Technical Engineering Services - RISK Dashboard

Audit Status

Findings Due February	8
Findings Overdue	1
Total Findings Open	18
Findings Closed 2018	1
Findings Opened 2018	3
Access Findings Open	14
Total Reports Published 2018	3
Unsat Reports Published 2018	1

Risk Info

Total Active Risks 2018	10
P1 Material Failures YTD	0
Financial Losses YTD	0
YTD P1 Problems	6
YTD DR Success	97%
Policies Updated	10%
Active Risk Acceptances	3
OoS Systems	25

Compliance

Network Next Training	92%
AML Training	87%
OBI Declarations	30%
YTD G&E Declared	234
PAT Alerts	22
BCM Actions Outstanding	18

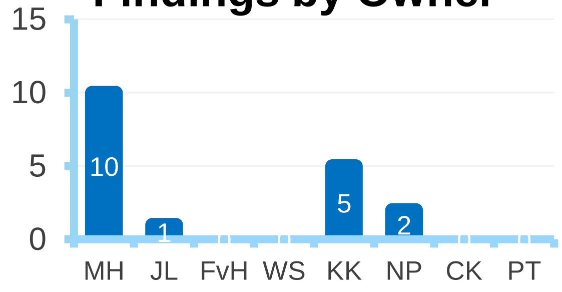
Technical Engineering Services - RISK Dashboard

February 2018

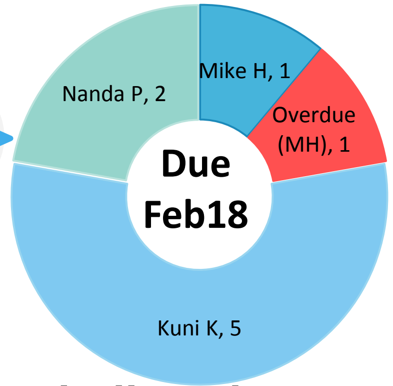
On Track

Backlog March 2018:
1) Update CTO Risk Cards and Reports
2) Close Audit Findings
3) CTO OpRisk Audit Finalization
4) Update 4 IT Standards

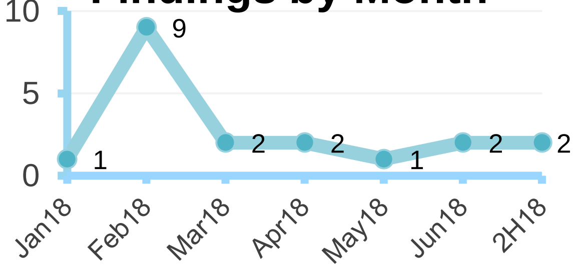
Findings by Owner

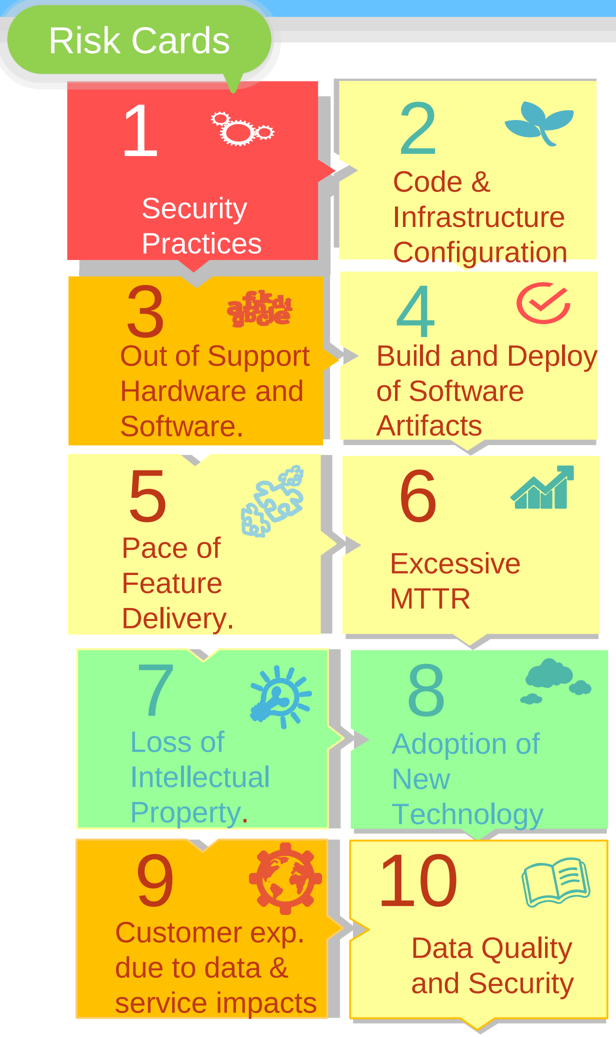


Audit Status



Findings by Month





Risk Cards

1 Security Practices

2 Code & Infrastructure Configuration

3 Out of Support Hardware and Software.

4 Build and Deploy of Software Artifacts

5 Pace of Feature Delivery.

6 Excessive MTTR

7 Loss of Intellectual Property.

8 Adoption of New Technology

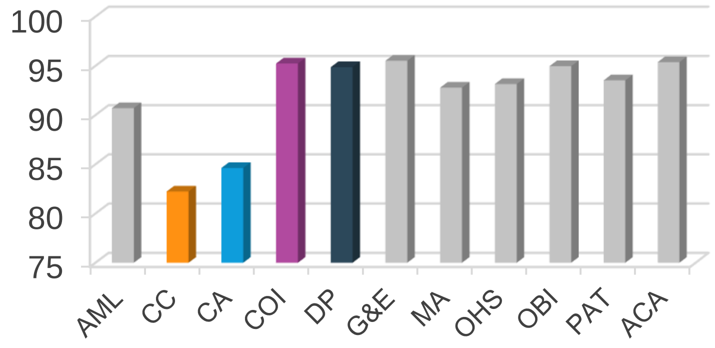
9 Customer exp. due to data & service impacts

10 Data Quality and Security

IT Policies &Standards Update 2018

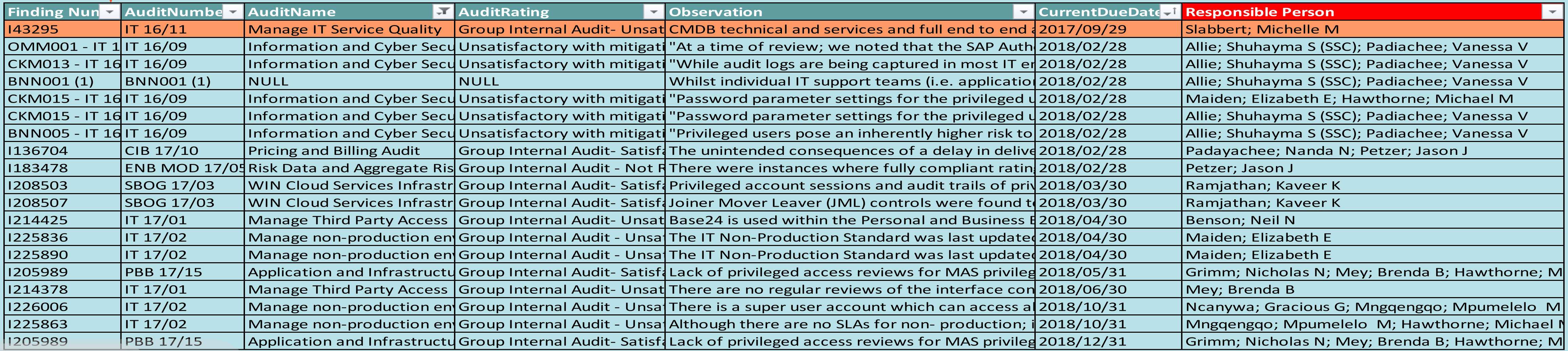
Published	
Waiting Approval	
Under Review	- IT Software Engineering - Software Quality Engineerin
Update In Progress	- Non Prod Environments - IT Cloud Management

Network Next Training



Technical Engineering Services - RISK Dashboard

Open Audit Findings



Finding Nun	AuditNumbe	AuditName	AuditRating	Observation	CurrentDueDate	Responsible Person
I43295	IT 16/11	Manage IT Service Quality	Group Internal Audit- Unsat	CMDB technical and services and full end to end	2017/09/29	Slabbert; Michelle M
OMM001 - IT 1	IT 16/09	Information and Cyber Secu	Unsatisfactory with mitigati	"At a time of review; we noted that the SAP Auth	2018/02/28	Allie; Shuhayma S (SSC); Padiachee; Vanessa V
CKM013 - IT 16	IT 16/09	Information and Cyber Secu	Unsatisfactory with mitigati	"While audit logs are being captured in most IT er	2018/02/28	Allie; Shuhayma S (SSC); Padiachee; Vanessa V
BNN001 (1)	BNN001 (1)	NULL	NULL	Whilst individual IT support teams (i.e. applicatio	2018/02/28	Allie; Shuhayma S (SSC); Padiachee; Vanessa V
CKM015 - IT 16	IT 16/09	Information and Cyber Secu	Unsatisfactory with mitigati	"Password parameter settings for the privileged u	2018/02/28	Maiden; Elizabeth E; Hawthorne; Michael M
CKM015 - IT 16	IT 16/09	Information and Cyber Secu	Unsatisfactory with mitigati	"Password parameter settings for the privileged u	2018/02/28	Allie; Shuhayma S (SSC); Padiachee; Vanessa V
BNN005 - IT 16	IT 16/09	Information and Cyber Secu	Unsatisfactory with mitigati	"Privileged users pose an inherently higher risk to	2018/02/28	Allie; Shuhayma S (SSC); Padiachee; Vanessa V
I136704	CIB 17/10	Pricing and Billing Audit	Group Internal Audit- Satisfa	The unintended consequences of a delay in delive	2018/02/28	Padayachee; Nanda N; Petzer; Jason J
I183478	ENB MOD 17/05	Risk Data and Aggregate Ris	Group Internal Audit - Not R	There were instances where fully compliant ratin	2018/02/28	Petzer; Jason J
I208503	SBOG 17/03	WIN Cloud Services Infrastr	Group Internal Audit- Satisfa	Privileged account sessions and audit trails of priv	2018/03/30	Ramjathan; Kaveer K
I208507	SBOG 17/03	WIN Cloud Services Infrastr	Group Internal Audit- Satisfa	Joiner Mover Leaver (JML) controls were found t	2018/03/30	Ramjathan; Kaveer K
I214425	IT 17/01	Manage Third Party Access	Group Internal Audit- Unsat	Base24 is used within the Personal and Business E	2018/04/30	Benson; Neil N
I225836	IT 17/02	Manage non-production en	Group Internal Audit - Unsa	The IT Non-Production Standard was last update	2018/04/30	Maiden; Elizabeth E
I225890	IT 17/02	Manage non-production en	Group Internal Audit - Unsa	The IT Non-Production Standard was last update	2018/04/30	Maiden; Elizabeth E
I205989	PBB 17/15	Application and Infrastructu	Group Internal Audit- Satisfa	Lack of privileged access reviews for MAS privileg	2018/05/31	Grimm; Nicholas N; Mey; Brenda B; Hawthorne; M
I214378	IT 17/01	Manage Third Party Access	Group Internal Audit- Unsat	There are no regular reviews of the interface con	2018/06/30	Mey; Brenda B
I226006	IT 17/02	Manage non-production en	Group Internal Audit - Unsa	There is a super user account which can access a	2018/10/31	Ncanywa; Gracious G; Mngqengqo; Mpumelelo M
I225863	IT 17/02	Manage non-production en	Group Internal Audit - Unsa	Although there are no SLAs for non- production; i	2018/10/31	Mngqengqo; Mpumelelo M; Hawthorne; Michael M
I205989	PBB 17/15	Application and Infrastructu	Group Internal Audit- Satisfa	Lack of privileged access reviews for MAS privileg	2018/12/31	Grimm; Nicholas N; Mey; Brenda B; Hawthorne; M

Risk Cards / Actions

	Risk Cards	1) SECURITY PRACTICES	2) CODE &INFRASTRUCTURE CONFIGS	3) OUT OF SUPPORT (OOS) HRW AND SWR	4) BUILD & DEPLOY OF SWR ARTEFACTS	5) PACE OF FEATURE DELIVERY	6) EXCESSIVE MTTR	7) LOSS OF INTELLECTUAL PROPERTY	8) ADOPTION OF NEW TECHNOLOG	9 CUSTOMER EXPERIENCE DUE TO DATA & SERVICE IMPACTS	10) DATA QUALITY	11) DATA SECURITY
	Residual Risk	🟥	🟨	🟧	🟨	🟨	🟨	🟩	🟩	🟧	🟨	🟨
	Owner	MH / JL	MH	MH	JL / MH	JL / MH	MH	JL / MH	JL / MH	MM	NP	NP
1	Mitigating Actions	IT Security Management Policy adherence	Monitor Configuration Drift, & its ability to revert within 30min	Manage technology roadmaps, and exit OoS technologies.	Continuum Baseline and Maturity Monitoring across estate.	Identify the primary contributors to cross-portfolio dependencies	Complete the Telemetry and Monitoring program	Rebalance the workforce to an 80:20 perm vs. non-perm ratio.	Implement a program to improve/acquire engineering skills..	IT Simplification, CSR, Security	Definition of IT responsibility for data stewardship	Complete Cyber Security Deep Dive Remediation Project
2		Security updates issued by vendors are applied. incl. Patch Management	Pilot version control and delivery pipeline across all Infrast "domains".	Implement OoS and Risk Acceptance approval process.	Acquire toolsets (CI/CD/Automated Testing, etc.)	Refactor monolithic applications.	Finalise Service Level Agreements with all Business Areas	Aggressively automate all "automatable" activities.	Make available different options for education and training	Address EoL / OoS Technologies	Alignment with Enterprise Data Committee Policies	Decommission and Replace Redundant platforms
3		Automated Pipelines for Continuous delivery , testing & access control	Train and skill Infrast staff in technologies and practices	Minimum contracting requirements (with Group Procurement)	Train swr engineers on the use of the requisite toolsets and practices.	Re-factor shared database architectures.	Rectify ITSM systems and enforce processes within IT.	Define and implement a program to improve/acquire engineering skills.	Change the recruitment process to attract and acquire top class talent	PI Planning - Includes Flow, MTTR, Security	Definition of minimum data requirements including customer data	Apply Security Standards across all Data Services Platforms
4		OoS technology is proactively managed to ensure security updates.	Rollout version control tools & practices across Infrastructure estate.	Proactive interface with CIO's ito Technology Life Cycle Management	Continuous Integration / Deployment across all development teams.	Decouple portfolio delivery by removing cross dependencies.	Benchmarked timescales to rectify certain outages			Automation – CD / CI Development Pipeline	Integration of systems and applications for Universal Bank	Onboard DS Staff onto SailPoint access management platform
5		Engineers are schooled in good security practices.	Next Generation Infrastructure and Network roll-out	The implementation & finalization of the resilience program.	Prioritize roll-out of CI/CD on SAFe program backlog.	Re-distribute mainframe workloads	Improve the accuracy of the Configuration Management Database			Control Assessments and Assurance	Increase usage of reference data management	Sourcing and Implementation of a data protection solution
6		There is visibility of security vulnerabilities across all of the estate..	Resilience Programme / Decommissioning / Simplification	Improve technology domain management ito hype cycles	Circuit Breaker Patterns & Service Monitoring for improved resilience	Quicker functionality testing using API's and to reduce flow	Fix number of incident and problem alerting, & reduce false positives			IT Service Continuity Management	Data management standard for customer data	Logical Access Management Reviews
7		Logical / PUM Access Management Policy and Standards adherence		Risk Acceptance for all EoI and OoS technologies		Roll out of Continuum across all feature teams to measure maturity.	Know the priority of all outages and focus on high alerts			IT Incident & Problem Management	IT Architecture Governance	
8										IT Change Management		