Business Managed Services Team

Monthly Report

Reporting Period August 2022

Fenchurch Bank

Date of data pull: 01/09/2022

Confidentiality

This document contains confidential and proprietary information of THYNK Limited ('THYNK'). Fenchurch Bank may not disclose the confidential information contained herein to any third party without the written consent of THYNK, save that Fenchurch Bank may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of Fenchurch Bank's evaluation of the document. Fenchurch Bank agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as Fenchurch Bank. As a condition of receiving this document, Fenchurch Bank agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of three (3) years from the issue date of this document.

Table of Contents

1 Introduction

This report is organized in five sections with focus on data visualization over information overload. When presenting graphs, percentages are rounded; when in tables, percentages are to two decimal places.

ServiceNow DataSources are the source of truth for this report.

1.1 Service Level Management Objectives

Our internal means measuring service performance against clear objectives are more demanding than Service Level Objectives (SLO), which are shown below:

1.1.1 Event Management

SLO	Target (HH:MM)	SLO Objective
Alert Response	<= 00:30	90%

1.1.2 Incident Management

SLO	Target (HH:MM)	SLO Objective
P1 First Update	<= 00:30	90%
P2 First Update	<= 03:00	
P3 First Update	<= 05:00	
P4 First Update	Next business day	
P1 Resolution	<= 10:00	
P2 Resolution	<= 12:00	
P3 Resolution	<= 24:00	
P4 Resolution	<= 48:00	

1.1.3 Service Request Management

SLO	Target (HH:MM)	SLO Objective
P3 First Update	<= 04:00	90%
P4 First Update	Next business day	
P3 Resolution	<= 10:00	
P4 Resolution	<= 30:00	

2 SLO Instance Details and Trends

The table below presents the SLO count, success ratio and total number of breaches in a table format for the current reporting period only.

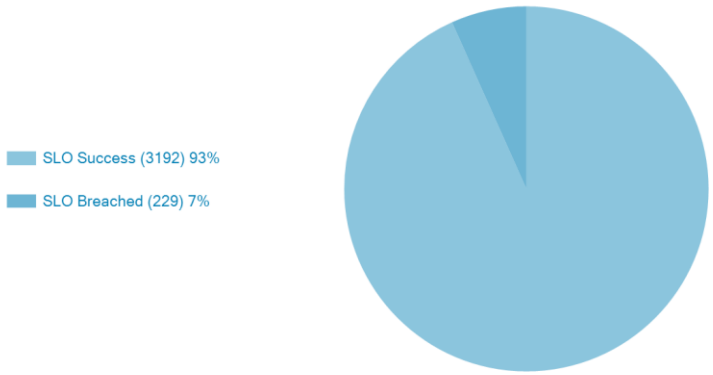
2.1 Instance Details

2.1.1 Event Management

SLO Definition	Target Time	Count	Success Ratio %	Breaches
Alert Response	<= 00:30	10109	96.95	308

2.1.2 Incident Management

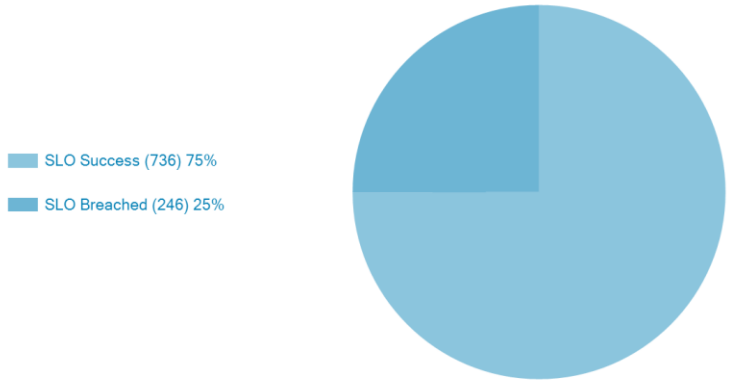
SLO Definition	Target Time	Count	Success Ratio %	Breaches
P1 First update	<= 00:30	1	100.00	0
P2 First update	<= 02:00	55	100.00	0
P3 First update	<= 04:00	686	100.00	0
P4 First update	<= 24:00	921	99.89	1
P1 Resolution	<= 08:00	2	100.00	0
P2 Resolution	<= 08:00	108	78.70	23
P3 Resolution	<= 24:00	750	85.33	110
P4 Resolution	<= 40:00	898	89.42	95
Total		**3421**	**93.31**	**229**



SLO Success and Breached

2.1.3 Service Request Management

SLO Definition	Target Time	Count	Success Ratio %	Breaches
P3 First update	<= 04:00	207	99.52	1
P4 First update	Next business day	299	99.67	1
P3 Resolution	<= 10:00	200	7.00	186
P4 Resolution	<= 30:00	276	78.99	58
Total		**982**	**74.95**	**246**

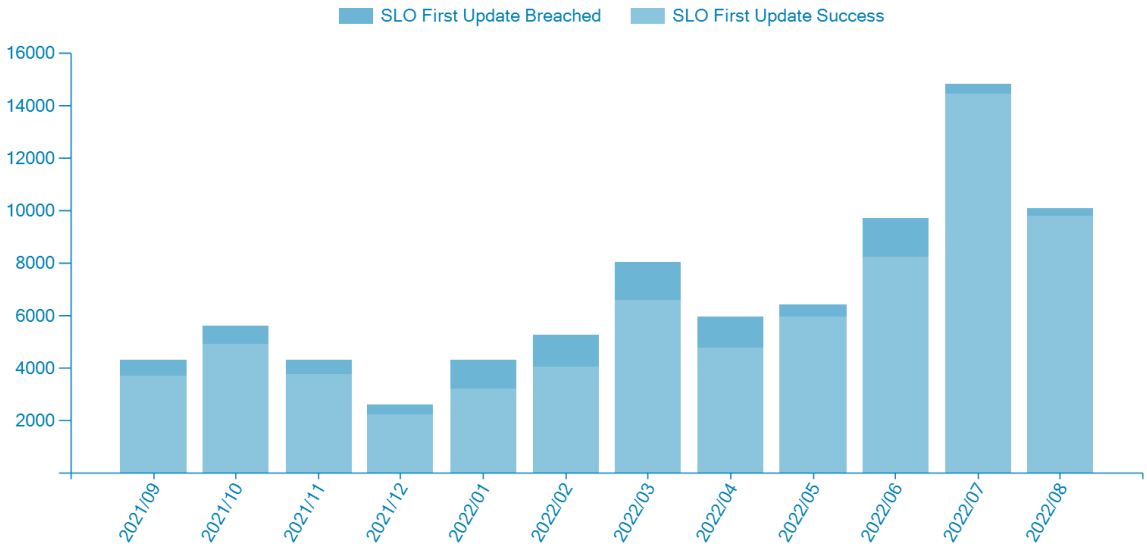


SLO Success and Breached

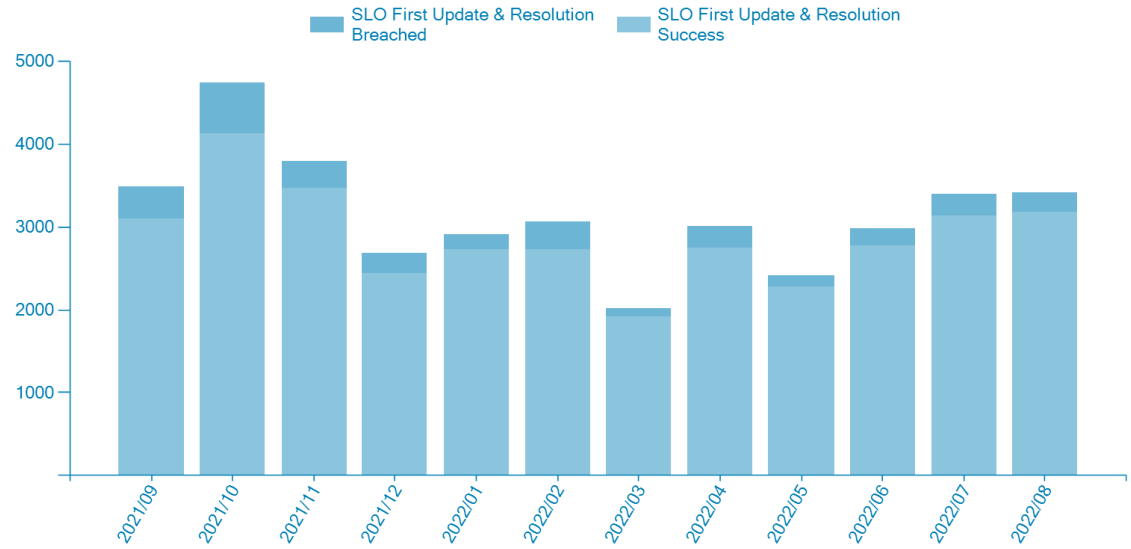
2.2 *SLO trend last 12 months*

The figure below presents the service level objective (SLO) trend in total number of SLO instances and number of breaches during last 12 months.

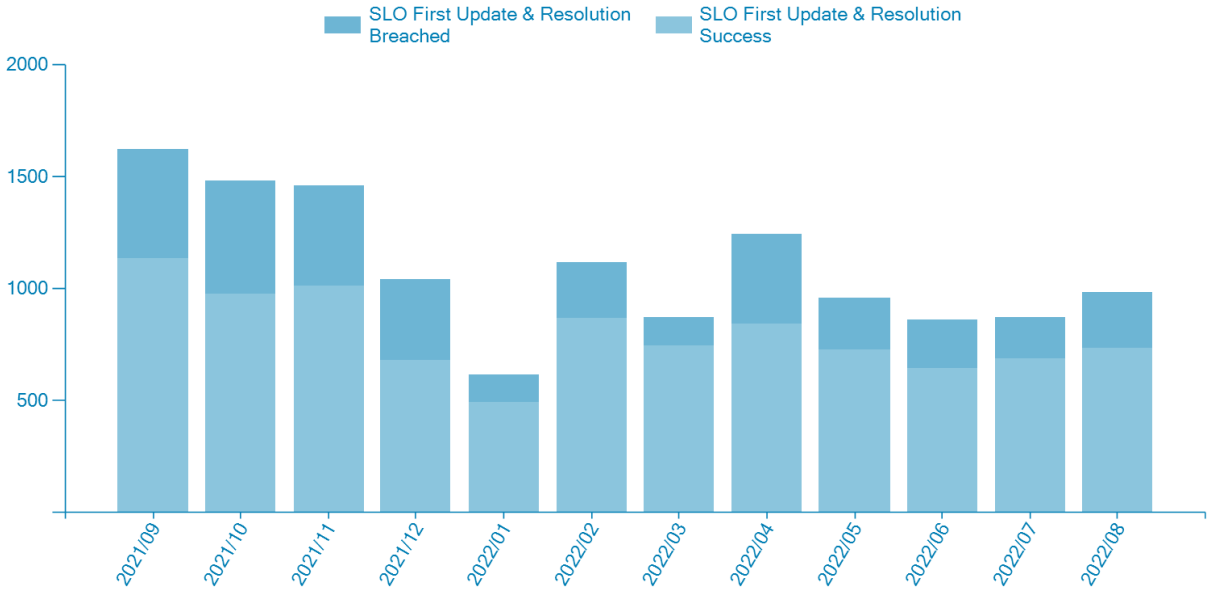
2.2.1 Event Management



2.2.2 Incident Management



2.2.3 Service Request Management



3 Incident Management

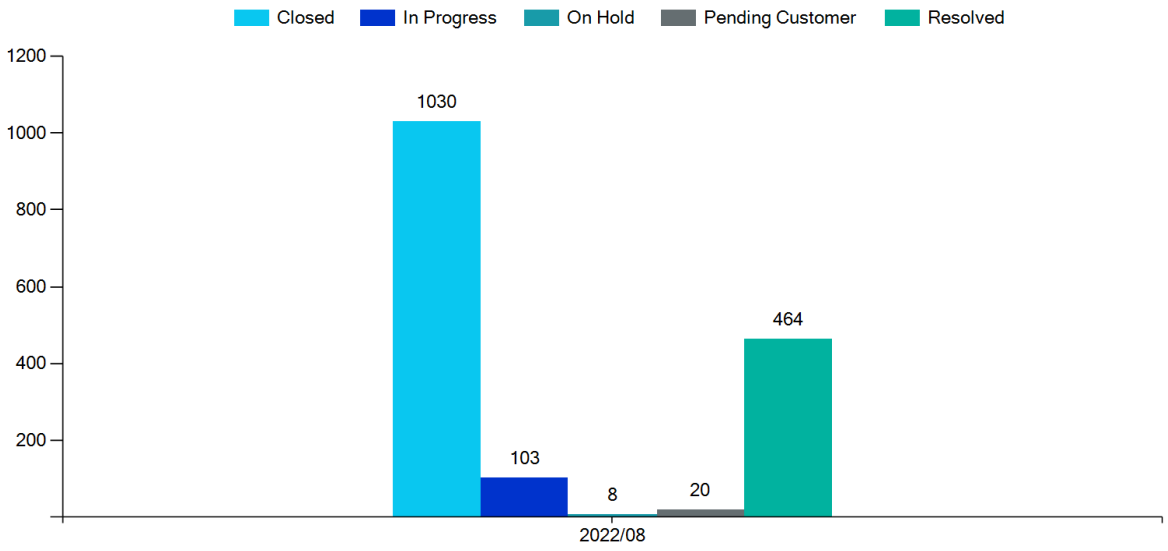
An 'incident' is an unplanned interruption to an IT service or reduction in quality of an IT service, or a failure of a CI that has not yet impacted an IT service. Incident Management restores normal service operation as quickly as possible and minimizes business impact so agreed levels of service are maintained.

The table below introduces the parameters that define the urgency and application of the priorities used to establish the weight and prioritization requirements of incident tickets:

Priority	Definition
P1	Solution Availability immediately impacted and/or detection of a Service Monitor alert. Multiple component failures affecting critical services within an End User Solution or an Incident affecting multiple End User Solutions.
P2	Solution performance degraded or availability likely to be impacted if Incident not resolved. Multiple component failures within an End User Solution not affecting solution availability.
P3	Incident has the possibility to degrade either performance or availability if not resolved
P4	Single component failure with a non-critical threshold, The incident has the possibility to degrade performance if not resolved.

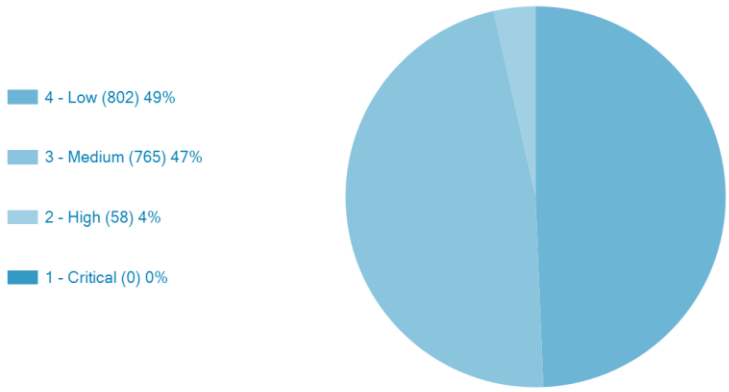
3.1 Created Incidents by state

The graph below presents the number of incidents opened during the reporting period grouped by state at the end of the month.



3.2 *Incidents by priority*

The graph below presents the number of incidents opened during the reporting period grouped by priority.



3.3 *Active Incidents by state*

The table shown here presents the number of incidents active (last day of the month) by state in a table format for the current reporting period only.

State	Count
In Progress	103
On Hold	8
Pending Customer	20
Resolved	464
Total	**595**

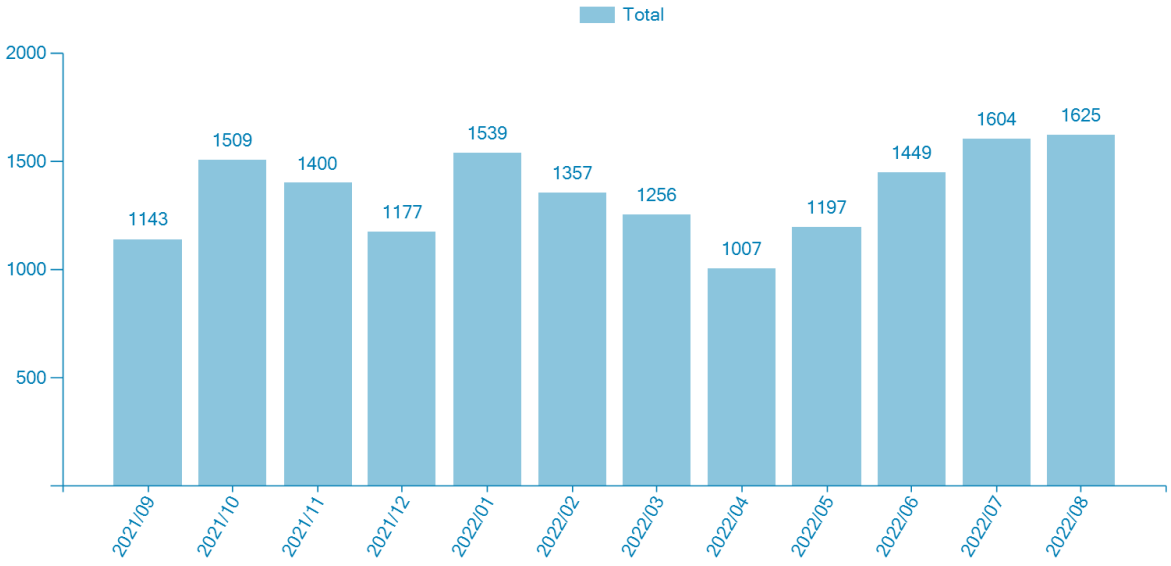
3.4 Incident distribution by top 10 CIs

The table shown here presents the number of incidents per Configuration Item & distribution percentage in table format for the current reporting period only.

Configuration Item Name	Count	Distribution %
DW3PRDGG09	112	16.47
DW3PRDQL04	89	13.09
DW3PRDRK05	88	12.94
DD3TESHD07	81	11.91
STPVVMVC01	75	11.03
DW4PRDRK01	67	9.85
SU3TESRM05	52	7.65
SU3PRODNC08	41	6.03
SU6PRODNC08	38	5.59
SP3PRODBC02	37	5.44
Total	680	100.00

3.5 Incident trend last 12 months

The graph below presents the number of incidents logged during the last 12 months.



4 Service Request Management

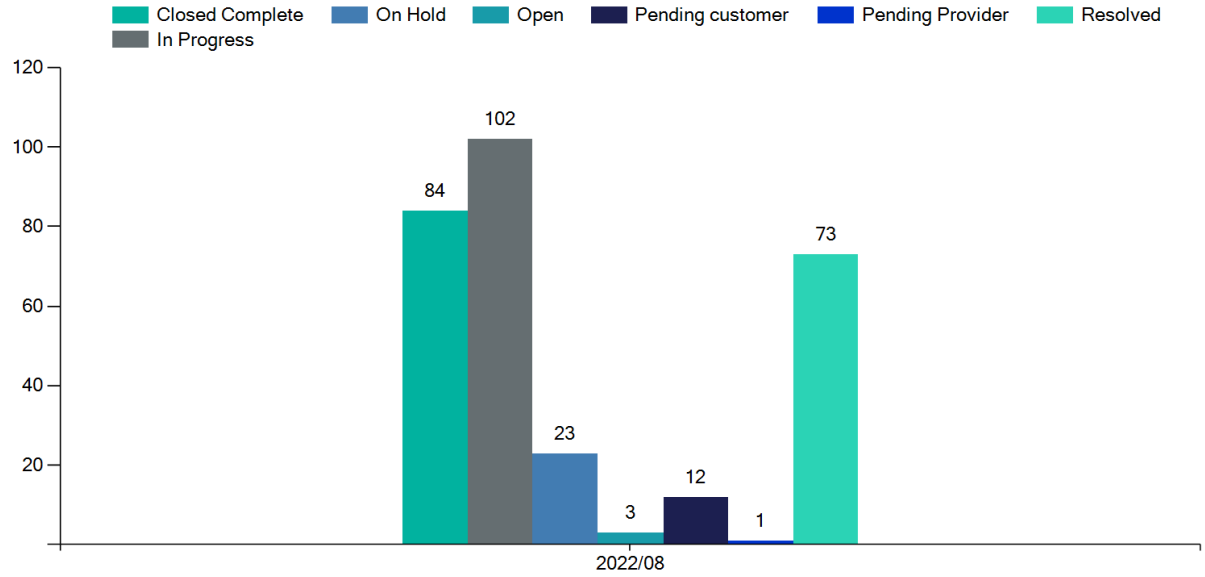
The purpose of the Service Request Management practice is to support the agreed quality of a service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner.

A Service request is a request from a user or a user's authorized representative that initiates a service action which has been agreed as a normal part of service delivery.

Each service request may include one or more of the following items: a request for a service delivery action, a request for information, a request for provision of a resource or service, a request for access to a resource or service, feedback, compliments, and complaints (for example, complaints about a new interface or compliments to a support team).

4.1 Created Service Requests by state

The graph below presents the number of service request opened during the reporting period grouped by state at the end of the month.



4.2 Active Service Requests by state

The table shown here presents active service requests by state in table format for the current reporting period only.

State	Count
In Progress	102
On Hold	23
Open	3
Pending customer	12
Pending Provider	1
Resolved	73
Total	214

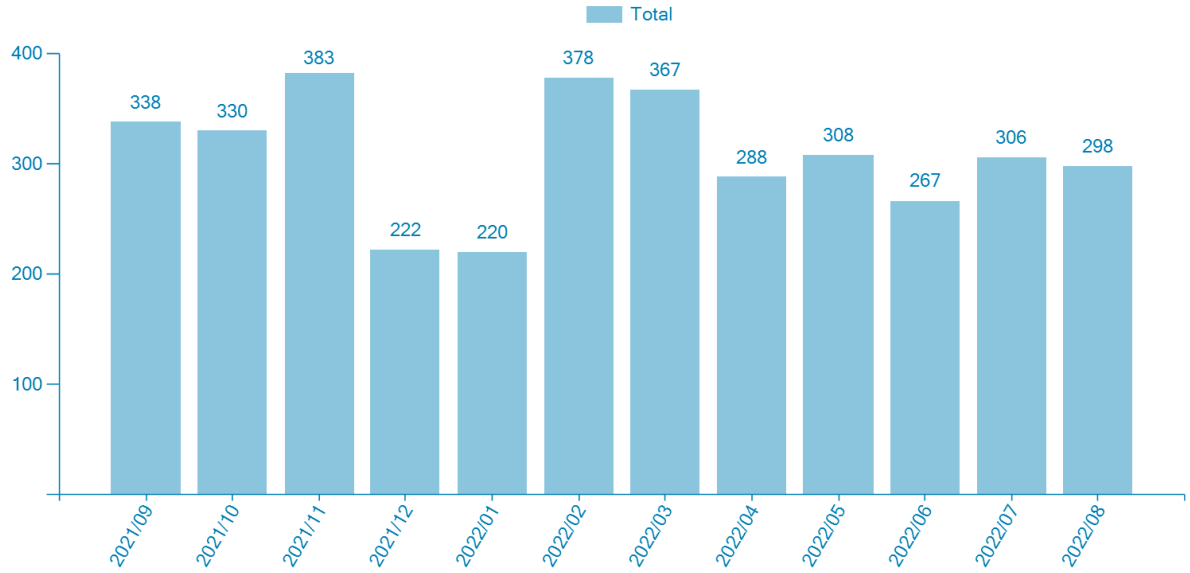
4.3 Service Request distribution by top 10 CIs

The table shown here presents the number of service requests per Configuration Item & distribution percentage in table format for the current reporting period only.

Configuration Item Name	Count	Distribution %
DD3TESHD07	142	59.17
Monitoring Item 1	51	21.25
FILESERVER 1	21	8.75
FILESERVER 2	6	2.50
CC28-WINPRT	4	1.67
RIM-WIN-FW21	4	1.67
WIN-SIM-FW01	3	1.25
GRTFFHDW01	3	1.25
GRTFFHDW02	3	1.25
RSK-WIN-FW03	3	1.25
Total	240	100.00

4.4 *Service Request trend last 12 months*

The graph below presents the number of service requests logged during the last 12 months.



5 Change Management

Change management is a process designed to understand and minimize risks while making IT changes. Businesses have two main expectations of the services provided by IT:

- The services should be stable, reliable, and predictable.
- Any service should be able to change rapidly to meet evolving business requirements.

The Change Management process is designed to help control the life cycle of strategic, tactical, and operational changes to IT services through standardized procedures.

The goal of Change Management is to control risk and minimize disruption to associated IT services and business operations.

The below tables define the type of change request avaliable:

Type	Definition
Standard	A templated Change that has been pre-approved by the client and is repeatable because there is an associated procedure for executing, testing, and rolling back the change.
Normal	A Change that is not a standard change or an emergency change. A Change with no predefined procedure that requires approval.
Emergency	A Change to fix an Incident or restore a service

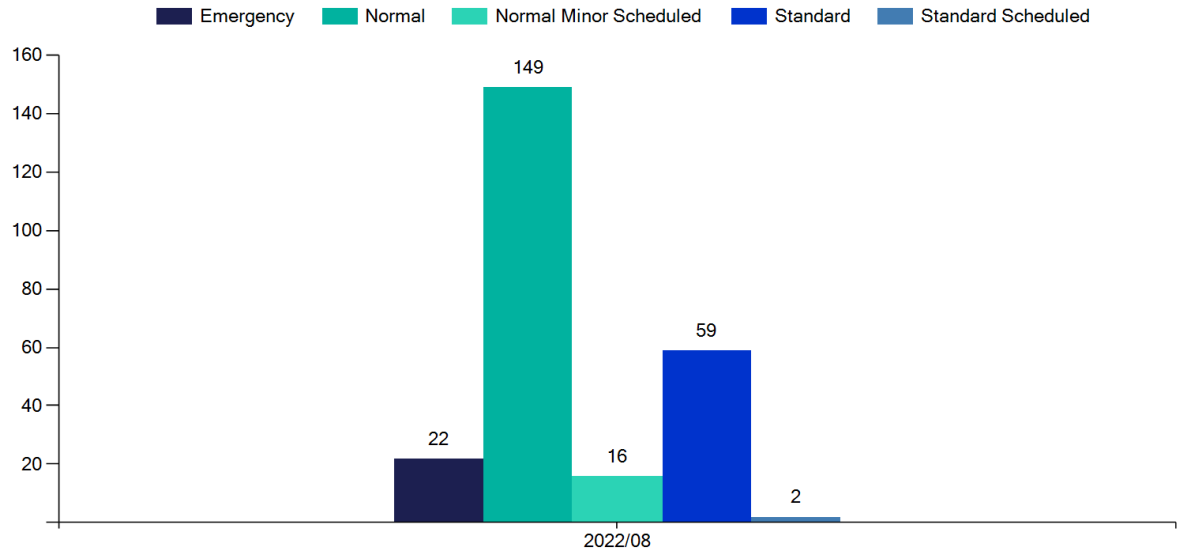
Depending on the Impact and the Risk, a Major or a Minor Change is raised:

All Change Types have the "Scheduled" option for when the intervention has to be performed at a certain time-window.

Impact / Risk	Very High	High	Moderate	Low	None
Total Loss	Major	Major	Minor	Minor	Minor
Degradation	Major	Minor	Minor	Minor	Minor
No impact	Minor	Minor	Minor	Minor	Minor

5.1 Created Change Requests by type

The graph below presents the number of Change Requests opened during the reporting period grouped by change type.



5.2 Change Request volumes by type and successful ratio

The table shown here presents the number of Change Request by change type and successful ratio in table format for the current reporting period only.

Change Type	Count	Distribution %	Success Ratio %
Emergency	22	8.87	100.00
Normal	149	60.08	98.66
Normal Minor Scheduled	16	6.45	78.57
Standard	59	23.79	96.61
Standard Scheduled	2	0.81	100.00

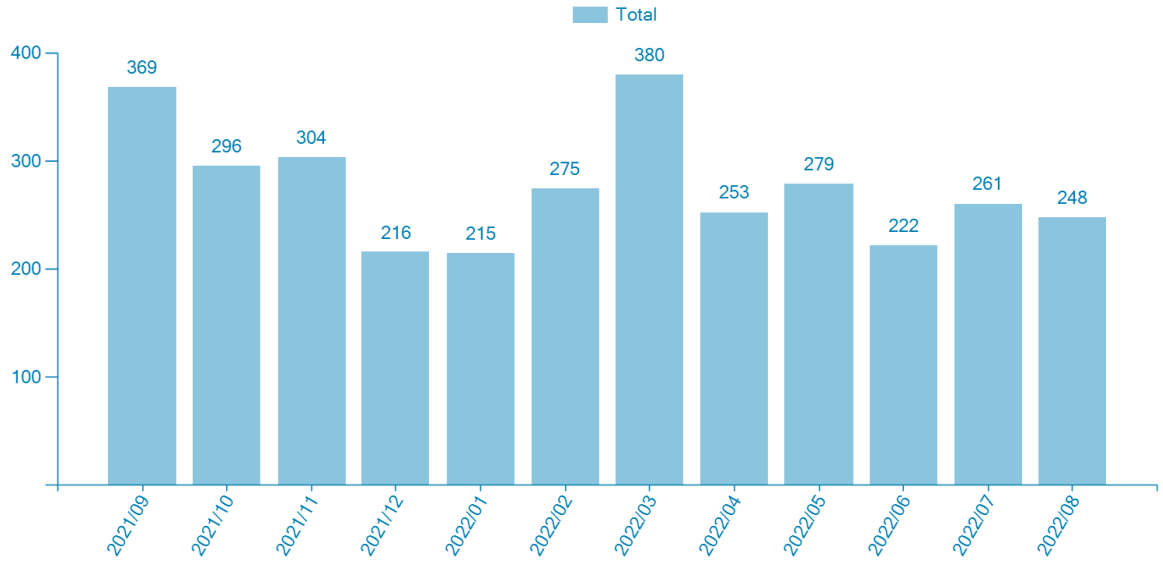
5.3 Change Request types by change outcome

The table shown here presents the number of Change Request by change type and change outcome in table format for the current reporting period only.

Change Type	Authorize	Closed	Implement	Review	Scheduled	Total
Emergency	-	22	-	-	-	**22**
Normal	-	149	-	-	-	**149**
Normal Minor Scheduled	1	13	-	1	1	**16**
Standard	-	59	-	-	-	**59**
Standard Scheduled	-	1	1	-	-	**2**

5.4 Change Request trend last 12 months

The graph below presents the number of change requests logged during the last 12 months.



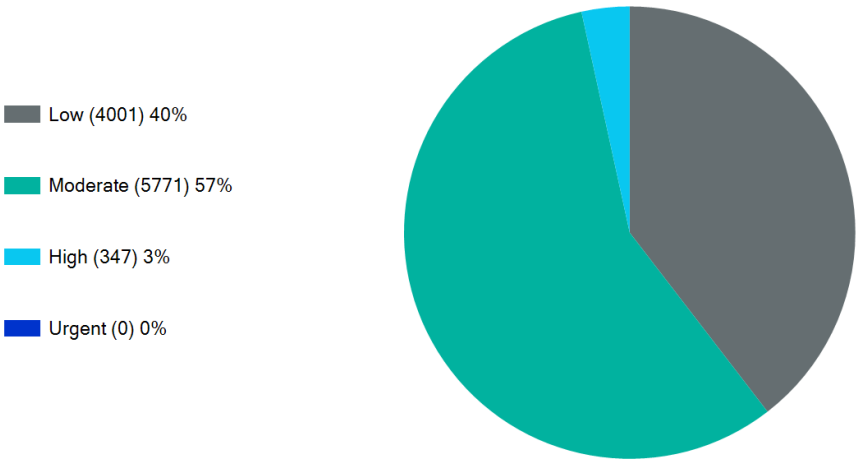
6 Event Management

Process that monitors all events that occur through the IT infrastructure. It allows for normal operation and also detects and escalates exception conditions.

When an event occurs, the monitoring systems send a notification to Service Now. These events will be processed by Service Now and converted into Alerts. Ops Center is responsible for checking the Alert Console and manage the alerts and escalate them to Incidents.

6.1 Alerts by Priority

The graph below presents the alerts percentage by priority during the reporting period only.



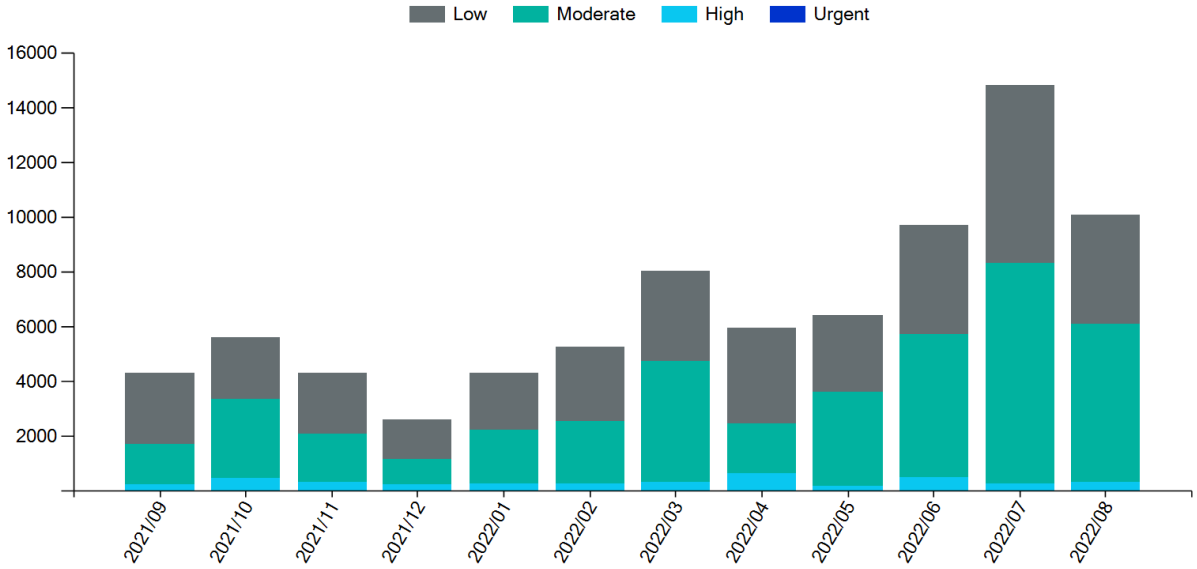
6.2 Top 10 Monitor types by number of alerts

The table shown here presents the top 10 monitor types by number of alerts, categorized by priority, in table format for the current reporting period only.

Monitor Type	Low	Moderate	High	Urgent	Total
Microsoft_SQLServer_Databases	700	2980	-	-	**3680**
Microsoft_SQLServer_AlwaysOnDatabaseReplicas	708	1240	3	-	**1951**
VMware_vSphere_HostPerformance	538	142	-	-	**680**
Ping	77	-	310	-	**387**
Microsoft_SQLServer_Troubleshooter	312	40	1	-	**353**
VMware_vCenter_HostStatus	3	286	2	-	**291**
HTTP-	204	-	-	-	**204**
Windows_Cluster_NodeState	184	14	-	-	**198**
HostStatus	32	124	16	-	**172**
Sec	26	122	-	-	**148**
Total	**2784**	**4948**	**332**	**0**	**8064**

6.3 Event Management trend last 12 months

The graph below presents the number of alerts logged during the last 12 months categorized by priority.



6.4 Top 10 Devices by number of alerts

The table shown here presents top 10 number of alerts per Configuration Item in table format for the current reporting period only.

Device Name	Count
SU6PRODNC08 (SV001217183)	1415
DW3PRDQL04 (SV001217163)	868
DW3PRDRK05 (SV001217165)	753
SU3TESRM05 (SV001583349)	632
SU3TESRM07 (SV001217184)	491
DW3PRDRK14 (SV001217176)	455
SV9PDRDWHSP03 (SV001217185)	453
DW4PRDRK01 (SV001217164)	407
STPVVMVC01 (SV001210478)	356
GRTFFHDW01 (SV001210439)	320
Total	6150

6.5 Top 10 Recurrent alerts

The table shown here presents the top 10 recurrent alerts per device handled in table format for the current reporting period only.

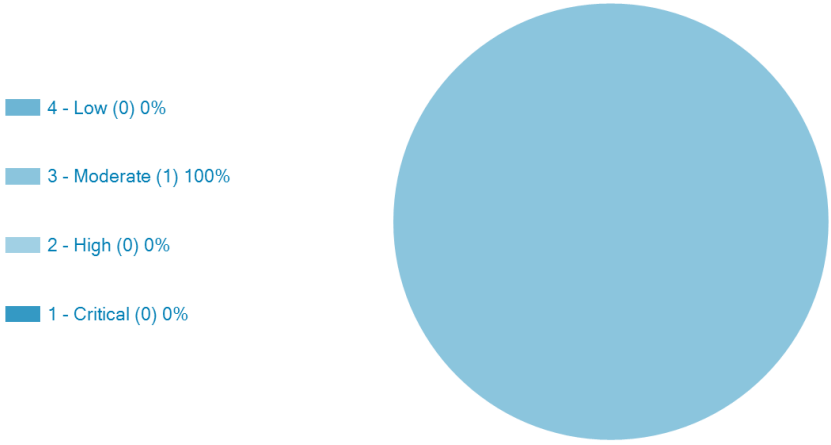
Device Name	Short Description	Count	Last Alert
GRTFFHDW01 (SV001210439)	Monitoring Alert - SV001210439 GRTFFHDW01 exitCode SQL Server Troubleshooter-MSSQLSERVER error: Integrated authentication failed. ClientConnectionId:	311	2022-08-17 06:24:37
STPVVMVC01 (SV001210478)	Monitoring Alert - SV001210478 STPVVMVC01 SystemHealth VMware Host Status-stphvmes07.prod.int.fcityb.co.uk	148	2022-08-31 19:20:16
STPVVMVC01 (SV001210478)	Monitoring Alert - SV001210478 STPVVMVC01 SystemHealth VMware Host Status-stphvmes04.prod.int.fcityb.co.uk	125	2022-08-31 15:04:50
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes06.prod.int.fcityb.co.uk	75	2022-08-31 19:57:16
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes03.prod.int.fcityb.co.uk	70	2022-08-31 14:29:15
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes10.prod.int.fcityb.co.uk	68	2022-08-30 22:35:31
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes11.prod.int.fcityb.co.uk	68	2022-08-31 15:39:21
HMGTVMES09 (MGT0001305)	Monitoring Alert - MGT0001305 HMGTVMES09 InErrors Interfaces-HP FlexFabric 10Gb 2-port 554FLB Adapter	57	2022-08-31 07:26:01
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes01.prod.int.fcityb.co.uk	56	2022-08-31 15:39:16
SU3TESRM05 (SV001583349)	Monitoring Alert - SV001583349 SU3TESRM05 DiskWriteLatency VMware Host Performance-wguhvmes02.prod.int.fcityb.co.uk	53	2022-08-31 14:21:30
Total		**1031**	

7 Problem Management

Problem Management is the set of processes and activities responsible for managing the lifecycle of all problems that could happen in an IT service. The main goal is to prevent problems and their resulting incidents from happening.

7.1 *Problems by priority*

The graph below presents the problems percentage by priority during the reporting period only.



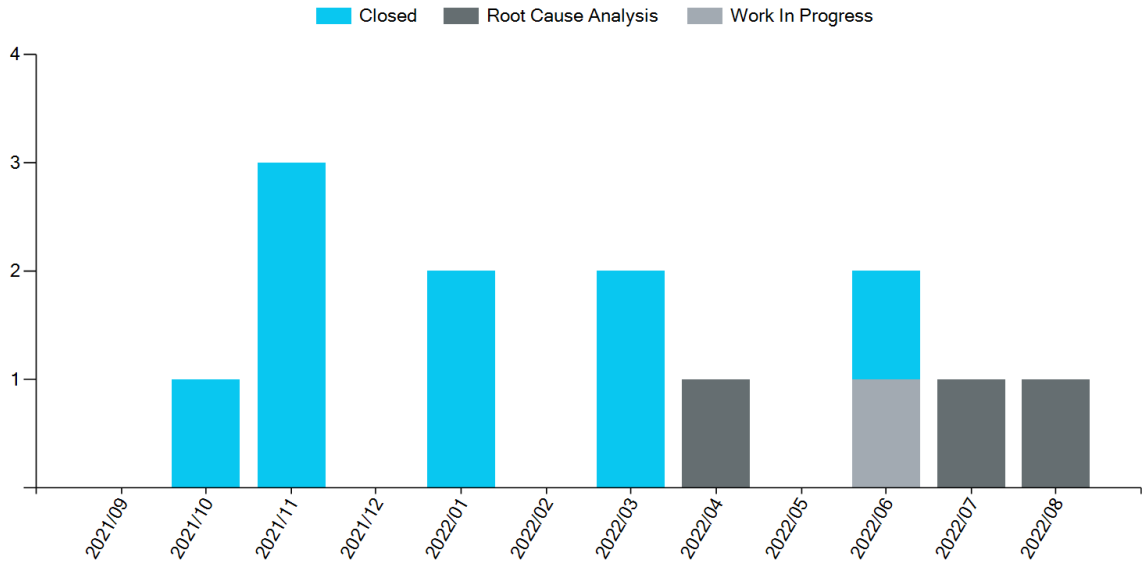
7.2 *Problem Distribution by top 10 CIs*

The table shown here presents the number of problems per Configuration Item & distribution percentage in table format for the current reporting period only.

Configuration Item Name	Count	Distribution %
DW4PRDRK01	1	100.00

7.3 Problem Management trend last 12 months

The graph below presents the number of problems logged during the last 12 months categorized by state.



7.4 Current Open Problems

The table shown here presents open problems registered in table format.

Problem Id	Short Description	Status	Created
P-0060361	Licensing registration for secondary node	Root Cause Analysis	2021-05-19 14:42:59
P-0060326	Wildcard on Firewall	Root Cause Analysis	2021-05-19 15:09:15
P-0061388	Repetitive Alert Status Jobs	Root Cause Analysis	2022-04-26 10:59:34
P-0061543	Repetitive Alerts - Ping	Work In Progress	2022-06-09 10:37:00
P-0061399	Errors and warnings	Root Cause Analysis	2022-07-05 12:39:22
P-0063817	FailOver to DW4PRDRK01	Root Cause Analysis	2022-08-25 14:52:48

8 Risk Management

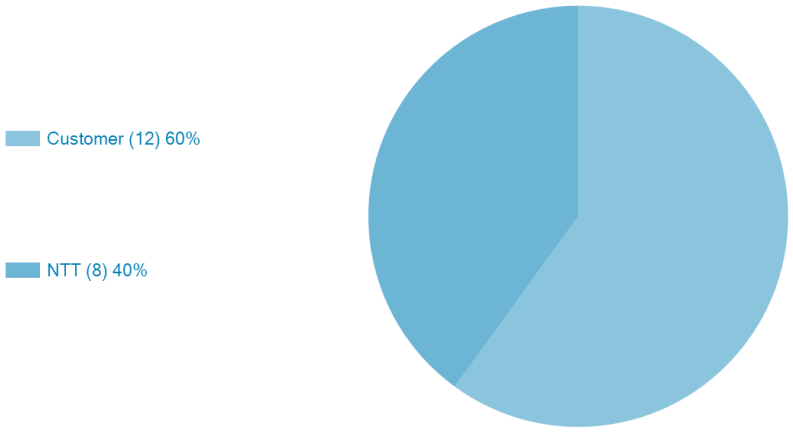
The main objectives of risk management process are to identify, assess, and control risks that have been identified using a risk matrix. This may involve analysing business assets, threats to those assets, monitoring threat parameters, and evaluating the business's vulnerability to those threats.

The table shown here defines the risk value definition:

Probability Level	Risk Matrix				
Very High	5	10	15	20	25
High	4	8	12	16	20
Medium	3	6	9	12	15
Low	2	4	6	8	10
Very Low	1	2	3	4	5
Impact Level	Very Low	Low	Medium	High	Very High

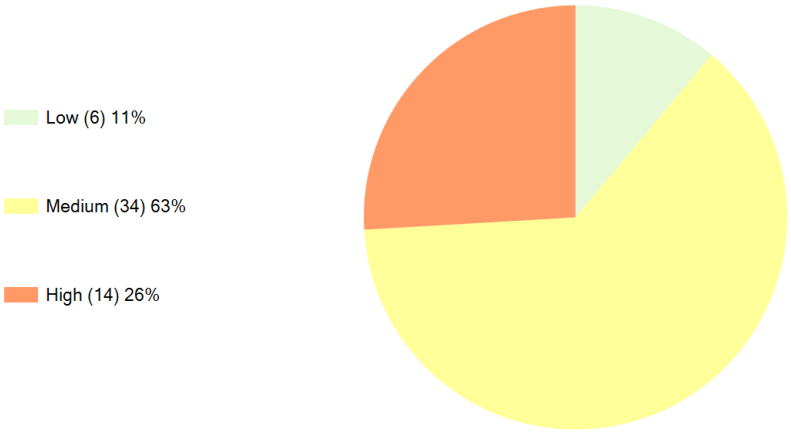
8.1 Risks in Progress by owner

The graph below presents the risks in progress percentage by owner.



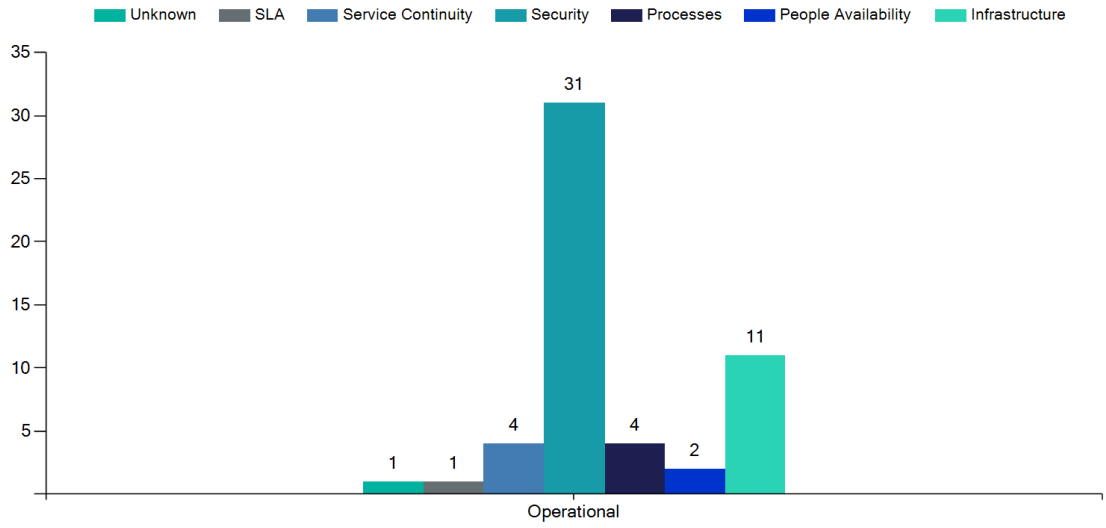
8.2 Active Risks by risk value

The graph below presents the risks percentage by risk value.



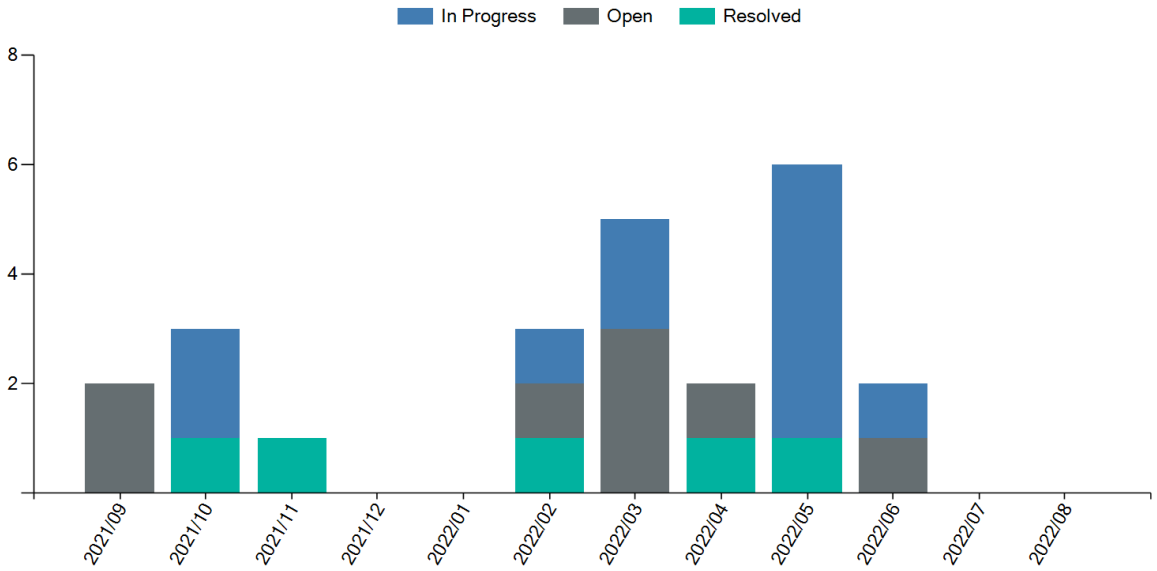
8.3 Active Risks by category

The graph below presents currently active risks by category and sub-category.



8.4 Risk Management trend by state last 12 months

The graph below presents the Risk Management trend by state during the last 12 months.



8.5 Top 10 Current Active Risks

The table shown here presents the top ten active risks registered in table format.

Risk Id	Short Description	Status	Created
R-0001729	Data encryption	Resolved	2019-07-04 00:00:00
R-0001731	CA certificates	Open	2020-01-15 00:00:00
R-0001733	Cloud Credentials	Open	2020-01-15 00:00:00
R-0001737	VM and ESXI Software - RIM	Open	2020-02-06 00:00:00
R-0001743	Devices with EOL	Open	2020-02-27 00:00:00
R-0001747	Policy breach	Resolved	2020-08-03 00:00:00
R-0002047	Vulnerabilities	Open	2021-02-05 13:45:25
R-0002503	Antivirus Software EOL	In Progress	2021-04-07 08:15:42
R-0002959	Azure administrator accounts	Open	2021-05-27 08:35:21
R-0002961	Using a browser that can have vulnerabilities	Open	2021-05-27 08:41:32