Integrated GRC

Akhenaton Marcano, Assistant General Manager – Group Operational Risk & Controls, First Citizens Bank

GRC SUMMIT 2019
BALTIMORE, JUNE 2-5
Hosted by MetricStream

Agenda

Organization Overview: Vision, Key Facts and Needs

GRC Program Governance & Challenges

R3: Readiness, Roadmap and Rollout

Business Value and Realized Benefits - Before and After

Key Learnings and Best Practices

Audience Questions and Discussion

Introducing First Citizens Bank

- Leading indigenous Trinidad & Tobago financial services group
- Publicly traded company listed on the Trinidad & Tobago Stock Exchange
- Majority state ownership by Government of Trinidad & Tobago
- Operations in the Caribbean and Central America
- Offers retail, commercial and corporate banking services as well as asset management, capital markets and brokerage products
- Consistently rated investment grade with current S&P rating of BBB (stable)
- Bank of the Year 2017 – The Banker
- Safest Bank in Trinidad & Tobago 2017– Global Finance

Introducing First Citizens Bank

Introducing First Citizens Bank

VISION

To be our stakeholders' preferred financial partner through excellence, care and integrity

MISSION

We build rewarding and sustainable relationships through a highly engaged team, versatile and secure technology, and innovative financial services

Introducing First Citizens

PERFORM WITH INTEGRITY

Introducing First Citizens

Key Banking Industry challenges in the English-speaking Caribbean:

- Executing an effective digital banking strategy that balances risk and reward in the context of customer readiness and payback period
- Addressing greater regulatory scrutiny and expectations around capital adequacy, information security, data privacy, financial crime (including AML and CFT) and customer care while remaining profitable
- Expansion of company footprint beyond domestic borders in the face of market saturation and unremarkable economic growth

First Citizens GRC Program

Governance Model and Decision Making among Stakeholders

- Board Enterprise Risk Management Committee implementation approval and high-level oversight of GRC progress
  - Quarterly Reporting with focus on overall alignment to Risk & Controls pillar of the Group's strategy
  - Provide high level guidance on the implementation and roll-out approach
- Executive-level Project Steering Committee (chaired by the CRO with membership of the CIO, CFO and other assurance leaders) responsible for integrative policy decisions, budget variation approvals and overall project risk management
  - Monthly Reporting with focus on achievement of scope, budget and timelines
  - Provide direction on cross-functional themes e.g. issue management
  - Interrogate benefits realization and monitor progress of roll-out
- Cross functional project team led by the Head – Group Operational Risk & Controls and coordinated by the Project Management Office
  - Execute tactical and operational activities e.g. training, use case development, testing
  - Recommend change requests and GRC policy positions to the Steering Committee
  - Troubleshoot day-to-day issues
  - Manage ongoing relationship with MetricStream

First Citizens GRC Program

Key Challenges

- People:
  - Assurance groups understanding changes in both the nature and the means of their work in the aftermath of eGRC
  - Persuasion of the business to explicitly accept their role as first line of defence in risk management
- Processes:
  - Understanding the linkages in the workflows across all the assurance groups and the implicit dependencies on each other
  - Appreciating the areas of ambiguity or inefficiency in the “as is” workflows
- Systems:
  - Shifting from an on-premise IT paradigm to the brave, new world of the cloud
  - Clarification of data ownership and accountability among the assurance groups as well as the business

R3 – Readiness, Roadmap and Rollout

MetricStream Solution Areas:

- Business Continuity
  - Readiness Level: High
  - Justification: Established BIA process, Existing inventory of critical processes, Existing call trees
- Operational Risk
  - Readiness Level: Moderate
  - Justification: Clearly defined operational risk tools, Existing inventory of risks and controls
- Compliance
  - Readiness Level: Low
  - Justification: Baseline awareness of compliance universe
- Policy & Document Management
  - Readiness Level: Moderate
  - Justification: Established document “approval” process, Existing inventory of documented policies and procedures
- Internal Audit
  - Readiness Level: Moderate
  - Justification: Established audit procedures, Established reporting formats

R3 – Readiness, Roadmap and Rollout

Roadmap:

- Philosophy for deployment: BCP is foundation, Op Risk is the centrepiece and Internal Audit is the apex
- Foundational Activities: Libraries
    - Organization – Arrive at a common view of entity hierarchies and reporting lines
    - Processes – Identify the critical processes
    - Assets – Identify the assets that support the critical processes
    - Risks – Define a risk taxonomy and a risk register/inventory
    - Controls – Create an inventory of controls relevant to the organization's risks
- Dependencies
    - Organization chart – Alignment of Compliance and BCP requirements
    - Risk-control linkages – Alignment of Operational Risk and Internal Audit libraries

R3 – Readiness, Roadmap and Rollout

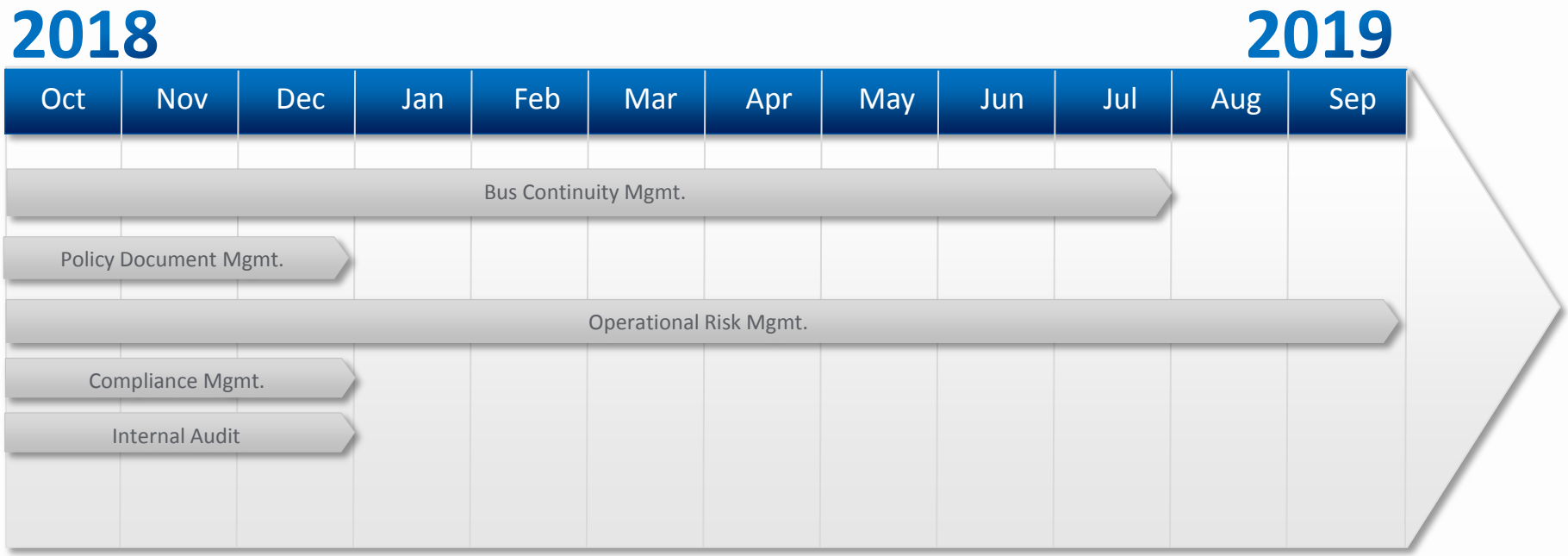
Key Deployment Challenges:

- First major enterprise SaaS implementation – iterative learning process for First Citizens
- Generating “quality” and “quantity” use cases during a FastTrak implementation

Implementation Rollout Strategy and Tactics:

- Life After UAT: Build Enthusiasm and App User Adoption
    - Multi-pronged end user engagement – high touch or low touch as required
    - Targeted evangelization – assurance staff, operations staff, line managers, senior managers
- Organization Change Management
    - Revised GRC processes – e.g. issue management
    - New information flows – e.g. org chart changes
- Communications from Project Team
    - Upward – Senior Management and Board via Steering Committee and Risk Committees
    - Downward – Line management and staff via e-mail advisories
    - Inward – Within assurance groups via workshops

Post-Deployment Rollout Schedule



Business Value and Realized Benefits

MetricStream Apps: Integrated GRC covering Operational Risk, Business Continuity, Regulatory Compliance, Policy & Document Management and Internal Audits on MetricStream Cloud

- Supports approximately 2,000 users – policies & procedures, business impact analyses, issue tracking to all relevant employees
- Enables qualitative and quantitative risk assessments, control self-assessments and KRIs
- Supports risk based audit planning, audit execution and reporting
- Facilitates continuous control monitoring for compliance and other key risks
- Strengthens enterprise-wide visibility into risk and compliance
- Reduced remediation time and action planning
- BEFORE:
  - Manual, duplicative workflows
  - Siloed GRC data
  - Risk is for the risk function
  - More assurance work = greater headcount
  - On-premise system requiring in-house support

AFTER:

- **Automated, efficient workflows**
- **Single GRC data repository**
- **Risk is everyone's business**
- **Extremely high scalability for assurance functions**
- **High-availability, secure SaaS solution**

Business Value and Realized Benefits – BCP Focus

- Coverage of over 1,000 “critical” processes
- Clear identification of critical assets related to those processes
- Centralized repository of critical employee contact information
- Enables rating of confidentiality, integrity and availability of information assets (aligned to ISO27001)
- Supports highly robust assessment of recovery time objectives
- Supports logical development of recovery strategies
- Enables the responsible parties to readily access their documented business continuity plans

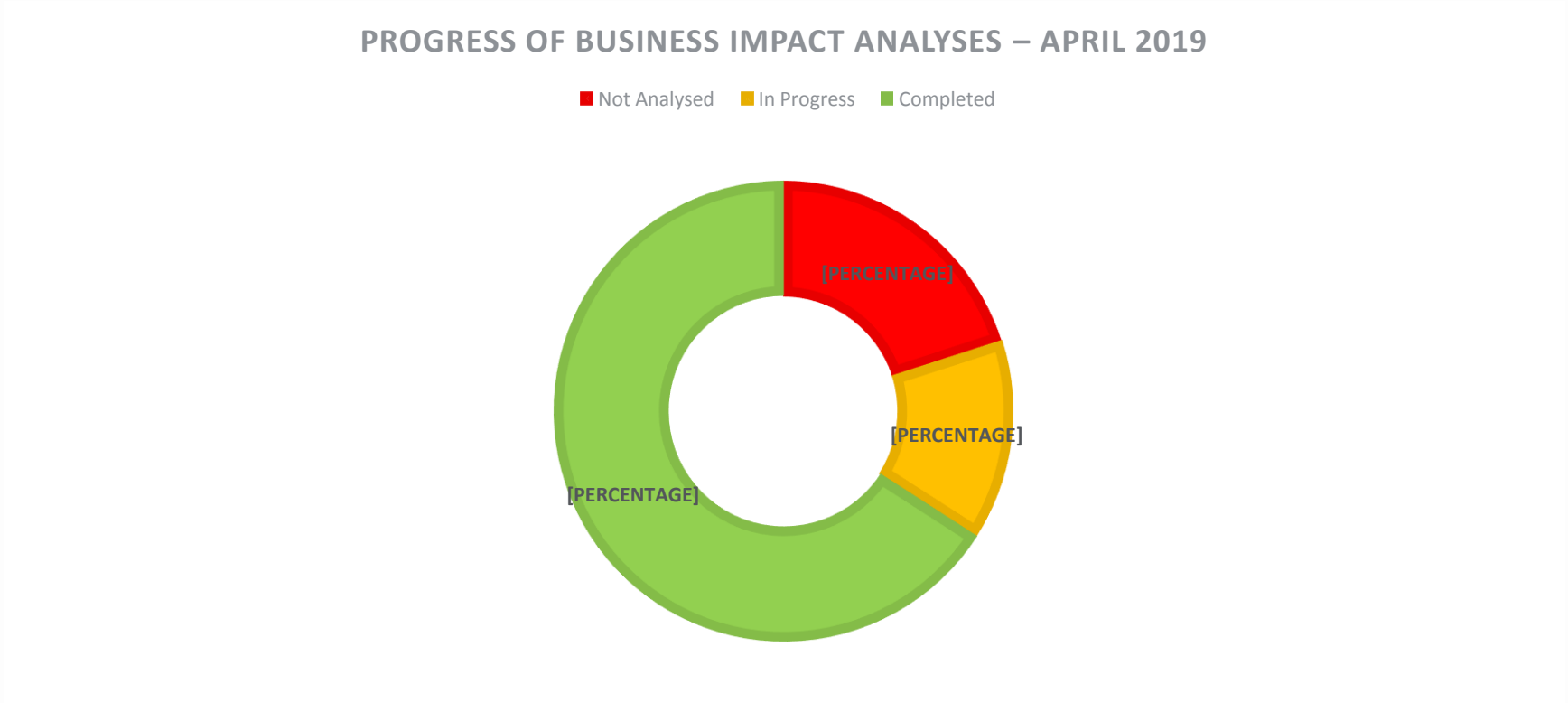
BEFORE:

- Manual, time-consuming workflows
- Siloed BCP workflows
- BCP is for the BCP function
- More BCP work = greater headcount

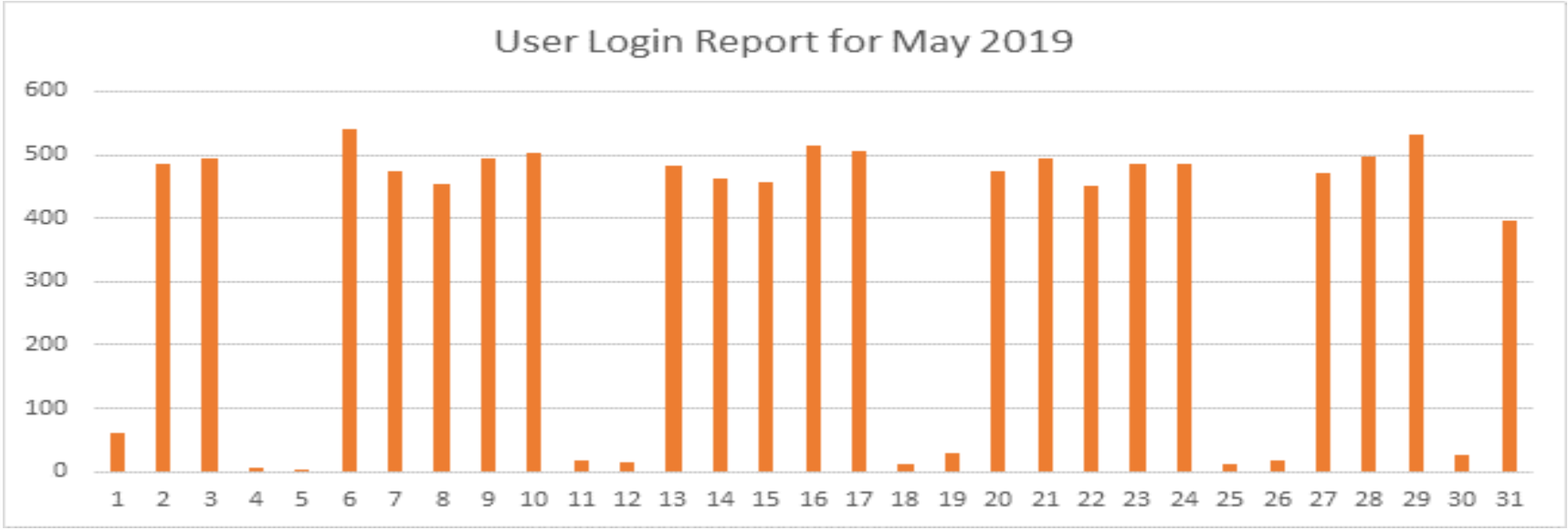
AFTER:

- **Automated, efficient workflows**
- **BCP workflows integrated with Information Security and Operational Risk workflows**
- **BCP is the business’ business**
- **Extremely high scalability for BCP**

Business Continuity Module Value Add



User Acceptance



Key Learnings and Best Practices

Key Learnings:

- Get the ducks in a row – take into account both logical flow and user readiness when sequencing multi-app deployment
- The whole is greater than the sum of the parts– build cross-functional use cases and devise integration tests
- More haste, less speed – treat rollout and user acceptance as a marathon, not a sprint

Best Practices:

- Invest in Metricstream University training for project team – it pays dividends in accelerating user acceptance
- Adopt out-of-the-box implementation – it may not be perfect but the alternative of significant customization has limited added value

The Road Ahead:

- Embedding eGRC into everyday operational activities e.g. e-mail notifications
- Extracting greater business value from eGRC e.g. reporting

QUESTIONS?

Thank You

Continue the conversation on #GRCSummit

GRC SUMMIT 2019

BALTIMORE, JUNE 2-5

Hosted by MetricStream