

National Cyber Security Authority (NCA) Compliance using

February 2024

drut.

Robotics GRC

speed on the wire



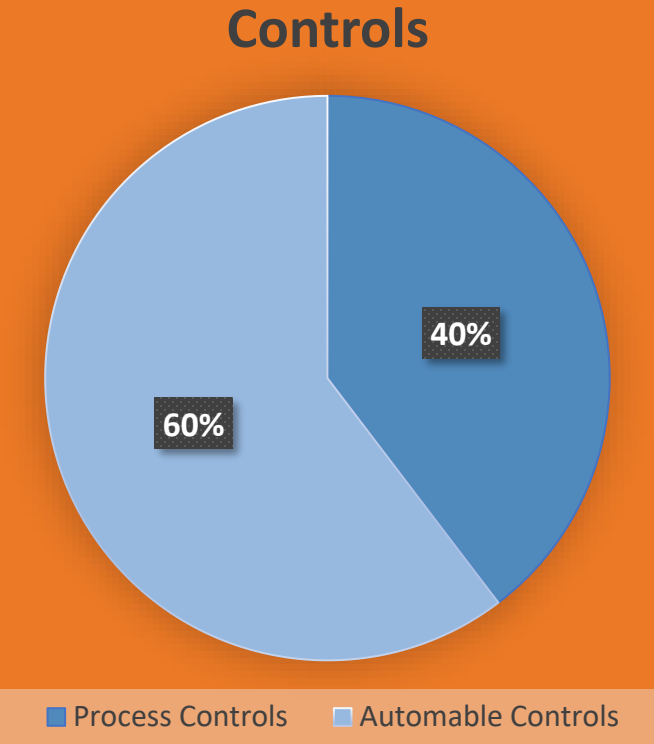
drut.



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

- The National Cybersecurity Authority (NCA) in Saudi Arabia established in 2017.
- Governmental agency responsible for enhancing and implementing cybersecurity measures to protect information systems and infrastructure
- Primary objective is to create a cyberspace that is robust, secure, and reliable, fostering growth and prosperity with trust
- The six main themes of this framework are as follows:
 - a. UNIFY - emphasizes the seamless integration of all components within the realm of cybersecurity regulation.
 - b. MANAGE -revolves around identifying critical infrastructures and managing cyber risks.
 - c. ASSURE –revolves around assuring the protection of cyberspace.
 - d. DEFEND - revolves around developing the national cyber defense mechanisms to protect against risks and threats.
 - e. PARTNER - revolves around setting up the appropriate mechanisms for building partnerships and sharing information.

SN	Domain	Total Controls	Process Controls	Automable Controls	Integrated in Drut
1	Cyber Governance	36	21	15	~50%
2	Cyber Defense	62	15	47	
3	Cyber Security Resilience	4	3	1	
4	Third Party and Cloud Computing	8	4	4	
5	Industrial Control Systems Cybersecurity	4	1	3	
	Total	114	44 (40%)	67 (60%)	



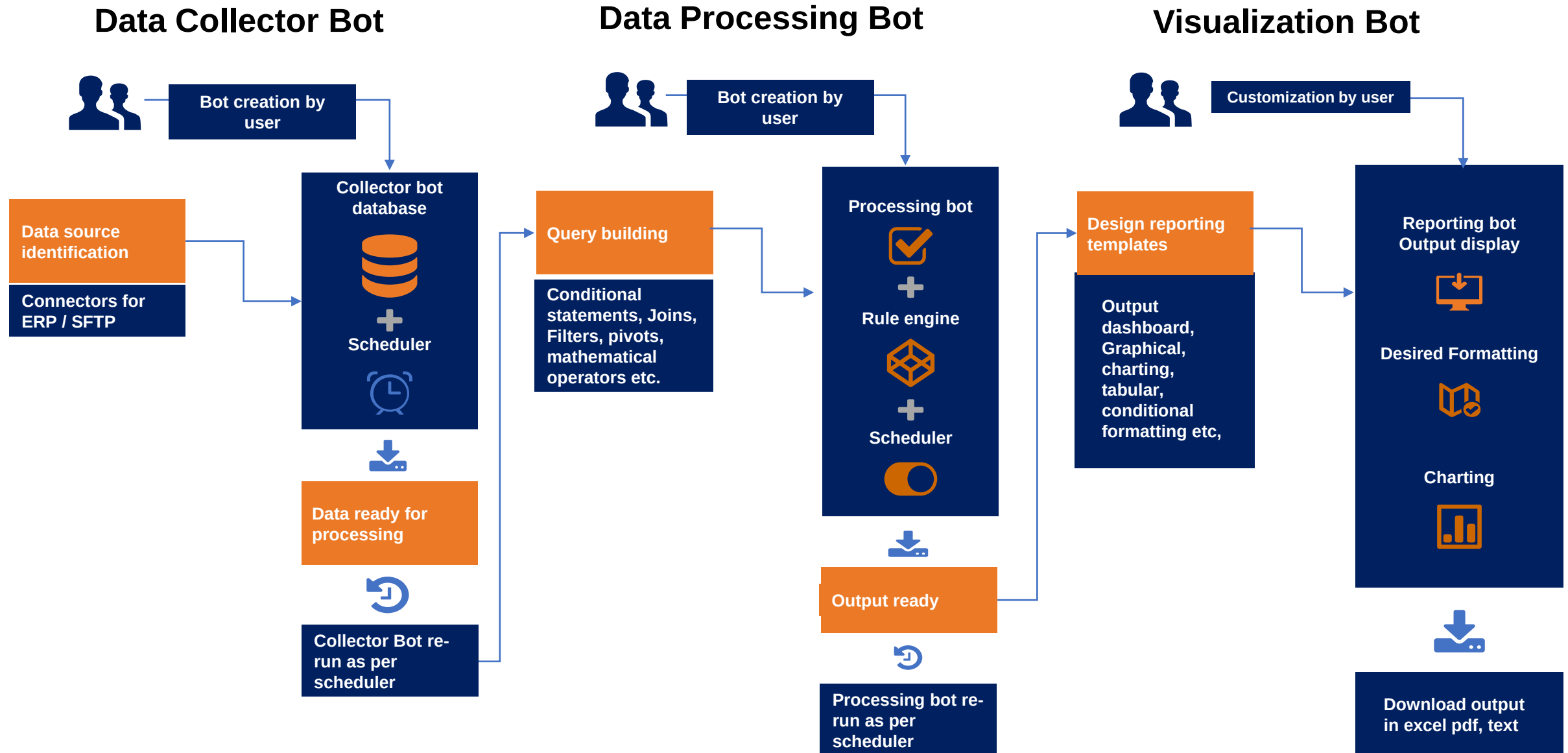
1. Cyber Governance

SN	Sub Domain	Total Controls	Process Controls	Automable Controls
1	Cybersecurity Strategy	3	3	0
2	Cybersecurity Management	3	2	1
3	Cybersecurity Policies and Procedures	4	3	1
4	Cybersecurity Roles and Responsibilities	2	2	0
5	Cybersecurity Risk Management	4	2	2
6	Cybersecurity in Information and Technology Project Management	4	2	2
7	Compliance with Cybersecurity Standards, Laws and Regulations	2	2	0
8	Periodical Cybersecurity Review and Audit	3	2	1
9	Cybersecurity in Human Resources	6	2	4
10	Cybersecurity Awareness and Training Program	5	1	4
	Total	36	21 (60%)	15 (40%)

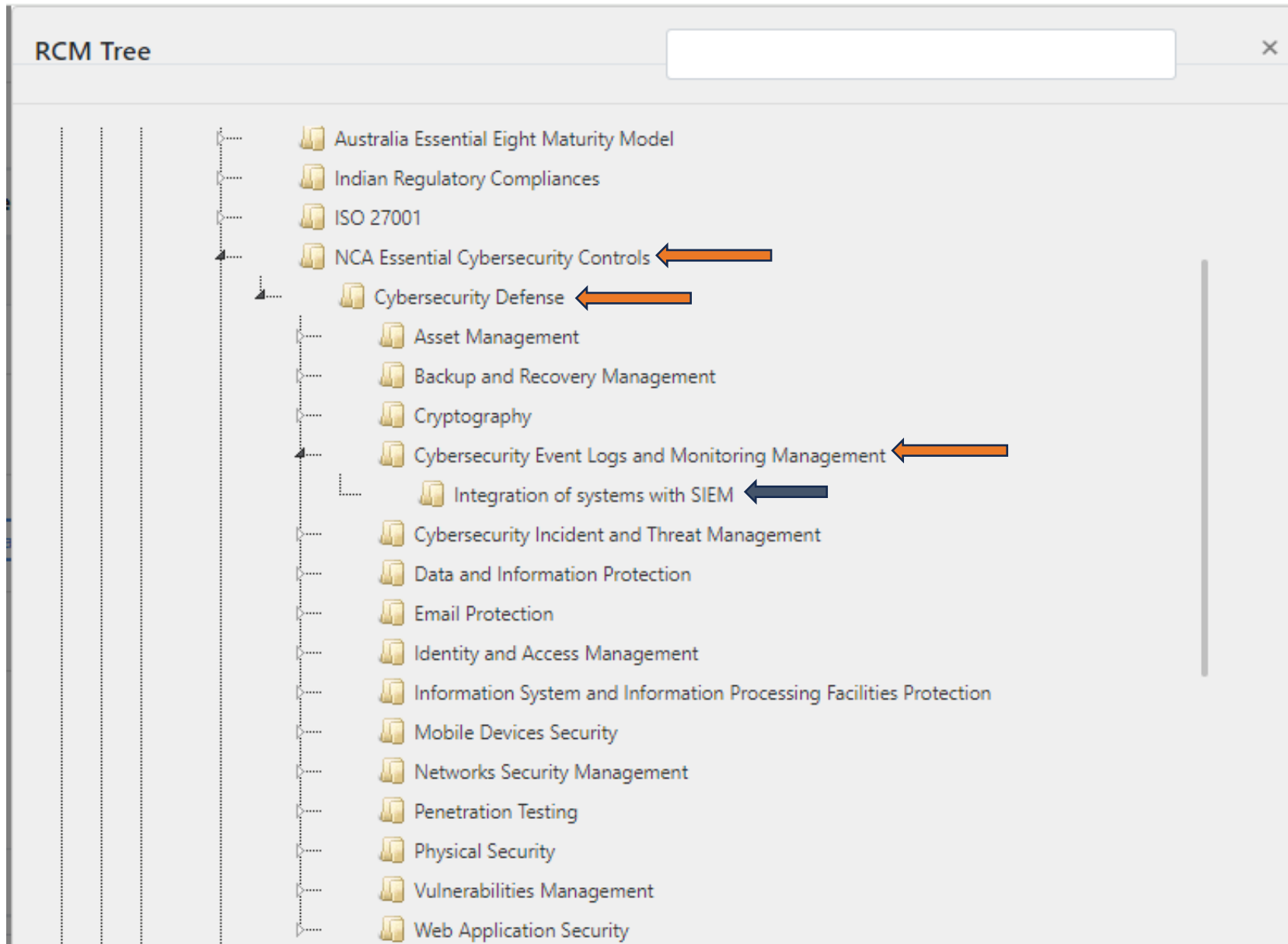
2. Cyber Defense

SN	Sub Domain	Total Controls	Process Controls	Automable Controls	Drut. works with *indicative list
1	Asset Management	6	2	4	Symphony AI
2	Backup and Recovery Management	4	0	4	emc networker
3	Cryptography	4	1	3	Bitlocker
4	Cybersecurity Event Logs and Monitoring Management	4	1	3	Qradar
5	Cybersecurity Incident and Threat Management	4	1	3	BMC Remedy
6	Data and Information Protection	4	1	3	Symantec DLP
7	Email Protection	4	1	3	O365
8	Identity and Access Management	4	1	3	Active Directory, Arcos
9	Information System and Information Processing Facilities Protection	4	1	3	Microsoft Defender and Ivanti
10	Mobile Devices Security	4	1	3	Microsoft Itune
11	Networks Security Management	4	1	3	Cisco, Sentinel One
12	Penetration Testing	4	1	3	Nessus, QualysGuard, Netsparker
13	Physical Security	4	1	3	Matrix
14	Vulnerabilities Management	4	1	3	Nessus
15	Web Application Security	4	1	3	Salesforce
	Total	62	15 (25%)	47 (75%)	

how drut will help in NCA Compliance?



Find your control in drut.'s RCM – Risk Control Matrix



Integration of Systems with SIEM– 1. run the bot



ANB / ANB Group / Compliance Standards / Compliance / NCA Essential Cybersecurity Controls / Cybersecurity Defense / Cybersecurity Event Logs and Monitoring Management / Integration of systems with SIEM

Show 10 entries

Search:

RCM Tree

↑↓	Sub Process ↑↓	Activity ↑↓	Risk ↑↓	Severity ↑↓	Control ↑↓	Automatable ↑↓	CheckPoint ↑↓	Update ↑↓	Robo ↑↓
⊖	Integration of systems with SIEM	The cybersecurity requirements for event logs and monitoring management must include activation of cybersecurity event logs on critical information assets	Analysis and correlation of logs may not be done which might result in security incidents not being reported	Medium	Ensure that systems are integrated with SIEM	Yes	Verify systems which are not integrated with SIEM as compared to the inventory	Edit Activity Edit Risk	Add Collector Add Analysis

Bot Name	Condition Name	Bot Type	Bot For	Schedule Type	Last Run Time	Next Run Time	Bot Status	Results	Edit	Delete
NCA SIEM Integration	Ensure that systems are integrated with SIEM	Analysis	Database	RunOnce	12/01/2023 14:46:44 PM	12/01/2023 14:37:00 PM	Finished	View Exceptions View ReportBI Add Risk Parameter Add Summary	Edit	
NCA SIEM Integration		Collector	Excel	RunOnce	12/01/2023 13:36:12 PM	12/01/2023 13:27:00 PM	Finished		Edit	

2. find the exceptions

drut.



View Report

Activity : The cybersecurity requirements for event logs and monitoring management must include activation of cybersecurity event logs on critical information assets

Annexure : List of systems which are not integrated with SIEM as compared to the inventory

Base Data
Total Number of Rows in Base Data

695

Exceptions
Number of Exceptions in Report

165

Deviation
Deviation between Total Rows and Exceptions

23%

As On Date 01-12-2023

Summary

Preview Result

Cards & Charts

Pivot Result

Base Files

Columns:

Hide

Sorting:

Off

View Data:

Lazy Loading

Search:

Caption	IP_Address	Type	Application	MachineType
Search Caption	Search IP_Address	Search Type	Search Application	Search MachineType
vepabx.anb.com	10.0.5.131	prod	epabx server	Windows 10 Pro
10.0.5.142	10.0.5.142	prod	netapp unified manager	Virtual Linux Appliance
vjmailsrv2.anb.com	10.0.5.143	prod	jmail server	Windows 10 Pro

Search For

Switch to ReportBI ☒

406080100

20

0

23% Low Risk



3. view your dashboard

drut.

drut.

NON INTEGRATION OF SYSTEMS WITH SIEM

Bot Run Date 12/01/2023 2:46:44 PM

Dashboard Ensure that systems are integr...

As On To 01-12-2023 Download

Total Systems

Total systems 695

Assessment Based On Operating System

Centos	29.02 %
Windows 2016 Server	41.49 %
Windows 10 Pro	85.23 %

Weighted Risk Parameter

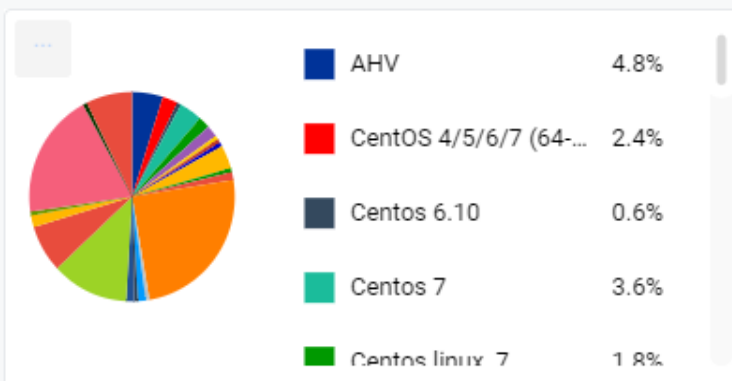
Centos	9.87 %
Windows 2016 Server	13.69 %
Windows 10 Pro	28.13 %

Risk Meter

Total 51.69% High

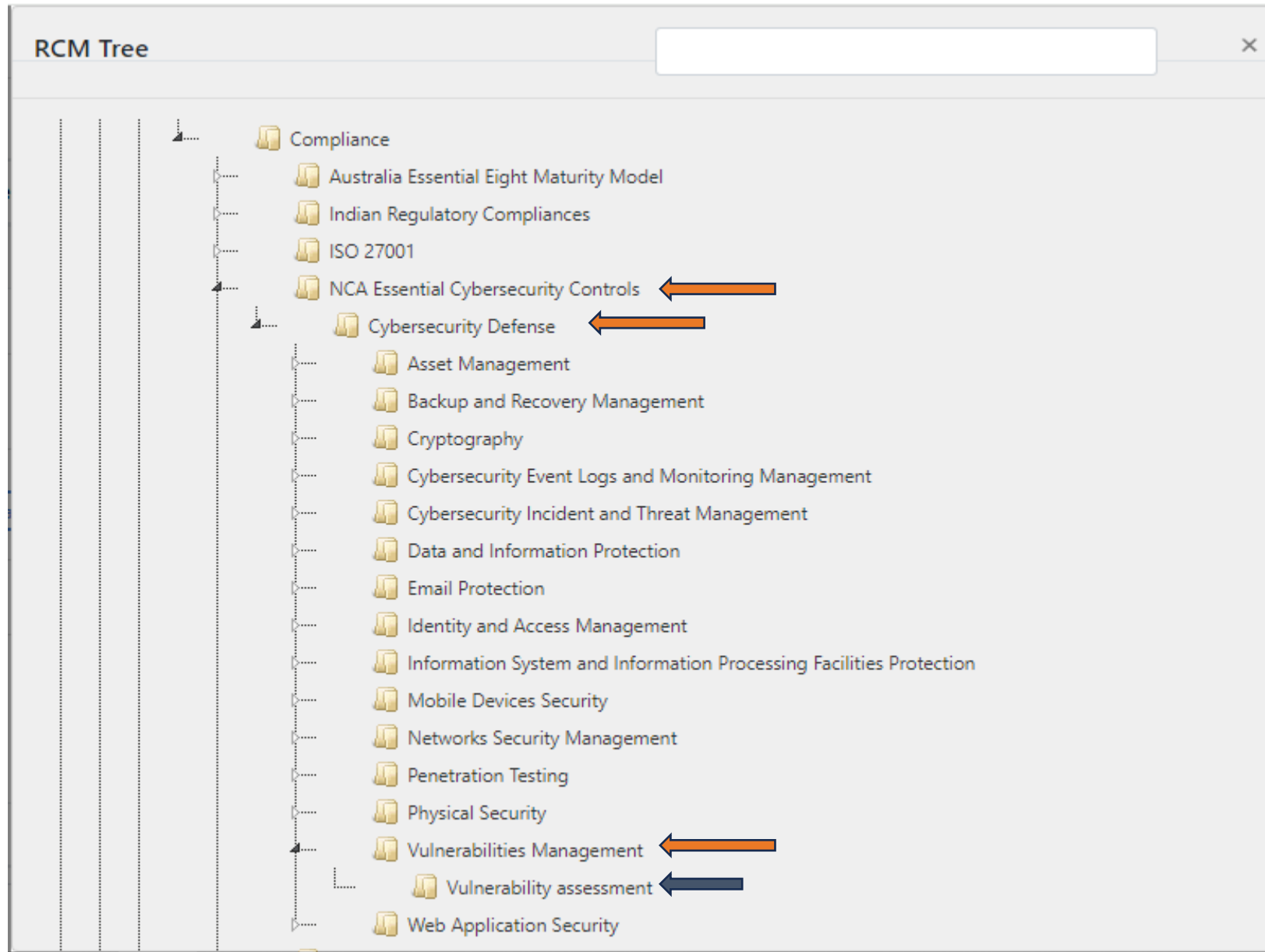


Machine Type Wise Exceptions



+

Another sample from drut's RCM – Risk Control Matrix



Vulnerability Assessment - 1.run the bot

drut.

drut.

ANB / ANB Group / Compliance Standards / Compliance / NCA Essential Cybersecurity Controls / Cybersecurity Defense / Vulnerabilities Management / Vulnerability assessment

Show 10 entries

Search:

RCM Tree

↑↓	Sub Process ↑↓	Activity ↑↓	Risk ↑↓	Severity ↑↓	Control ↑↓	Automatable ↑↓	CheckPoint ↑↓	Update ↑↓	Robo ↑↓
	Vulnerability assessment	The cybersecurity requirements for technical vulnerabilities management must include vulnerabilities remediation based on classification and associated risk levels	Known vulnerabilities may not be identified and addressed which may lead to exploitation of such vulnerabilities to launch attacks	Medium	Ensure low risk vulnerabilities are fixed within 90 days medium risk vulnerabilities fixed within 60 days critical risk vulnerabilities fixed within 7 days	Yes	Verify vulnerabilities not closed as per the severity levels wise timelines	Edit Activity Edit Risk	Add Collector Add Analysis

Bot Name	Condition Name	Bot Type	Bot For	Schedule Type	Last Run Time	Next Run Time	Bot Status	Results	Edit	Delete
NCA VA		Collector	Excel	RunOnce	12/01/2023 17:46:12 PM	12/01/2023 17:36:00 PM	Finished		Edit	
NCA Vulnerabilities closure	Verify vulnerabilities not closed as per the severity levels wise timelines	Analysis	Database	RunOnce	12/07/2023 16:58:19 PM	12/07/2023 16:45:00 PM	Finished	View Exceptions View ReportBI Add Risk Parameter Add Summary	Edit	

2. find the exceptions

drut.

View Report

Search For

Switch to ReportBI ☐

Activity : The cybersecurity requirements for technical vulnerabilities management must include vulnerabilities remediation based on classification and associated risk levels

Annexure : List of vulnerabilities not closed as per the severity levels wise timelines

Base Data 47
Total Number of Rows in Base Data

Exceptions 19
Number of Exceptions in Report

Deviation 40%
Deviation between Total Rows and Exceptions

As On Date 07-12-2023

Summary

Preview Result

Cards & Charts

Pivot Result

Base Files

Columns:

Sorting:

View Data:

Search:

Host	Risk	Type	Scan_date	Status	Date_of_closure	Timelag
Search Host	Search Risk	Search Type	Search Scan_date	Search Status	Search Date_of_closure	Search Timelag
202.123.2.6	Medium	TCP/IP TIMESTAMPS SUPPORTED	2022-12-25 00:00:00	Closed	2023-03-10 00:00:00	75
202.123.2.6	Medium	NESSUS SCAN INFORMATION	2022-12-25 00:00:00	Closed	2023-03-10 00:00:00	75
202.123.2.6	Medium	DEVICE TYPE	2022-12-25 00:00:00	Closed	2023-03-10 00:00:00	75

3. view your dashboard

drut.

Home

Reports

Dashboards

+

drutgateway.anbglobal.com:2019/ui/init/#/dashboard?dashboardName=VERIFY%20VULNERABILITIES%20NOT%20CLOSED%20AS%20PER%20THE%20SEVERITY%20LEV...

All Bookmarks

VERIFY VULNERABILITIES NOT CLOSED AS PER THE SEVERITY LEVELS WISE TIMELINES

Bot Run Date 12/07/2023 4:58:19 PM

As On To 07-12-2023 Download

Total Vulnerabilities Found

Total Vulnerabilities 47

Total Number Of Exceptions

Vulnerabilities open < 90 days 17.02 %

Vulnerabilities open < 60 days 29.79 %

Risk Parameter

Vulnerabilities open < 90 days 10.21 %

Vulnerabilities open < 60 days 11.91 %

Overall Risk

Total 22.12% Low

Low 0.00-30.00

Medium 30.01-60.00

High 60.01-100.00

Risk Based Assessment

Critical 63.2%

Medium 36.8%

Status Based Assessment

Closed

Open

Status

Vulnerabilities

Some more NCA ECC Controls we can help with

Domain	Activity	Risk Name	Control	Checkpoint in drut
1. Cyber Governance	Review of Cybersecurity policies and procedures	Leads to arbitrary process in absence of approved documented policy and process	Cyber related policy document are approved by Board	Review version control, approval and frequency for reviewing the Policy and procedure/process document
1. Cyber Governance	User Access Review	If users are not reviewed periodically unrequired users may be present which may lead to unauthorized access to data and systems	Ensure that privileged user access review is carried out periodically	Check if user access review is carried out periodically during the year
2. Cyber Defense	Backup Restoration	If backup is not tested one cannot ensure that data can be retrieved in the event of disaster	Ensure that backup of critical system is resorted on a periodic basis	Verify critical systems for which backup is not restored periodically
2. Cyber Defense	Incident Resolution	Untimely closure of incidents may affect systems availability leaving the systems exposed to potential exploitation by unauthorized users and damage of reputation	Ensure that incidents are closed within the agreed timelines	Verify incidents that are not closed within 6 weeks

Some more NCA ECC Controls we can help with

Domain	Activity	Risk Name	Control	Checkpoint in drut
3. Cyber Security Resilience	Review of BCP Policies and Procedures	Review of BCP Policies and Procedures	Review of BCP Policies and Procedures	Review of BCP Policies and Procedures
4. Third Party and Cloud Computing	Third Party Risk Assessment	Risks associated with vendors might not be evaluated resulting in principles of confidentiality availability and integrity being affected	Ensure that vendor risk assessments is conducted for all critical vendors	Identify critical vendors whose risk assessment is not carried out
5. Industrial Control Systems Cybersecurity	Patching of Systems	In absence of patching identified vulnerabilities might be exploited by threats and security flaws would continue to exist	Ensure that systems scheduled for patching are be patched successfully	Verify that systems scheduled for patching are patched successfully
5. Industrial Control Systems Cybersecurity	Installation of Malware Solution	Absence of malware solution may expose the systems to malware and ransomware attacks	Ensure that malware software is installed on all systems	Check that malware solution is installed and running on all desktops, laptops and servers.

Connect with Us

drut.

speed on the wire

Nirma Varma

Director – Technology and Risk

nirma.varma@drut.com

Nirmiti Chutke

Go to Market - Manager

nirmiti.chutke@drut.com



Follow us on
www.drut.com
[@drut.bot](#)