Strategies for Building a

COMPLIANCE MONITORING PROGRAM

for C-Suite, Compliance Officers and Other Professionals

Danielle Sugden, Senior Manager, Accretive Solutions

Core Competencies – C24

Representation

- Roles
- Industry
- New/existing monitoring programs

Interests / Expectations

Biography

- Large cap, small/mid cap, startups/SBA
- Financial institutions, life sciences, retail, professional services, other
- Project management background
- Advisory background
  - Finance and accounting, governance, enterprise risk management, compliance, fraud, internal audit, QAR, strategy, go-to-market, thought leadership, process improvement, data integrity, business transformation, implementation
  - Outsourced, co-sourced, subject matter expertise (SME)
- Client portfolio management
  - Managing multiple concurrent teams and initiatives
  - Leveraging employees, clients, contractors, remote/off-shore
- End-to-end
  - Thought leadership, proposal process, scoping, project and collateral design, resourcing, project management, SME, management and executive reporting, metrics, performance management

Learning Objectives

- Current environment
  - Themes, drivers, authorities
- Second line of defense
  - Governance and oversight
  - Leveraging GRC
  - Risk assessment
  - Approach to ongoing monitoring/testing
  - Communication
  - Reporting
- Project management
- Implementing monitoring programs

CURRENT ENVIRONMENT

A1

Key Drivers

- Data breach
- Lawsuits
- Regulatory penalties
- MOUs, cease-and-desist orders
- Consumer protection
- Effectiveness, oversight, productivity, speed

Common Themes and Priorities

- Cyber attacks
- Privacy
- Data protection
- Anti-corruption
- Model risk management
- Third-party risk
- End customers
- Fraud
- Export compliance

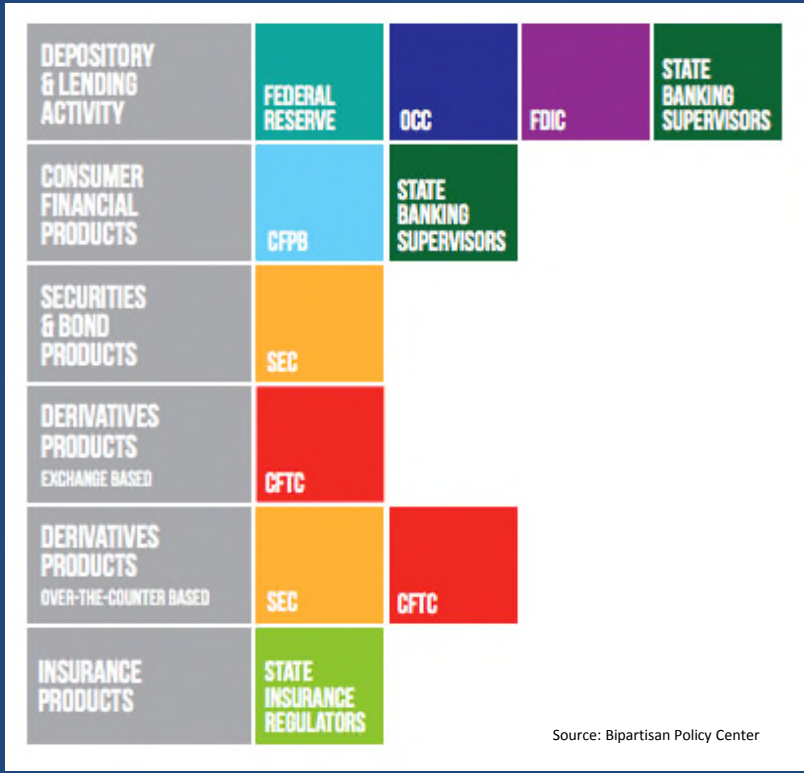
Example Authorities – Direct & Indirect

Example x-industry rules and authorities:

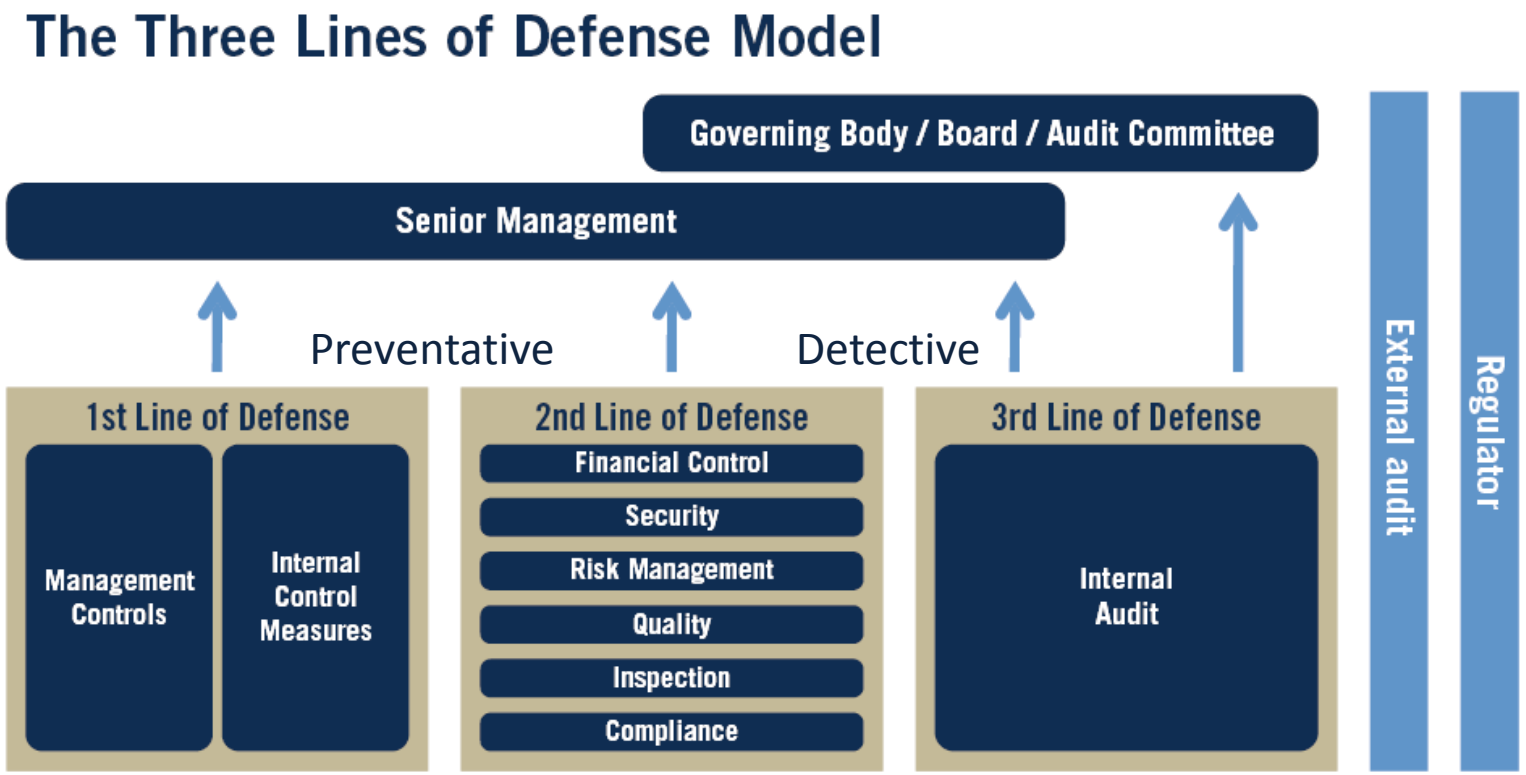
- SEC/GAAP, PCAOB
- Exchanges
- FTC
- GLBA, EU privacy laws
- HIPAA
- PCI
- OSHA, ADA

Example industry-specific rules and authorities:

- BASEL, BHC
- FRB, OCC, FDIC
- FFIEC, BSA/AML, OFAC
- FINRA
- State insurance regulators
- CFPB
- UDAPP

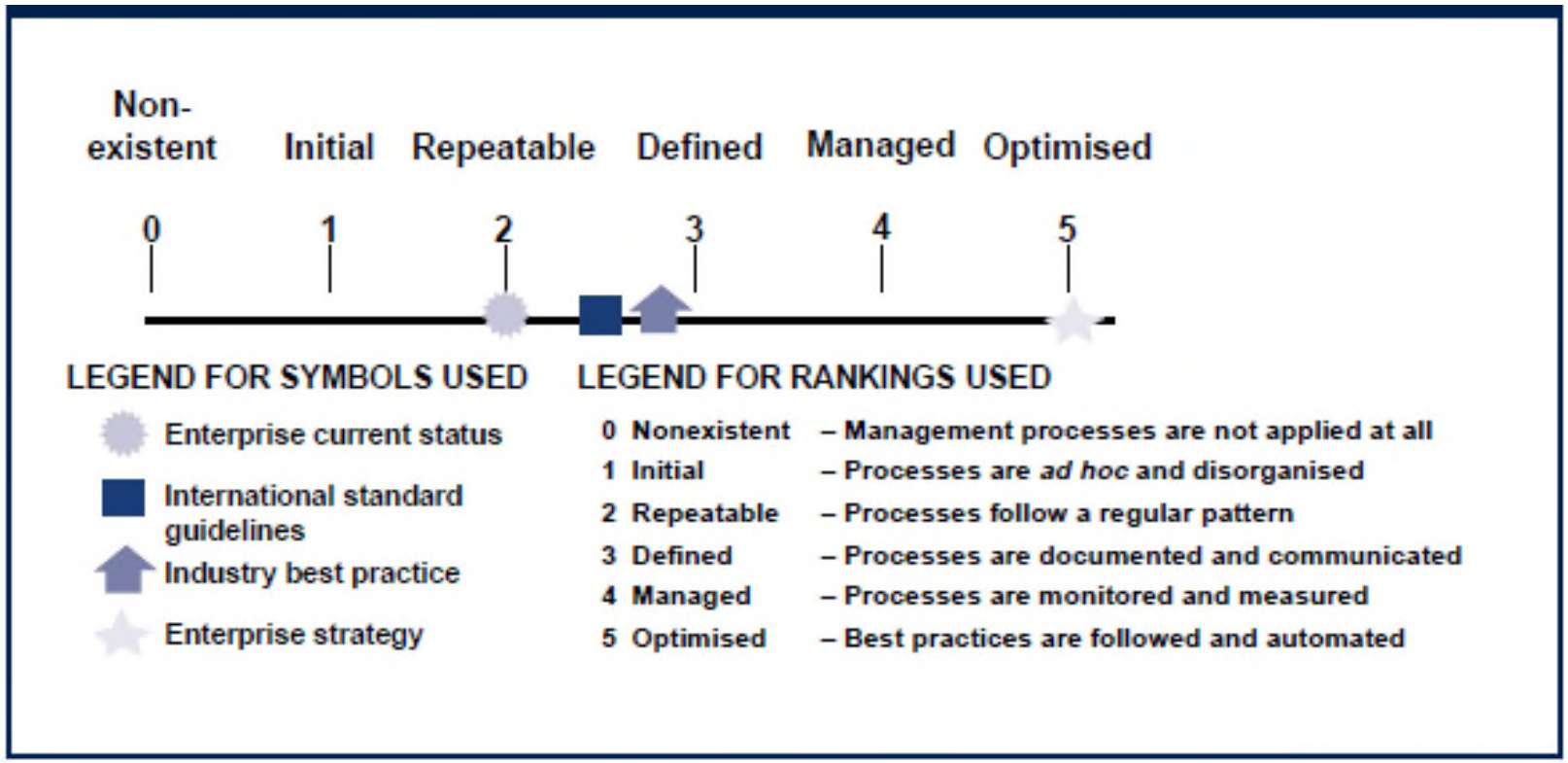


The Three Lines of Defense



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Maturity Model



Summary: Current Environment

- Key drivers
- Common themes and priorities
- Direct and indirect authorities
- The three lines of defense
- Maturity model

SECOND LINE OF DEFENSE: CONTINUOUS MONITORING

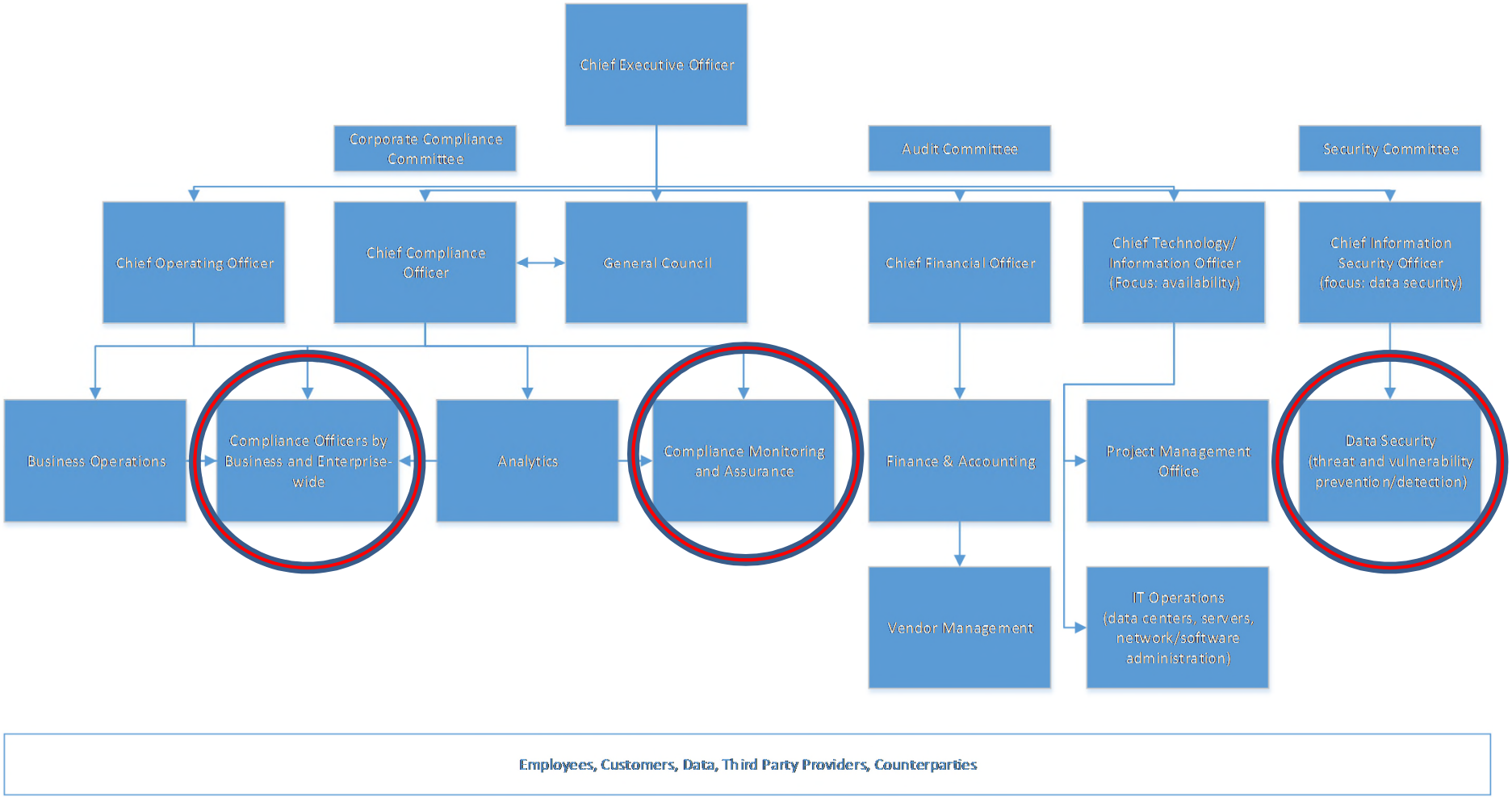
Continuous Monitoring Framework

- Governance and oversight
  - Leveraging GRC
  - Importance of data analytics
- Risk assessment
- Positioned ongoing monitoring/assurance
- Communication
- Reporting
- Project management

Governance and Oversight

- Structure
- Clear roles (enterprise-wide) and accountability
- Qualified business partners (technical, PMs)
- Program charter, standards, methodologies
- Tools and collateral
  - Workflow, sharing, version control, repository
- Roadmap the future state goals
- Strategic objective alignment

Example Monitoring Placement



Governance, Risk and Compliance

- Strategic alignment
- Consistent methodology and approach
- Coordination and connectivity
- Example partners:
  - Enterprise Risk Management, Compliance counterparts, Finance, Internal Audit, Regulatory Reporting, Security, Fraud Prevention, Detection and Investigations, Vendor Management, Human Resources, Corporate Training

GRC Tools-Vendor Comparison

Vendors	**Usability**	**Cost**	**Maturity**	**Scalability**	**Flexibility**	**Collaboration**	**Total Score**
Lockpath	5	5	3	4	3	4	24
Archer (RSA)	3	3	5	4	5	4	24
Compliance 360	3	3	2	2	3	2	15
GRC Cloud (Resolver)	5	5	1	3	2	2	18
RSAM	3	4	4	3	3	3	18
Agilliance	5	5	2	3	3	3	21
Modulo	3	4	3	2	2	4	18
Thompson Reuters (Accelus)	4	3	4	3	3	3	20

Scale: 5 = Great 4 = Good 3 = Average 2 = Below Average 1 = Poor

Source: IANS, 2014 www.iansresearch.com

Tools and Collateral

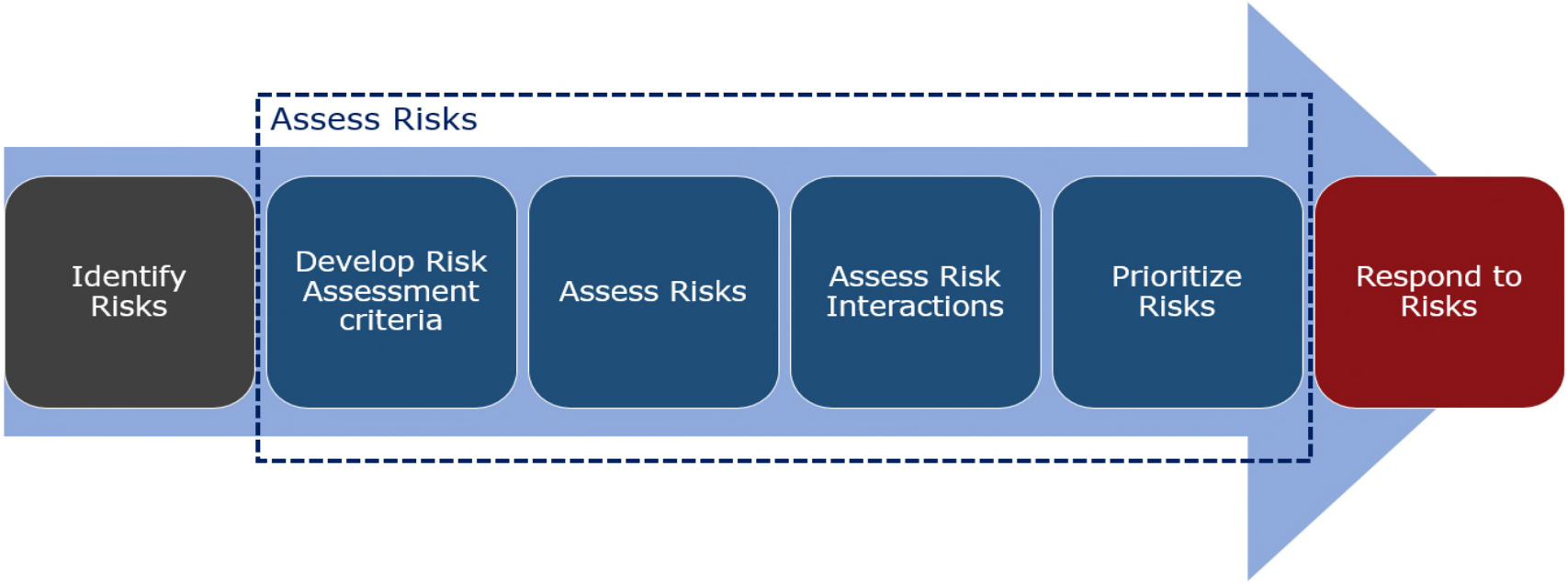
- Program charter, policy, procedures
- Risk (materiality) assessment
- Flowcharts and/or narratives
- Risk/regulatory inventory and control matrices
- Reporting templates
- Dashboards

Data Analytics

- Platform maturity/automation
  - Enterprise architecture
  - Complexity of organization/processing
  - Sensitivity of data
  - Control environment (e.g., change management)
- Automation, modeling technologies
- Key report reliance
- Spreadsheets and databases

Risk Assessment

- Inherent risk identification/inventory
- Company materiality analysis **involve staff in the planning process*
- Risk scoring (drives prioritization and scoping)



Assessing Likelihood and Impact

Sample criteria for prioritizing:

- Products, services, functions
- Laws, regulations, guidance
- Threat and vulnerability
- Systems (customer facing vs. financial reporting)
- Volumes and ($) materiality
- Off-balance sheet impact
- Maturity of control environment
- Recent changes (people, process, systems), losses, emerging risks
- Outsourced and off-shoring relationships: (TPPs, CFPB)
- Unique business transactions (RPs, assets, customers)
- Regulatory required monitoring

ERM – Risk Categories

- Strategic and model
- Credit and market (liquidity, interest and price)
- Operational (transactional)*
- Compliance (legal)
- Fiduciary (legal)
- Reputational*
- Third-party provider, counterparties (TPP, concentration)
- Information security
- Business continuity / disaster recovery

*Not directly relevant to compliance monitoring

Annual and Rolling Plan

- 1-to-3 year rolling plans
- Verticals and horizontals

Monitoring Roles

- 1st line of defense
- 2nd line of defense (2a)
  - Compliance advisory
  - Pre-submission and quality control
    (SOD, Management or Compliance, depending)
  - Shared services / centers of excellence
- 2nd line of defense (2b)
  - Compliance monitoring/assurance: verticals, horizontals
- 3rd line of defense
  - Internal audit

Continuous Monitoring Approach

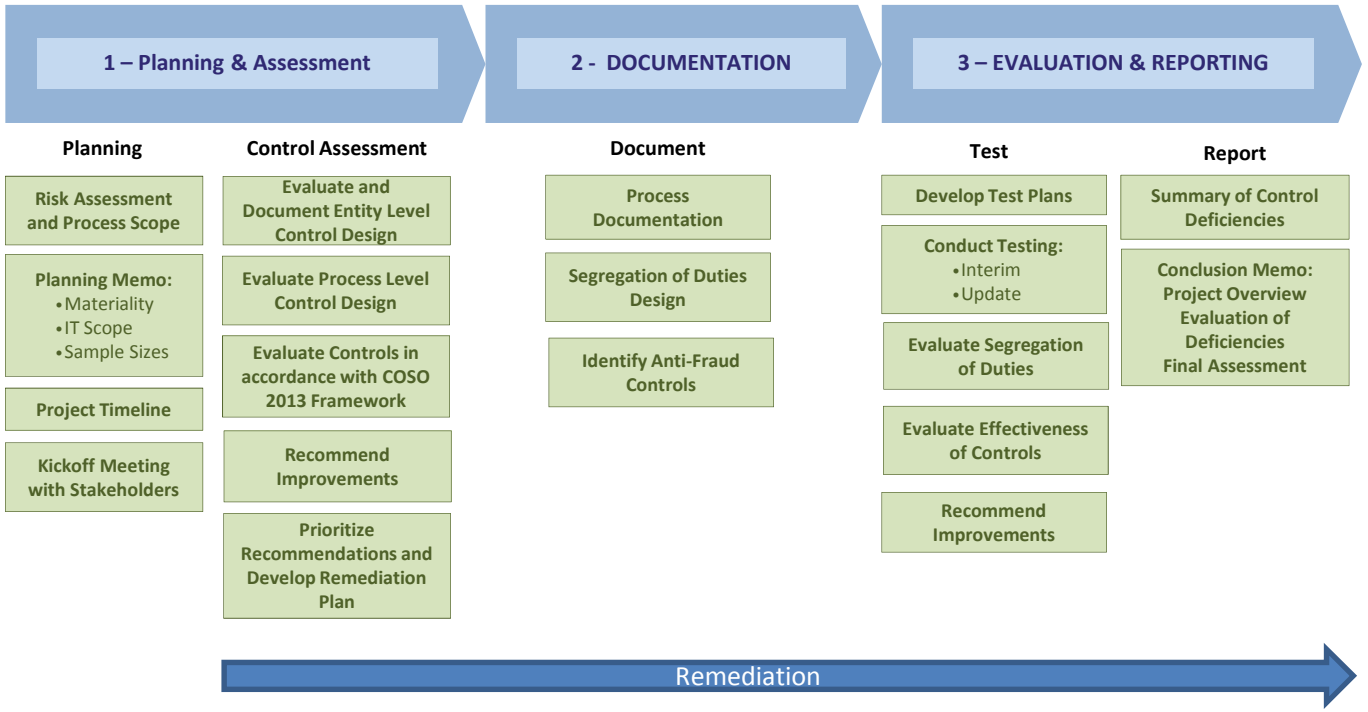
Staggered approach in scoping and assurance:

- Modeling technologies and red flag reporting
- Data analytics and targeted sampling
- Control-based testing
- Substantive testing
- Complaint management and incident tracking
- Remediation testing
- Targeted ongoing monitoring

Leveraging Internal Controls and GRC

- Base year:
  - Walkthroughs, design assessment
  - Integrative reviews
  - Controls identification (process, sub-process)
  - Control mapping and gap analysis
  - GRC/ELC mapping (BOD, ARC, CCC, CRC, etc.)
  - Key analytics identification
  - Targeted operating effectiveness and substantive testing
  - Cross-functional leadership meetings
  - Implementation
- Year two and beyond:
  - Changes, losses, emerging risks
  - Process optimization
  - Program benchmarking
  - (Balanced) collateral optimization

Controls-based Overview



Communication

- Share program vision, tie-in to strategic objectives
- Partner with regulators and other authorities
- Set a common language, policies and procedures
- Set communication channels
- Train at onset and via periodic refreshers
- Require business line management certify periodically

Management and Executive Reporting

- Reporting on issue, impact, action plan
- Self identified vs. third-party identified
- Incentive-based performance management
- Executive dashboards
- Tools

Remediation

- Tracking
- Portfolio impact analysis and prioritization
- Resolution and closure
- Escalation
- Executive reporting

PROJECT MANAGEMENT

Project Management

- Budgeting
- Scheduling
- Time tracking
- Leveraging firms and contractors
- Status reporting
- Subject matter expertise
- Feedback loops

Third Party Reliance

- Quality, re-performance standards, workpapers
- Enhanced reliance by:
  - Internal Audit
  - Regulators
  - Other third parties
  - Business partners

Performance Management Metrics

Measuring the effectiveness of Compliance:

- Quantitative and qualitative metrics (hours, spend, capacity, quality)
- Reporting
- Remediation
- Self assessment
- Balanced scorecards and surveys
- Benchmarking
- QAR / third party reviews

IMPLEMENTING A CONTINUOUS MONITORING PROGRAM

Implementation Planning

- Gap analysis and roadmap
- Board / Management support
- Project manager, sponsor(s), stakeholders
- Project planning: timeline, budgeting, dependencies, contingencies, metrics
- Communications

Common Challenges

- Common methodology, defined standards, training
- Planning
  - Calendaring, readiness, budgeting, redundancy/coordination, emerging projects
- Managing to the plan
  - Over/under-testing (e.g., scope creep, ineffective testing)
  - Balancing quality and efficiency
  - Flexibility / scope adjustments
- Quality
  - Independence
  - Re-performance standards
  - Measurement: specific and verifiable
- Communication and reporting

Monitoring as a Value Driver

- Platform for culture setting
- Competitive market positioning (risk profiles, risk-taking)
- Compliance as a Consultant
- Efficiency and efficacy
- Customer experience and branding

Monitoring as a Value Driver

- Enables information security
  - Categorizing information systems
  - Assessment of security controls
  - Monitoring security controls
- Improves situational awareness
  - Improves understanding of assets in the environment and allows for dynamic adjustments
  - Reduces opportunities of threats and risks impacting the network
- Reduces program cost
  - Reduces costs involved with systems and network maintenance
  - Reduces costs and improves security posture and risk management
- Monitoring examples
  - User access or user log monitoring
  - Security controls monitoring – regular self audit, security access, physical security, ITGCs, application controls, logging and monitoring – real time security threats – security performance vs assurance of security practices – level of security drives scope – threat and vulnerability testing, realtime threat assessments, logging and monitoring (login attempts) looking for anamolies, system determines what is normal activity vs. anomalies, someone has to review the output, Drip Wire tool = file integrity monitoring, network traffic monitoring, packet sniffer, tools sit on top of real time data
  - File integrity monitoring
  - Encryption of data monitoring
  - Applications and systems change management monitoring

Takeaways / Action Planning

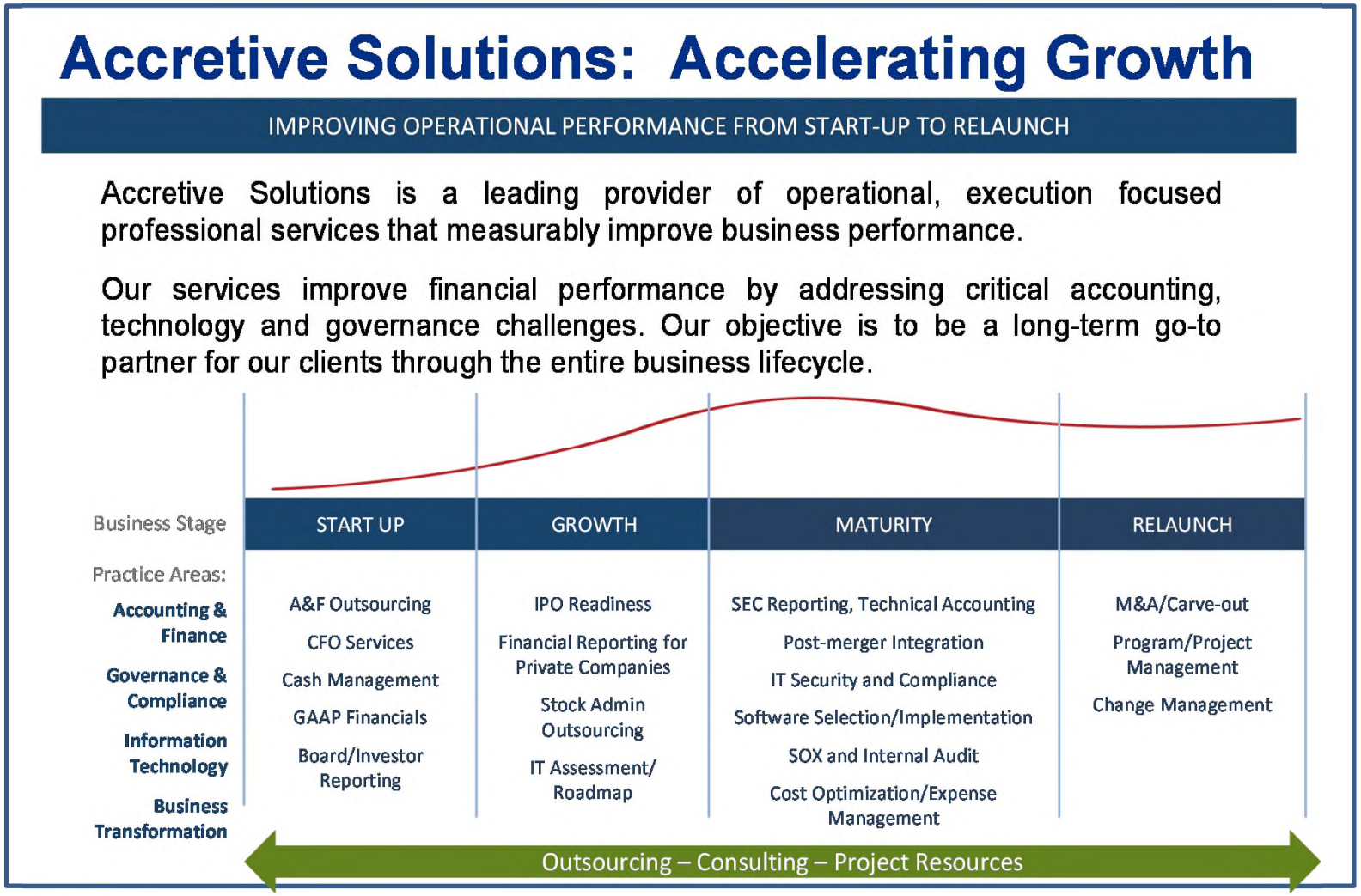
Immediate needs

Mid-term needs

Long-term needs

Nice to haves

Accretive Solutions



Q&A

Thanks for your time!

Danielle Sugden
Senior Manager
dsugden@accretivesolutions.com
linkedin.com/in/daniellesugden
510.421.0496

Resources

Resources	ISACA/COBIT
	COSO Treadway
	ISO 27001
	PCAOB
	SEC
	CFPB
	FFIEC
	American Bankers Association
	California Bankers Association