Business Continuity & Disaster Recovery

(Chapter - 3 : DISSA Course)

Arijit Chakraborty

June 13 , 2021

NATIONAL STOCK EXCHANGE OF INDIA LIMITED

Continuity Planning(BCP)/Disaster Recovery (DR)

1. *Securities Market heavily dependent on IT infrastructure.*
2. *Break down of IT infrastructure could occur from major disasters such as **Earthquakes, floods, fires, riots or war etc.,** which could lead to interruptions to business functions.*
3. *In the past, there have been a couple of occurrences of such disasters in India due to which it is very essential that the **Trading Members should establish a well defined Business Continuity/DR plan.***

- *Given the current technology intensive environment in which Indian Securities market operates, in **order to ensure stability in operations of Members** so that interest of investors and market at large is not adversely impacted, **members are advised to sufficiently review all potential risks along with its impact on the business and put in place BCP/DR plan.***
- *Members who have established BCP/DR plan may please **submit the details of their plan to Exchange** in the format enclosed at Annexure I.*
- *Members **who intend to establish BCP/DR needing any guidance** on establishing such BCP/DR plan may please get in touch with _____*

RECOVERY CAPABILITY FOR VARIOUS DISASTER SCENARIOS

- ***Level 1:.Minor Outage Scenario***
- *In the event of a **minor outage**, business processes may experience **minor damage / outage and will run at a sub-standard level.** Scenarios include :*

✓ *link connectivity being temporarily down,*

✓ *switch or router port failures,*

✓ *System or network CPU failures, System Fan failures,*

✓ *System or Network Power supply failures,*

- ***Level 2: Moderate Outage Scenario***
- *In this scenario, some or all business processes at the location **may experience moderate damage / outage.** Processes may not continue **or may run at a degraded level.** An alternate site **may not be required** for continuing business **but alternate equipment may be required** depending on the criticality of the business process*
- *Some of the examples of such scenarios can be:-*

✓ *Equipment is damaged due to Power surge.*

✓ *ISDN/VSAT/Circuit router failure*

✓ *Core access layer switch failure*

✓ *Access/Distribution switch failure.*

✓ *LAN switch or router failure. / Temporary outage of power.*

- ***Level 3: Disaster Scenario Risks***

✓ *Member infrastructure **may experience a severe disaster resulting in the total shut down of infrastructure of the Member.***

✓ *Full processing capability of all business processes like **Trading, Risk Management, settlement systems etc. from that location** and related infrastructure may be down.*

✓ *Key personnel **may not be able to access** the premises.*

✓ *There may also be non-availability of key resources in the building.*

- ***Some of the examples of such scenarios** can be*
- *1. **Flood / Rain/Fire** making office premises like building and Datacenters inaccessible.*
- *2. **Riots /war etc., at a location near one of the offices** or within the premises of the member may render the office premises inaccessible.*
- *3. **Complete power shutdown** due to unavailability of generators.*
- ***Members may have to switch their business over to the BCP site**.*
- *Key factors for RTO - **key personnel availability, resilient IT infrastructure and robust BCP processes***

- ***Level 4: Catastrophe***
- *In this scenario,* ***major disaster strikes which would result in a major disruption of services****.*
- ***Full processing capability cannot be achieved*** *for a substantial period of time.*
- *Recovery will require use of* ***alternate processing site as well as offsite offices for employees over an extended period of time***

Some of the examples of such scenarios can be

- *1. War*
- *2. Earthquake*
- *3. Extended Communal Riots etc*
- *In such a scenario,* ***capability to achieve their RTO*** *would critically depend upon :*
- ***Key personnel availability, resilient IT infrastructure and robust BCP processes.***

NSE

Press Release

National Stock Exchange Of India Limited

NSE successfully completes live trading from its Disaster Recovery (DR) site

Mumbai, March 05, 2020: National Stock Exchange of India Ltd (NSE) has successfully completed live trading and other operations from its Disaster Recovery (DR) site, on Monday 2nd March and Tue 3rd March 2020. The entire technology and business operations were executed from the DR site which is located in another city and is a replica of the main production site in Mumbai. The live trading was to simulate a level 4 city wide disaster, in which the main site would not be available. The exercise was done in a smooth manner and has successfully demonstrated the robustness of its DR capabilities. The entire activity was done without affecting the market participants including members, clearing banks and depositories. The successful live operations at a time when the markets were quite volatile, has demonstrated strength of NSE's BCP operations.

The live trading on these 2 days was followed by a successful revert of operations to the main site on Wednesday 4th March 2020.

Circular for BCP DR Test – March- April 2021

NSE

Circular

National Stock Exchange Of India Limited

Department : CAPITAL MARKET SEGMENT

Download Ref No: NSE/CMTR/47781 Date : March 25, 2021

Circular Ref. No: 38/2021

All Members,

Live trading sessions from Disaster Recovery (DR) site

The Exchange shall be conducting trading sessions (Mock & Live) from its Disaster Recovery (DR) site. The schedule for the same is given below:

<table>
<tr><th>Date</th><th>Trading sessions</th><th>Location & Configuration</th><th>Schedule & Instructions</th></tr>
<tr><td>March 27, 2021</td><td>Mock Trading</td><td rowspan="4">Disaster Recovery (DR)</td><td>Annexure 1 & Annexure 2</td></tr>
<tr><td>March 30, 2021</td><td rowspan="3">Live Trading</td><td rowspan="4">As per normal market timings</td></tr>
<tr><td>March 31, 2021</td></tr>
<tr><td>April 01, 2021</td></tr>
<tr><td>April 05, 2021</td><td>Live Trading</td><td>Primary site</td></tr>
</table>

Important instructions for members:

- Kindly participate actively in the mock trading session to check the connectivity and to avoid login problems in live trading sessions from DR site.

- Members are requested to note that the Exchange Contingency Tests shall be carried out between 1:30 pm to 3:30 pm for mock trading on Saturday, March 27, 2021.
  Members are requested to plan their activities accordingly.

- The Connect2NSE and Extranet facility will not be available for members (Timings are applicable to Leased Line/ Internet)
  - From 1 am on Saturday, March 27, 2021 to 07:00 am on Sunday, March 28, 2021
  - From 1 am on Friday April 02, 2021 to 08:00 am on Friday, April 02, 2021

- Lease-line members are requested to connect to below mentioned IP address for Extranet from March 27, 2021 to April 01, 2021.
  - Extranet - 172.19.125.71
  - C2N-172.19.125.70

- Latencies experienced by Colo Participants will be different on Disaster Recovery/BCP day as compared to a normal trading day.

- New/revised announcements with respect to mock trading on March 27, 2021 to live trading on March 30, 2021, March 31, 2021 and April 01, 2021 and if any, shall be available on the website www.nseindia.com.

- For connecting to Primary/DR site, no changes in NEAT Adapter settings are required. Settings of live session as of Friday March 26, 2021 in NEAT Adapter shall be retained to connect to all the above sessions of Primary/DR site.

Annexure – 1

Schedule and Important instructions for Mock trading session on Saturday, March 27, 2021

Saturday, March 27, 2021	Start Time	End Time
Morning Block Deal Window– Session 1	09:45 hrs	10:00 hrs
Pre Open*	10:00 hrs	10:08 hrs
Special Pre-Open Session*	10:00 hrs	10:45 hrs
Normal Market/Odd lot	10:15 hrs	15:30 hrs
Normal market open time for stocks in special preopen session	11:00 hrs	15:30 hrs
Call Auction Illiquid session (5 sessions of 1 hour each)*	10:30 hrs	15:30 hrs
Afternoon Block Deal Window– Session 2	12:15 hrs	12:30 hrs
Auction Market	11:30 hrs	12:15 hrs
Closing Session	15:40 hrs	15:50 hrs
Trade Modification	10:15 hrs	16:00 hrs

Important instruction for members:

- Trades resulting from mock trading session on Saturday March 27, 2021 shall not attract any obligation in terms of funds and/or securities pay-in and/or pay-out. Kindly do not transfer any data files for this session.

NSE DR Circular signed, dated , authorised

For and on behalf of
National Stock Exchange of India Limited

Khushal Shah
Associate Vice President

Toll Free No	Fax No	Email id
1800 266 0050	+91-22-26598155	msm@nse.co.in

SBI RFP Resource profile:

1. *The team needs to be headed by an* ***Expert with practical industry experience in conducting similar activity for organizations****.*
2. *We expect team leader be* ***experienced enough in reviewing ISMS and with full understanding of latest ISO developments & global trends.***
3. ***The team leader/member should have ISO27001 LA Certification****.*
4. *The team leader* ***will submit the daily tracker report*** *after evaluation thereof.*
5. *The review activity* ***needs to be completed within fixed time periods*** *hence dedicated resources will be needed for the current activity.*

- ***Deliverables: Certification Audit with observations with reference to ISD of SBI.***
- ***Conduct confirmatory audit, if required and award ISO 27001:2013 Certification for SBI- ISD from UKAS (UK accreditation Service).***

Deliverables

- 2. Conduct 2 consecutive Surveillance Audits for for maintaining the Certification.
- **Deliverables: Surveillance Audit with observations with reference to wings of SBI ISD.**
- **Conduct confirmatory audit, if required and maintain ISO 27001:2013 Certification of ISO & CS wings**
- Impart training to 15 ISO Officials for ISO 27001:2013 LA Certification.
- **Deliverables: Impart training to 15 ISO Officials for ISO 27001:2013 LA Certification and award the participation/pass Certificate to the participants**

Other Conditions:

- 1. The **progress of the activities shall be discussed and communicated** by Lead Auditor with Chief Manager (ISO) and Advisor (ISD).
- 2. During the audit, **the observations should also be shared with the respective Information Security Coordinators** at EOD, so that **they can be closed during the audit itself and will not reflect in final audit report.**
- 3. The Auditors **must possess ISO 27001:2013 LA certificate** and suitable experiences in this area.
- 4. The **Certification Audit report** should be submitted within 3 days from study of evidences and interviews etc.

Ministry of Electronics & IT

F.No. 11(6)/2018-CCA
Government of India
Ministry of Electronics & Information Technology
Office of Controller of Certifying Authorities
Electronics Niketan, 6, CGO Complex, New Delhi-110 003.

Empanelment of Auditors
for auditing Infrastructure of Certifying Authorities

A. Office of the Controller of Certifying Authorities (CCA) desires to empanel Audit Organizations as Auditors for auditing physical and technical infrastructure and the defined and implemented practices of both prospective and licensed Certifying Authorities (CAs) & eSign Service Providers (ESPs) as per the requirements prescribed under the Information Technology Act, 2000.

B. The Audit organization should have personnel with the following qualifications:

(i) Knowledge of trusted computer information systems & trusted networking environments with relevant experience in information systems audit having ISO27001 Lead Auditor certification along with either CISA,DISA,CISSP Certification or other relevant certification. The company should have minimum of five numbers of Information Security auditors with CISA and ISO 27001 Certification on their rolls and should have at least five years experience in conducting security audits. The applicant company should have done minimum 25 nos. of Information Security Audits.

Application format

1. Name of the Organization:
2. No. of years of experience in Information Security audit.
3. Total number of IT systems audits done by the organization (from Jan, 2012):
4. Details of Information Security audit done as mentioned in Sl. 3 above in the following format:

S.No.	Type of Audit (Choose from following) a) Certifying Authority (CA) & eSign Service Provider (ESP) Audit under IT Act, 2000 b) Information Security process audit c) Information Security Technology audit d) Other information systems audit	Name of the Organization where audit was carried out	Year of Audit	Duration (in days)

5. List of Certified Information Security Auditors (in the following format):

Name of the auditor	No. of years of experience	ISO 27001	CISA	DISA	CISSP

6. Qualifications & Number of other Information System auditors:
7. Total number of Auditors on Role of Organization:
8. Details regarding knowledge of digital signature technology, standards and practices:
9. Certification of the Organization, if any (ISO27001/ISO9001, etc.) (Yes/No)

Office of CCA will make a panel of technically acceptable Audit Organizations by benchmarking. After due examination of the financial proposal of the technically qualified (acceptable) proposals, the Office of CCA will fix a man-day rate, which shall be made uniformly applicable to all selected Audit Organizations, subject to their acceptance of rates/terms & conditions. **(Please note that auditor's name performing any given audit will be required to be shared with office of CCA. Minimum one auditor ISO27001 LA qualified and one auditor CISA qualified should be part of audit team)**

RBI IS Audit

निरीक्षण विभाग

सूचना प्रौद्योगिकी कक्ष

With reference to our Expression of Interest (EOI) sought for "Empanelment of Firms for Conducting Information Systems / Information Technology (IS/IT) Audit" within the Bank, we advise that the following firms have been included in the panel for conducting Information Systems / Information Technology Audit, as under:

i. AAA Technologies
ii. Auditime
iii. Deloitte
iv. Digital Age Strategies Pvt.Ltd
v. KPMG
vi. Mahindra SSG
vii. PWC

Terms and conditions

1. *The panel will remain valid for a **period of 3 years**, in normal course, subject to the condition that the firms/individuals continue to be on the panel of approved auditors released by CERT-In.*
2. *The broad scope of work would be on similar lines as that indicated in CERT-In empanelment and may, inter alia, include the following:- **conduct of VA&PT, security assessments/reviews of - application, network, operating systems, databases, source code, SDLC** etc.*
3. *Any firm/company empanelled with the Bank in this process shall cease to exist in Bank's panel of external IS Auditors, if the firm's/ company's CERT-In empanelment is revoked and/ or if the firm/company **is blacklisted by any Government Agency/ Public Sector Undertaking/ Scheduled Commercial** Bank in India any time during the period of validity of the Bank's panel.*

- *4. For the purposes of computation of man-days, the following definition will apply: "Auditing Man-day" shall mean IT Security auditing effort (both on-site as well as off-site)* ***of minimum 8 hours, excluding breaks****, by a person with suitable* ***IT Security auditing related qualification such as CISSP, ISO 27001 Lead Assessor, CISM, CISA, CEH etc.***
- *5. Bank reserves the right to limit the number of audits that can be concurrently executed by a firm for the Bank.*
- *6. The empanelled firms shall be required to enter into a contract with the Bank before undertaking any assignment.*

IPPB

Request For Proposal

For

Empanelment of Information Security Audit Vendor

for providing Auditing Services to Bank

Date: 05-08-2020

Scope of IS Audit

2. Scope of Work

Bidder is expected to carry out IT Systems and Security Audit activities including but not limited to the points mentioned below for respective domains. Further the Bidder has to evaluate and comment on compliance by Bank as per RBI Circular on Cyber Security Framework, Information/Cyber Security Policy/ Procedures/Processes of the Bank, ISO 27001 standards, other RBI & regulatory guidelines for Payment Banks and Industry best practices etc. IT Systems and Security Audit will cover entire gamut and with special reference to the following:

2.1 Locations/office to be covered

- Data Centre -
- Disaster Recovery Centre
- Near Disaster Recovery Centre
- Corporate office
- CPC
- Contact Center
- HO/SO/BO
- Global Service Desk
- Management Unit
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements

b.) Application review:

- Perform Applications Security Testing and Penetration Testing on the Applications.
- Review that periodic checks/audits have been done to ensure that operationa level controls are in place for all business applications of the bank
- Review if the periodic checks are done in the rightful manner
- Periodic review of application to ensure that security controls are in place for web-facing & critical applications.

c.) Hardware & infrastructure review:

- Review and evaluation of the infrastructure landscape to support all the applications
- Review of DC, DR and NDR sites to review their capacity, readiness, securit and adequacy
- WAN/LAN audit
- Inventory of IT assets

d.) Audit of Vulnerability Assessment and Penetration testing (VAPT) carried out b selected/ on boarded SI

- Perform VAPT on the servers.
- Review and ensure that VAPT was done properly and all observations were highlighted and corrective actions were taken as per the defined risk appetite level of the bank

e.) IT review/Security architecture review

- IT Audit vender should review IT /Security architecture implementation vis-à-vis RBI guidelines and security best practices and suggest the solution if any

f.) Review of Access Control & Change Management Process
g.) Review of Data Center/DR/ Near DR installation as per the standard.
h.) Any Adhoc requirement as part of application/product implementation
i.) Perform "APK" audits for various internal and External applications
j.) Compliance testing

IS Audit Report Content

1. **Observations,**
2. **Evidences and document details** and suggest suitable mitigation actions.
3. **Audit report of current quarter** with status Repeat/ Exception or New
4. **Compliance status and observations** of previous quarter report –
5. Identify and **highlight deficiencies** in VAPT performed for the bank.
6. **Categorize the Risk classifications** basis Banks deployed - High, Medium, and Low
7. Servers/Resource affected
8. Risk implications of the issue highlighted
9. **Explicit reference to key policy**, process and procedure documents of the Bank against identified risk/observation
10. **Recommendation for risk mitigation**/ removal and identification of risk probability

- •11. **Suggestions for improvement** – additional voluntary standards or regulations applicable to the banking industry as best practices
- 12. **Summary of audit findings** including identification tests, tools used and results of tests performed
- **Empanelment Period**
- *The empanelment shall be valid **for a period of 24 months** from the date of result of empanelment. The same will be reviewed on yearly basis subject to satisfactory performance of the bidder. However, if in any case it is found that the services offered are not satisfactory, the Bank may consider termination of the empanelment of the Vendor*
- *Bidder should be **CISA/DISA/ CISM & or ISO 27001 (ISMS) certified***
- *The bidder should be an empanelled Info **Security Auditing Firm with CERT-IN as on RFP publication date** and also during the course of Audit*

Evaluation parameters

- *The bidder must be having on their roles, on permanent employment basis in India ,a minimum no. Of professionals (mentioned below) who hold **professional certifications like CEH / DISA (certificate issued by ICAI) / CISSP / CISM/ CISA / ISO 27001** with requisite experience to handle the work as per the scope (valid as on date)*
- **Desired experience :**

✓ Process Audit, Site Audit

✓ VA/PT

✓ Forensic Audit

✓ Application Audit

✓ Network Audit

✓ Audit of Security devices/Solutions

✓ Database Audit

✓ Migration Audit

- **TATA Power BCP - Vision**
- To preserve human life , environment and minimize economic losses of Unit with implementable BCDM Plan, which has 5 components

✓ Prevention (Mitigation),

✓ Response,

✓ Resumption,

✓ Recovery and

✓ Restoration.

- **Mission**
- *To successfully implement "Business Continuity & Disaster Management Plan" through well trained, well-resourced and committed people.*

DRP – Chapters

- **Chapter 1** –brief description of Organization, its context, risk appetite & need
- **Chapter 2** –Objectives and Scope of BCDMP. ,Corporate Policy on Business Continuity as approved by Top Management with assumptions & limitations
- **Chapter 3** –Organizational Structure for BCDMP & roles & responsibilities of each designated Officer during pre- incident stage as well as post-incident stage till full normalization
- **Chapter 4** –Vital Installations & Technology, Vital Data and Vital people for post-incident management.
- **Chapter 5** –classification of functions, BIA for any disruptive incident & calculation of BIA, **MTPD** – Maximum Tolerable Period of Disruption & **RTO**
- **Chapter 6** – **Plans under BCDMP** viz **Mitigation Plan**, **Response Plan** including **Warning procedure** about impending incident, **Evacuation Plan, Incident Management Plan, Casualty Management plan**, **Resumption Plan**, **Recovery Plan** , **Restoration Plan** and **Notification process**.
- **MTPD** – Maximum Tolerable Period of Disruption, **MBCO** – Minimum Business Continuity Objectives and **RTO**

- **Chapter 7** –procedure of organizing Testing of **“DMP”** &**“BCP”.**
- organising **Team Exercise,**
- mentions periodicity of exercises / testing & maintaining record of each activity followed by corrective actions wherever necessary.
- **Chapter 8** –Performance Evaluation of organization in case of any disruptive incident as well as during exercises / Testing & Management Review for corrective actions.

Risk Analysis

- Risk assessment : exercise of identifying and analyzing potential vulnerabilities and threats.
- **Sources**

✓ Natural Calamities (Flood, earthquake, storm)

✓ Terrorism / Sabotage

✓ Fire

✓ Catastrophic failure of critical equipment

✓ Community-wide hazardous events (Strike, Riots/ curfew)

✓ Accidents causing extreme material disruptive incident

✓ Security threats, network and communication failures

✓ Disastrous application errors

- Each risk is assessed considering: **Loss of Human life; Environmental Damages, Financial Loss, Statutory, legal & regulatory requirements, impact on interested parties and impact on business objectives**
- **Risk** levels are classified as Catastrophic, Critical. High, Medium and Low

BCM Team- Tata Power Ltd

Sr. No.	Position	Name of the Officer	Designation	E-mail Address	Landline No.	Mobile No.
1	BC Team Leader-North		Zonal Head - North			
2	BC Team Leader-Central		Zonal Head - Central			
3	BC Team Leader-South		Zonal Head- South			
4	BC Team Leader- Trans. Lines		Zonal Head- Trans. Lines			
5	BC Team Leader- EHV Cables		Zonal Head- EHV Cables			
	Site Controller -Borivli		Nodal Head - Borivli			
	Site Controller-Saki		Nodal Head-Saki			
	Site Controller-Salsette		Nodal Head-Salsette			
	Site Controller-Carnac		Nodal Head-Carnac			
	Site Controller-Parel		Nodal Head-Parel			
	Site Controller-Dharavi		Nodal Head-Dharavi			
	Site Controller-Vikhroli		Nodal Head-Vikhroli			
	Site Controller-Kalyan		Nodal Head-Kalyan			
	Site Controller-Chembur		Nodal Head-Chembur			
7	Site Controller- Trans. Lines		Nodal Head-Trans. Lines			
8	Over-all In-charge		Chief - Transmission			
9	BC Coordinator		Group Head - MIS & Capex			
10	BC Administrator		Group Head- Performance Assurance			

Damage Assessment Team

Sr. No.	BC Position	Designation	Name of the Officer	E-mail Address	Mobile No.	Landline No.
1	DA Team Leader	Respective Nodal Head				
2	DA Team member	Respective NSMC engineers				
3	DA Team member	Resident Testing Engineer of the Zone				
4	DA Team member	Specialist - Trans. Lines				
5	DA Team member	Lead Engineer - EHV Cable				
6	DA Team member	Lead Engineer - SCADA				

BIA

A. Critical functions – If these business functions are interrupted or unavailable for some time, **can completely jeopardize business and cause heavy damages**

- B. **Essential functions** – whose **loss would seriously affect** organization's ability to function for long.
- **C. Necessary functions** –organization can continue functioning; however, absence of these functions **would limit their effectiveness**, to a great extent.
- D. **Desirable functions** –would be beneficial; however, their absence **would not affect capability** of organization.

BCP Activation

Categorization	Type of Emergency	Resources
Level 1	Minor Emergency	Fire Fighting, First Aid & Communication Equipment & Manpower available in Unit Invoke DMP
Level 2	Major Emergency	Fire Fighting, First Aid & Communication Equipment & Manpower available in Unit as well as mobilization of Mutual Aid Group. Invoke BCP
Level 3	Disaster	Fire Fighting, First Aid & Communication Equipment & Manpower available in Unit as well as mobilization of Mutual Aid Group and Government Agencies Invoke BCP

Siren Codes

- **Emergency**: siren shall be wailing sound 3 times for 30 seconds with a gap of 5 second after every 30 seconds
- **DISASTER** : siren shall be wailing sound 5 times for 30 seconds with a gap of 5 second after every 30 seconds
- **ALL CLEAR**: siren shall be straight run sound for 2 minutes
- **Warning for Earthquake:**
- - In case of earthquake related incidents, evacuation procedure wailing siren indicated by "Siren Code - Disaster" will be given

Terrorist attack

- **NO SIREN** will be issued.
- A message "TERRORIST ATTACK" will be shouted 3 times over "Public Address System", (PAS) by any person, who cites such terrorists.
- **Warning for Fire related incidents:**
- evacuation procedure - wailing siren indicated by "Siren Code - Emergency" will be issued.

BCP Internal Audit

- *"essential for the organization to conduct internal audits at planned intervals so that it makes sure that the BCMS conforms to organization's own requirements and the requirements of this International Standard.*
- ***It is essential to conduct internal audits of the BCMS** to ensure that the BCMS is **achieving its objectives, that it conforms to its planned arrangements and has been properly implemented and maintained,** and to **identify opportunities for improvement.***
- *Internal audits of the BCMS shall be conducted **at half-yearly intervals** to determine and provide information to top management on appropriateness and effectiveness of the BCMS as well as to provide a basis for setting objectives for continual improvement of BCMS performance "*

BCM- Internal Audit
: Tata Power

- *'' The Company's, internal audit programme shall be based on the full scope of the BCMS, however, each audit need not cover the entire system at once.*
- *Audits **may be divided into smaller parts,** so long as the audit programme ensures that all organizational units, functions, activities and system elements and the **full scope of the BCMS are audited in the audit programme within the auditing period.''***

BCP IS Audit Case

- **Client :** one of Top 5 Hospitals in India
- ***Department –wise:***

1. *Critical Business process*
2. *Critical Equipment or Resources*
3. *Technology & Equipment Critical Processes*
4. *Staffing Positions*
5. *Critical Records*
6. *Departmental Dependencies – internal/external*

The Deadly Power of Software

- Can a software design fault kill hundreds of human beings at once ?
- OEM = Global leader

Boeing's role – Root Cause Analysis
Business & Cost issues

- Intense competition **from Airbus A320 NEO**
- **Order book loss** if Competing product not launched fast
- MAX designed around new set of engines - LEAP-1Bs.
- Much more efficient than engines on 737NG, but **much heavier and larger.**
- This created **a design problem --- 737 Max = stopgap measure**
- Boeing **saved billions of dollars in engineering costs** by basing Max in 737 platform
- Aggressive branding & promotion of Boing 737 MAX campaign **masked faulty software design & production process, without system testing & stretched to breaking point.**
- FAA **overlooked** MCAS – Certifying tests not adequate
- MCAS built to Boeing's specifications by Collins Aerospace
- **A single sensor input – MCAS Software will kick in (no consistency check)-** reliance on a single angle-of-attack sensor ?

Ethiopian Airlines Crash 2019 - Flight 302

- ***10 March 2019 - Ethiopian Airlines 302***
- 05:38 UTC, Ethiopian Airlines flight 302, Boeing 737-8(MAX), ET-AVJ, took off from Addis Ababa Bole Int. Airport bound to Nairobi.
- Shortly after takeoff, AOA sensor recorded value became erroneous
- Due to flight control problems, **Captain was unable to maintain the flight path** and **requested to return back** to the departure airport.

Crew lost control of aircraft which **crashed at 5: 44 UTC**

- UTC – Coordinated Universal Time

Cockpit electronics & Master warnings & cautions (Black Box – CVR Transcript)

- Stabilizer movement **will increase force needed to hold control column**, by **about 40 to 50 pounds** for a 2.5 degree movement.
- Ground Proximity Warning System sounded in cockpit: ***"DON'T SINK. DON'T SINK."***
- ***"DON'T SINK. DON'T SINK."*** **(Repeat WARNING)**
- **"Pull up! Pull up!" – Captain**
- 15 seconds later, airplane crashed **at over 500 knots** of airspeed into a field near town of Bishoftu, Ethiopia.
- **None of the 157 people** aboard survived.

Aftermath of 2 crashes

- Crash : Lion Air, Ethiopian Airlines , 346 casualties
- MAX 8 Flights grounded in all countries
- Software update being developed
- Financial impact on Boeing : Credit rating, damages, lawsuits , revenue loss etc
- Cascading risk impact : Spicejet, Jet Airways

Boeing's official press release on MCAS Software update - 2020

- *Boeing has developed an MCAS software update to provide additional layers of protection if the AOA sensors provide erroneous data.*
- *The software has been put through hundreds of hours of analysis, laboratory testing, verification in a simulator and numerous test flights.*
- *Before it is finalized, the software will be validated during in-flight certification tests with Federal Aviation Administration (FAA) representatives.*
- *These updates are expected to reduce the crew's workload in non-normal flight situations and prevent erroneous data from causing MCAS activation.*
- *We continue to work with the FAA and other regulatory agencies on the certification of the software update.*
- **FAA - Federal Aviation Administration**

MCAS Software update

- *The additional layers of protection **that are being** proposed include:*
- *Flight control system **will now compare inputs from both** AOA sensors.*
- *If the sensors **disagree by 5.5 degrees** or more with the flaps retracted, **MCAS will not activate.***
- *An **indicator on the flight deck display** will alert the pilots.*
- *MCAS **can never command more stabilizer input** than can be **counteracted by the flight crew** pulling back on the column.*
- *The pilots **will continue to always have the ability to override MCAS** and manually control the airplane.*

Lessons learnt

New software must :

1. Undergo extensive testing and review

2. Undergo new certification by Regulators

(maybe as a new model)

3. **Be communicated to pilots** through AFM , airline operators & included in a **conspicuous manner** in FCOM / FCTM - **pilots adequately trained in its operation & respond appropriately in times of crisis**

4. Zero tolerance game = safety / security is to be always **accorded top priority over cost control and winning in the market competition.**

5. **Keep software systems in complex machines as simple as possible**

6. **Not to impose software on intractable hardware fault**

7. **Implementing software system redundancy**

Arijit Chakraborty