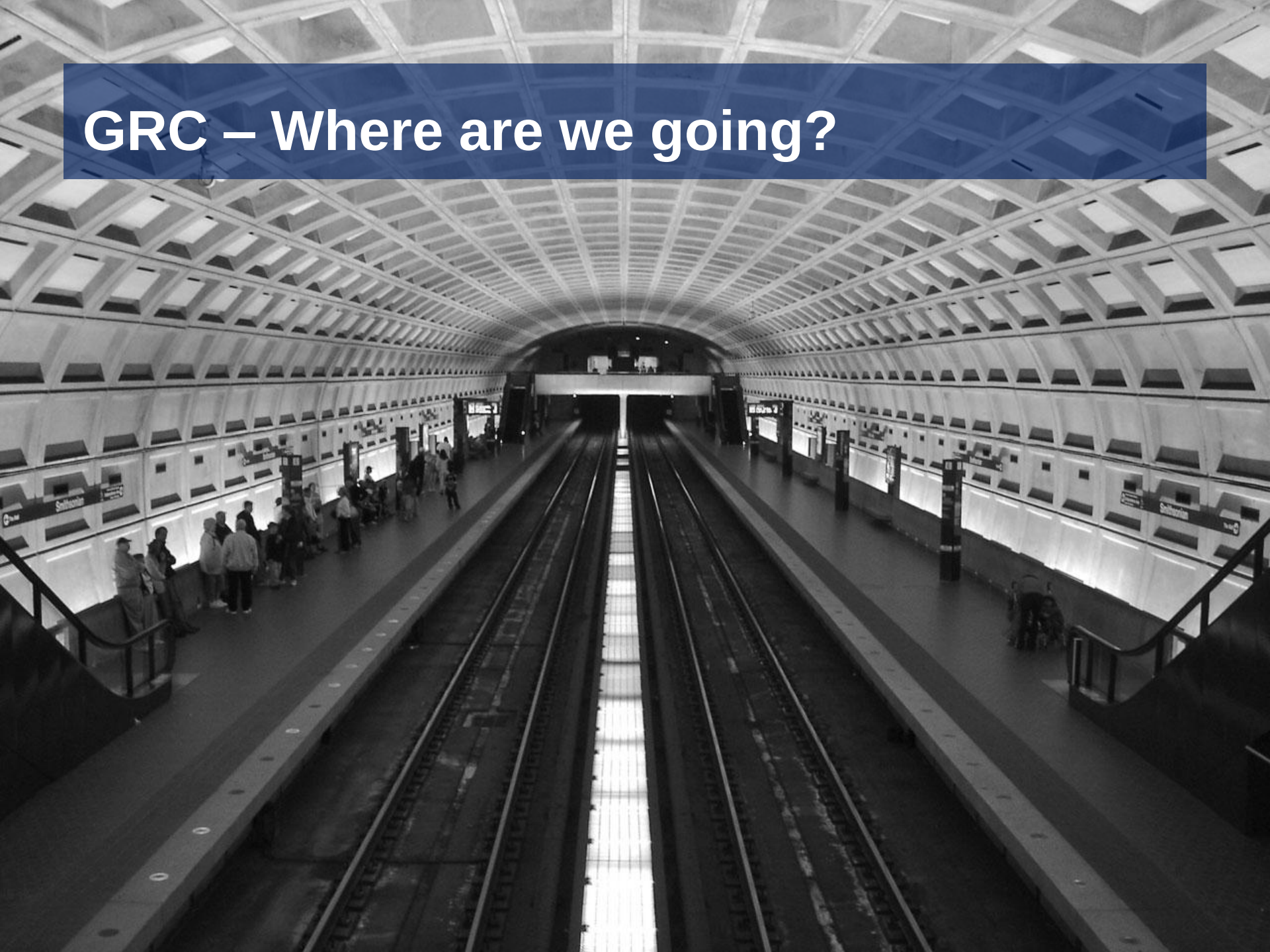
Base: 69 Customer references for the Enterprise GRC Platforms Wave, Q3 2009

Base: 121 Customer references for the Enterprise and IT GRC Platforms Waves, Q4 2011

The GRC TechRadar

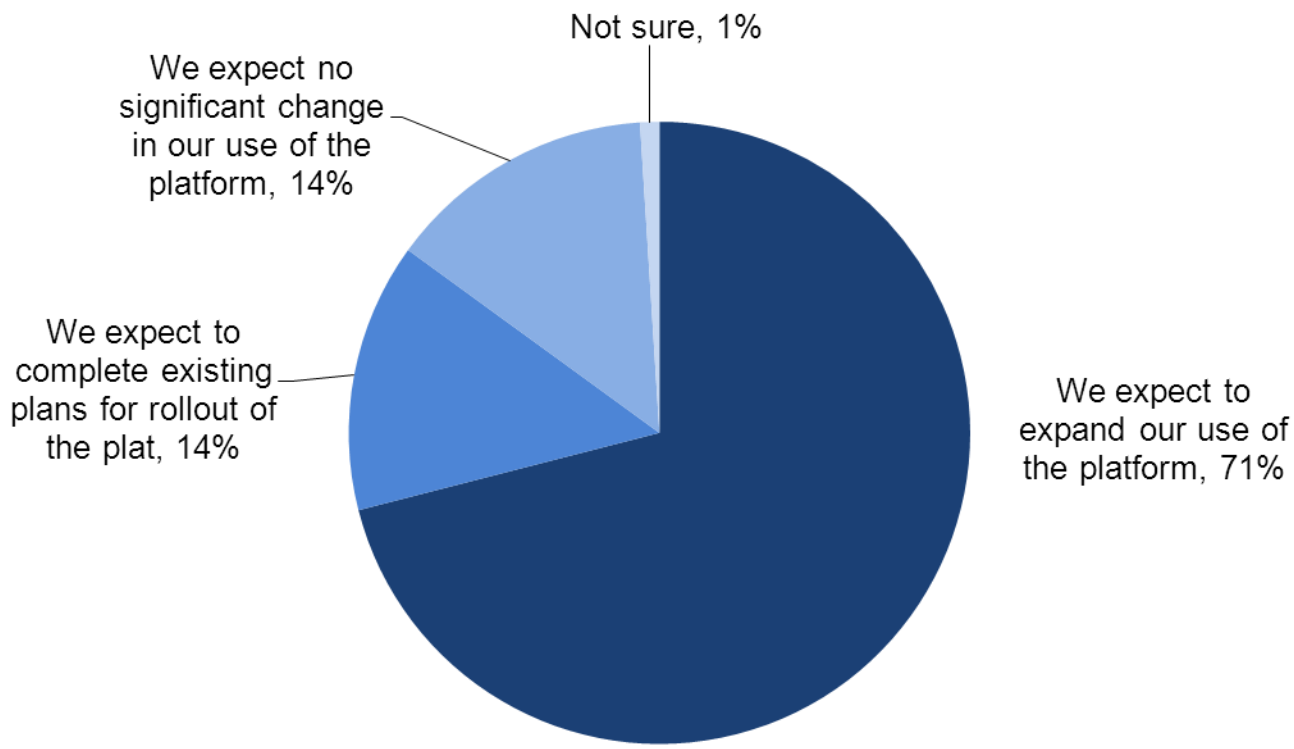


GRC – Where are we going?



Future Plans for GRC Platforms (2009)

How do you expect your work with this product and vendor to change over the next year?

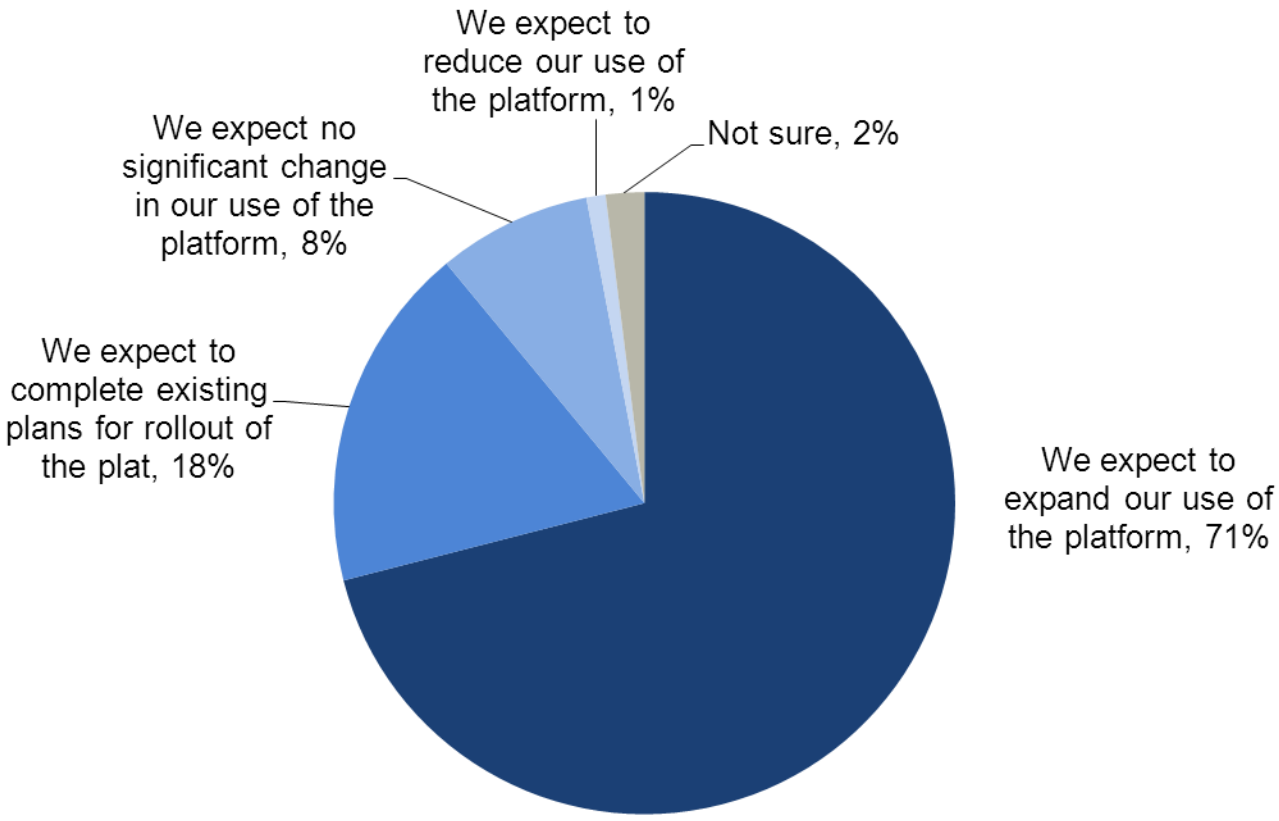


Base: 69 Customer references for the Enterprise GRC Platforms Wave, Q3 2009

Source: Forrester's Q3 2009 Governance, Risk, And Compliance Platforms Wave Customer Reference Online Survey

Future Plans for GRC Platforms (2011)

How do you expect your work with this product and vendor to change over the next year?



Base: 120 Customer references for the Enterprise and IT GRC Platforms Waves, Q4 2011

Source: Forrester's Q2 2011 Global Governance, Risk, And Compliance Platforms Wave Customer Reference Online Survey

Drivers to expand are plentiful

*“More compliance and risk programs and processes will be incorporated into the tool; **other department have seen the benefits** of using this tool.”*

*“Since **all the assets are mapped and the policy is structured**, we will add more modules to support our operational risk management and our business continuity management. Internal audit department is interested in the system as well.”*

*“**Users are very satisfied**. More and more subsidiaries ask for this product, module by module (internal control, internal audit, etc...).”*

*“We plan to expand the use of the platform to **further automate our audit management capabilities**, roll out the control self assessment process to additional functions and for formalizing our ERM program.”*

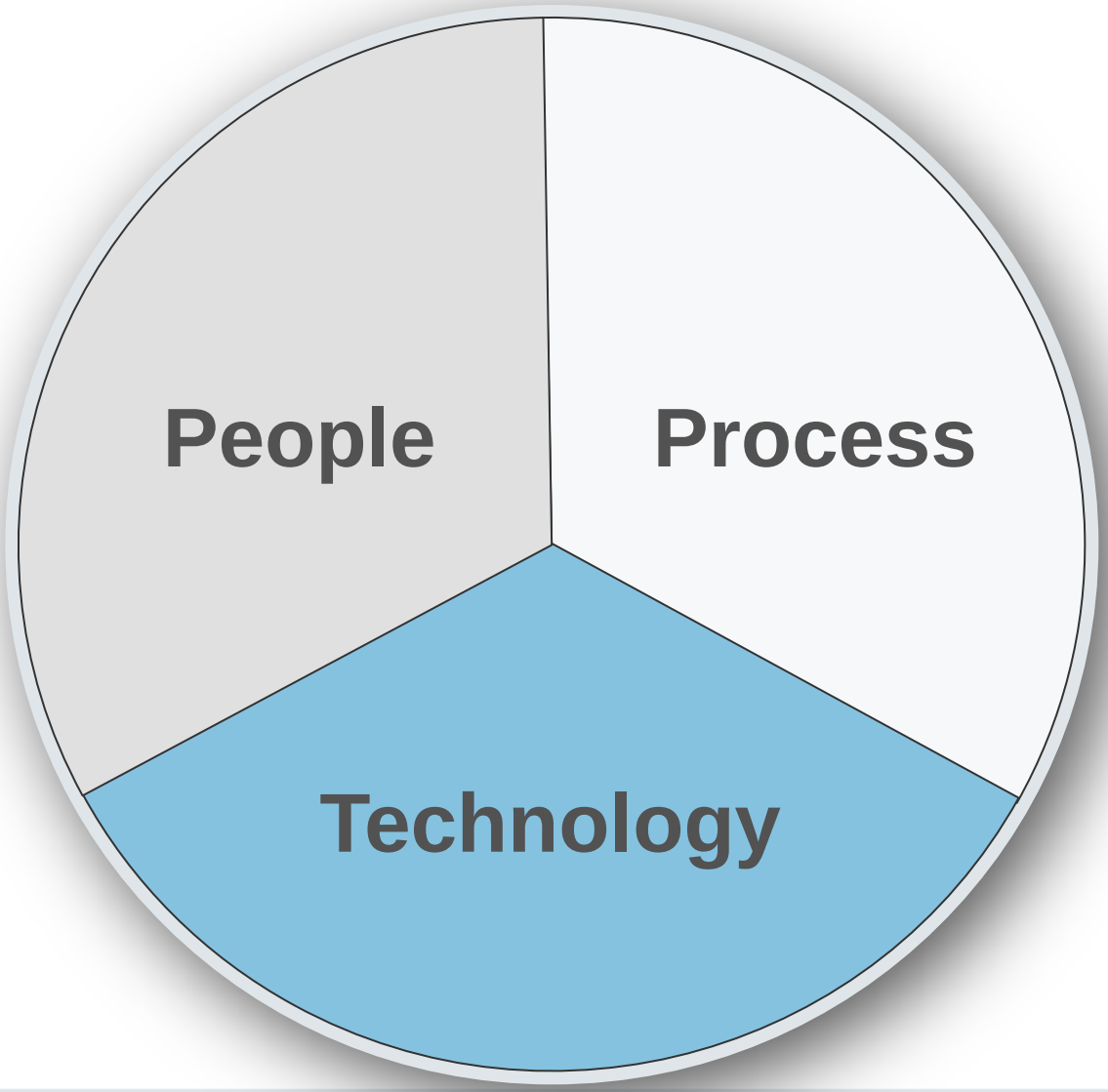
*“A **large merger underway** meaning numerous more requirements to monitor.”*

Roadmap questions

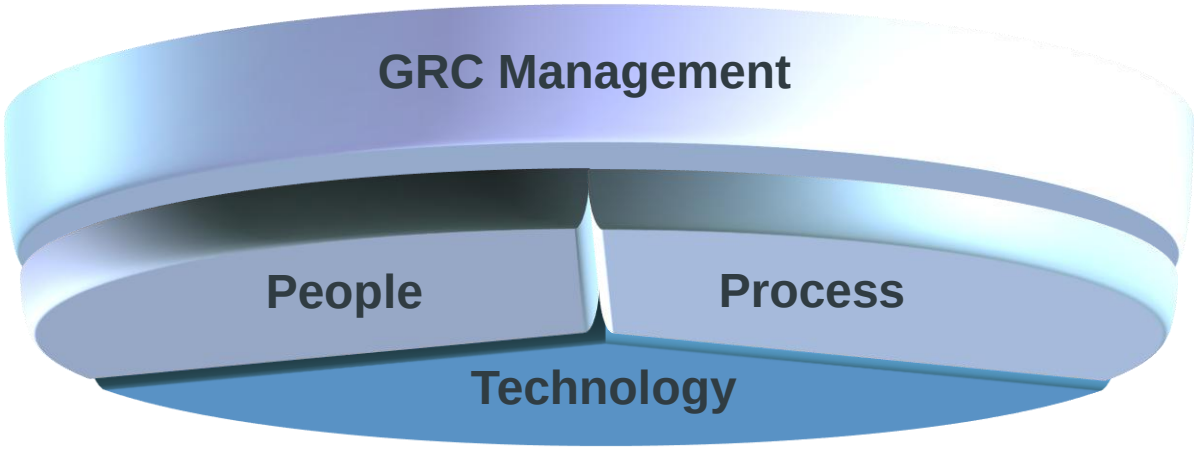
- *Is GRC consolidation worth the trade-offs?*
- *What do we expect will be the organizational challenges over the next 3-5 years?*
- *Who are the primary users, occasional users, and audience/stakeholders?*
- *What functions could/should be automated, facilitated, or left manual?*
- *What are the expected outcomes in 6 months, 1 year, 3 years?*

Are We Mature Yet?

GRC Framework



GRC Framework



GRC Framework

GRC MANAGEMENT
Strategy
Governance
Coordination

GRC Framework

GRC MANAGEMENT
Strategy
Governance
Coordination

PEOPLE
Culture
Organization
Relationships

GRC Framework

GRC MANAGEMENT
Strategy
Governance
Coordination

PEOPLE
Culture
Organization
Relationships

PROCESS
Risk
Compliance
Audit

GRC Framework

GRC MANAGEMENT
Strategy
Governance
Coordination

PEOPLE
Culture
Organization
Relationships

PROCESS
Risk
Compliance
Audit

TECHNOLOGY
Technology/data integration
Content/data management
Facilitated workflow
Analytics and reporting

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	
1 – Ad hoc	
2 – Repeatable	
3 – Defined	
4 – Measured	
5 – Optimized	

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	
2 – Repeatable	
3 – Defined	
4 – Measured	
5 – Optimized	

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	Occasional, not consistent, not planned, disorganized, reactionary.
2 – Repeatable	
3 – Defined	
4 – Measured	
5 – Optimized	

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	Occasional, not consistent, not planned, disorganized, reactionary.
2 – Repeatable	Intuitive, relatively consistent, not documented, occurs only when necessary
3 – Defined	
4 – Measured	
5 – Optimized	

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	Occasional, not consistent, not planned, disorganized, reactionary.
2 – Repeatable	Intuitive, relatively consistent, not documented, occurs only when necessary
3 – Defined	Documented, predictable, evaluated occasionally, understood
4 – Measured	
5 – Optimized	

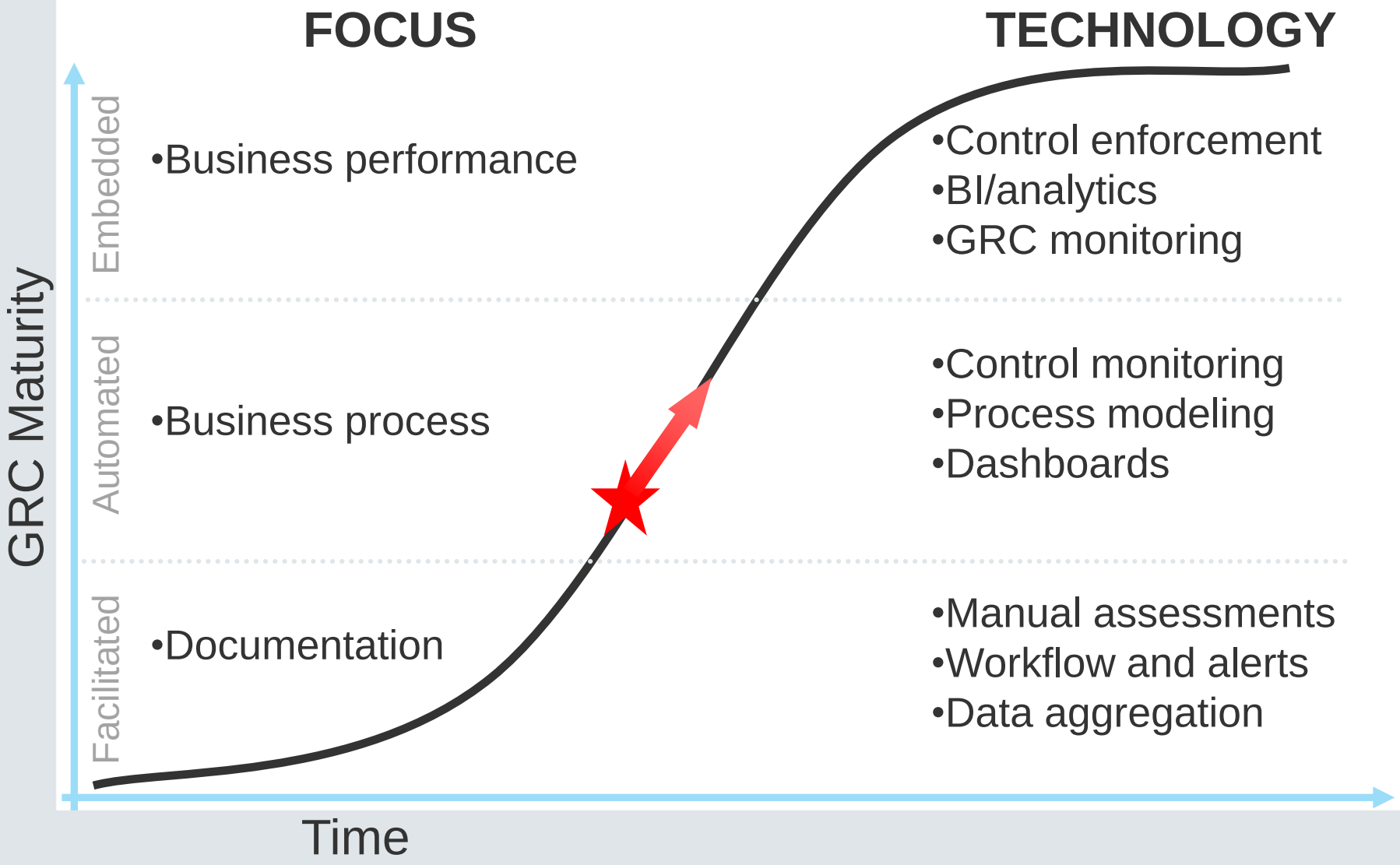
Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	Occasional, not consistent, not planned, disorganized, reactionary.
2 – Repeatable	Intuitive, relatively consistent, not documented, occurs only when necessary
3 – Defined	Documented, predictable, evaluated occasionally, understood
4 – Measured	Well managed, formal, evaluated frequently, elements are often automated
5 – Optimized	

Measuring maturity

LEVEL	CHARACTERISTICS
0 – Nonexistent	Not understood, not formalized. Need is not recognized
1 – Ad hoc	Occasional, not consistent, not planned, disorganized, reactionary.
2 – Repeatable	Intuitive, relatively consistent, not documented, occurs only when necessary
3 – Defined	Documented, predictable, evaluated occasionally, understood
4 – Measured	Well managed, formal, evaluated frequently, elements are often automated
5 – Optimized	Effective, integrated, proactive, continually evaluated and improved, elements are usually automated

The momentum of GRC programs



GRC benefits

CATEGORY	BENEFITS	METRICS
Efficiency	• Reduced costs of risk assessments and aggregation • Speed of policy development, approval, distribution • Improved speed/cost of risk reporting • Improved speed/cost/coverage of audits	• Staff-hours saved per process • Payroll savings from delay or avoidance of staff increase • Reduction in costs for internal and external audits

GRC benefits

CATEGORY	BENEFITS	METRICS
Efficiency	• Reduced costs of risk assessments and aggregation • Speed of policy development, approval, distribution • Improved speed/cost of risk reporting • Improved speed/cost/coverage of audits	• Staff-hours saved per process • Payroll savings from delay or avoidance of staff increase • Reduction in costs for internal and external audits
Risk reduction	• Reduction in incidents, near misses, loss events • Reduction in regulatory fines, actions, law suits, etc. • Reduction in time to discover control gaps, violations • Reduction in audit/assessment findings	• Reduced number and cost of incidents • Reduced number/size of fines • Reduced cost of capital • Reduced insurance premiums

GRC benefits

CATEGORY	BENEFITS	METRICS
Efficiency	• Reduced costs of risk assessments and aggregation • Speed of policy development, approval, distribution • Improved speed/cost of risk reporting • Improved speed/cost/coverage of audits	• Staff-hours saved per process • Payroll savings from delay or avoidance of staff increase • Reduction in costs for internal and external audits
Risk reduction	• Reduction in incidents, near misses, loss events • Reduction in regulatory fines, actions, law suits, etc. • Reduction in time to discover control gaps, violations • Reduction in audit/assessment findings	• Reduced number and cost of incidents • Reduced number/size of fines • Reduced cost of capital • Reduced insurance premiums
Strategic support/ Enhanced performance	• Use of risk info in management/exec decisions • Improved decision making when risk is considered • Risk intelligence coverage • Risk management process coverage • Improved reputation among stakeholders (partners, regulators, customers, etc.)	• Reduction in reactionary costs • Frequency of risk data used in business decisions • Improvement in financial or operational metrics

Tips for Success

- Remember that a large part of maturity will come with connections made between functions, roles, and frameworks.
- Consider the benefits of efficiency and cost reduction first, then look for risk reduction and strategic support for long-term value.
- GRC maturity doesn’t truly happen until you’ve achieved vertical and horizontal reach.

Thank you

Chris McClean

cmcclean@forrester.com

forrester.com