Cyber Security Framework for UCBs-A Graded Approach

Level II – Basic Controls

પ્રાથમિક (શહેરી) સહકારી બેંકો (UCBs) માટે વ્યાપક સાયબર સુરક્ષા માળખું (Comprehensive Cyber Security Framework) – તબક્કાવાર (Graded) અભિગમ

ભારતીય રિઝર્વ બેંક (RBI) દ્વારા ઓક્ટોબર 2018માં પ્રાથમિક (શહેરી) સહકારી બેંકો (UCBs) માટે મૂળભૂત (Baseline) સાયબર સુરક્ષા નિયંત્રણો અમલમાં મૂકવા સૂચનાઓ આપવામાં આવી હતી.

ત્યારબાદ થયેલી સમીક્ષા અને મૂલ્યાંકનના આધારે RBI એ હવે UCBs માટે **"Comprehensive Cyber Security Framework"** અમલમાં મૂકવાનો નિર્ણય કર્યો છે. આ માળખું **Graded Approach (તબક્કાવાર અભિગમ)** પર આધારિત છે.

આ અભિગમ હેઠળ દરેક UCB માટે સાયબર સુરક્ષાના ધોરણો નીચેના પરિબળોને ધ્યાનમાં રાખીને નક્કી કરવામાં આવશે:

- બેંકની **ડિજિટલ સેવાઓ (Digital Products)** નું પ્રમાણ અને વ્યાપ.
- **ચુકવણી પ્રણાલીઓ (Payment Systems)** સાથે બેંકનું જોડાણ (Interconnectedness).
- બેંકમાં **માહિતી ટેક્નોલોજી (IT)** નો ઉપયોગ અને તેનો વ્યાપ.
- બેંક સામે રહેલા **સાયબર સુરક્ષા જોખમો (Cyber Security Risks)** નું મૂલ્યાંકન.

Graded Approach નો મુખ્ય હેતુ

આ માળખા હેઠળ બેંકોને તેમની ડિજિટલ સેવાઓના **પ્રકાર, સંખ્યા અને વ્યાપ** અનુસાર તબક્કાવાર વધુ મજબૂત સાયબર સુરક્ષા વ્યવસ્થા અમલમાં મૂકવી ફરજિયાત રહેશે.

અર્થાત્, જેટલી વધુ ડિજિટલ સેવાઓ, જેટલો વધુ ટેક્નોલોજીનો ઉપયોગ, એટલી વધુ સાયબર સુરક્ષા વ્યવસ્થા જરૂરી રહેશે.

- **"RBI હવે તમામ UCBs માટે એકસરખા નિયમો લાગુ કરતું નથી. જે બેંક જેટલી વધુ ડિજિટલ સેવાઓ આપે છે, તેના માટે સાયબર સુરક્ષાના ધોરણો પણ એટલા જ વધુ કડક રાખવામાં આવ્યા છે. આને જ 'Graded Approach' કહેવાય છે."**
- **"આ ફ્રેમવર્કનો હેતુ માત્ર સાયબર હુમલા અટકાવવાનો નથી, પરંતુ UCBs ને Commercial Banks જેટલી સક્ષમ અને સજ્જ બનાવવાનો છે જેથી ગ્રાહકોનો વિશ્વાસ જળવાઈ રહે અને ડિજિટલ બેંકિંગ સુરક્ષિત બને."**

Baseline Cyber Security and Resilience Requirements for Level II UCBs in addition to requirements for Level I UCBs

Level II UCBs for this purpose mean all UCBs, which are sub-members of Centralised Payment Systems (CPS) and satisfying at least one of the criteria given below:

- offers internet banking facility to its customers (either view or transaction based)
- provides Mobile Banking facility through application (Smart phone usage)
- is a direct Member of CTS/IMPS/UPI.

RBI Requirement: લેવલ-II બેન્કોને લેવલ-I બેન્કોને લાગુ પડતી બેઝલાઈન રિક્વાયરમેન્ટ ઉપરાંત નીચેની વધારાની રિક્વાયરમેન્ટ લાગુ પડશે.

દરેક UCB એ એવો એક જવાબદાર અધિકારી નિયુક્ત કરવો જોઈએ (તેનું પદ CISO હોવું જરૂરી નથી), જે બેંકની માહિતી સંપત્તિ (Information Assets) ની સુરક્ષા માટેની નીતિઓ બનાવે, તેનો અમલ કરાવે અને RBI દ્વારા સમયાંતરે આપવામાં આવતી Information Security તથા Cyber Security સંબંધિત તમામ સૂચનાઓનું પાલન થાય તેની ખાતરી કરે.

"Cyber Security માત્ર IT વિભાગનું કામ નથી. પરંતુ કોઈ એક અધિકારી એવો હોવો જોઈએ જે સમગ્ર Cyber Security વ્યવસ્થાની જવાબદારી લે."

તેનું મુખ્ય કાર્ય:

- Cyber Security Policy તૈયાર કરવી
- તેનો અમલ કરાવવો
- IT વિભાગ સાથે સંકલન કરવું
- RBI ની તમામ Cyber Security Guidelines નું પાલન કરાવવું
- Cyber Security Incident સમયે કાર્યવાહીનું સંકલન કરવું

ઘણી સહકારી બેંકોમાં Cyber Security માટે કોઈ એક જવાબદાર અધિકારી ન હોવાથી જવાબદારી સ્પષ્ટ રહેતી નથી.

આથી RBI કહે છે: **"Everyone's responsibility often becomes no one's responsibility."** એટલે એક અધિકારીને સ્પષ્ટ જવાબદારી સોંપવી જરૂરી છે.

For Example: ABC Urban Co-operative Bank માં IT Manager ને Cyber Security Officer તરીકે નિયુક્ત કરવામાં આવે તો તેની જવાબદારીઓ:

✔ VA/PT કરાવવું

✔ Cyber Incidents Report કરવો

✓ Password Policy તૈયાર કરવી

✓ Employee Training

✓ RBI Compliance

1. Network Management and Security

1.1. Maintain an up-to-date/centralised inventory of authorised devices connected to UCB's network (within/outside UCB's premises) and related network devices in the UCB's network.

RBI Requirement

બેંક પાસે તેના નેટવર્ક સાથે જોડાયેલા તમામ અધિકૃત Devices નો Central Inventory હોવો જોઈએ. બેંકમાં કેટલા: Desktop, Laptop, ATM, Server, Router, Switch, Firewall, Wi-Fi Devices છે તેની સંપૂર્ણ યાદી હોવી જોઈએ. કારણકે જો તમને ખબર જ ન હોય કે Network પર કેટલા Devices જોડાયેલા છે, તો Hacker માટે કોઈ અજાણ્યું Device જોડવું સરળ બની જાય. **Example:** Audit દરમિયાન જાણવા મળ્યું એક જૂનું Laptop હજુ પણ CBS સાથે જોડાયેલું હતું, **જેની** કોઈને ખબર નહોતી. આ મોટું જોખમ છે. **" જેની Inventory નથી તેનું Security પણ નથી."**

1.2 Boundary Defence

Boundary defences should be multi-layered with properly configured firewalls, proxies, DMZ (De-Militarized Zone), Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place.

બેંકના કોમ્પ્યુટર નેટવર્કને બહારના સાયબર હુમલાથી સુરક્ષિત રાખવા માટે બહુસ્તરીય (Multi-layered) સુરક્ષા વ્યવસ્થા હોવી જોઈએ. તેમાં નીચેના સાધનોનો સમાવેશ થવો જોઈએ: Firewall, Proxy Server, DMZ (De-Militarized Zone), IDS (Intrusion Detection System), IPS (Intrusion Prevention System)

સાથે સાથે બહારથી આવતો (Inbound) અને બહાર જતો (Outbound) બંને પ્રકારનો Network Traffic તપાસીને જ મંજૂર કરવો જોઈએ.

આજના Cyber Attack માત્ર Firewall થી અટકતા નથી. જો એક સુરક્ષા સ્તર નિષ્ફળ જાય તો બીજું સ્તર હુમલો અટકાવે. આને Defence in Depth કહેવામાં આવે છે. એક મજબૂત બેંકમાં એક નહીં પરંતુ અનેક સુરક્ષા સ્તરો હોય છે.

ઉદાહરણ: ધારો કે Hacker બેંકની Website Hack કરવાનો પ્રયાસ કરે છે. સૌપ્રથમ- Firewall તેને ચેક કરે છે. જો Firewall ચૂકી જાય તો IDS શંકાસ્પદ પ્રવૃત્તિ શોધે છે. જો હુમલો સાચો હોય તો, IPS હુમલો તરત જ Block કરી દે છે. જો Web Server Compromise થાય તો, DMZ હુમલાને CBS સુધી પહોંચવા દેતું નથી. એટલે સમગ્ર Core Banking System સુરક્ષિત રહે છે.

એક જ દરવાજા પર એક જ ચોકીદાર રાખવાથી સુરક્ષા થતી નથી. બેંકની Cyber Security માં અનેક ચોકીદારો સાથે મળીને કામ કરે છે. Firewall પ્રથમ સુરક્ષા છે, પરંતુ અંતિમ સુરક્ષા નથી. IDS, IPS અને DMZ મળીને બેંકને સુરક્ષિત બનાવે છે. "Cyber Security માં સૌથી મહત્વનો સિદ્ધાંત છે – Defence in Depth, એટલે કે એક પછી એક અનેક સુરક્ષા સ્તરો."

1.3 LAN segments for in-house/onsite ATM and CBS/branch network

બેંકની ATM સિસ્ટમનું Local Area Network (LAN) અને CBS/Branch Office નું LAN એક જ નેટવર્ક પર ન હોવું જોઈએ. "Cyber Security નો એક મૂળભૂત સિદ્ધાંત છે – 'Separate Critical Systems'. ATM અને CBS ને અલગ Network Segment માં રાખવાથી એક સિસ્ટમ પરનો હુમલો બીજી સિસ્ટમ સુધી પહોંચતો નથી. આ જ Network Segmentation નું મહત્વ છે." બંને માટે અલગ-અલગ Network Segments (અલગ VLAN અથવા Subnet) બનાવવાના રહેશે.

RBI આ શા માટે કહે છે?

ATM એક Public Facing Device છે. CBS બેંકનું સૌથી સંવેદનશીલ (Critical) System છે. જો ATM અને CBS એક જ Network પર હશે, તો ATM પર થયેલો Cyber Attack CBS સુધી પહોંચી શકે છે. તેથી RBI કહે છે કે ATM Network ને CBS Network થી સંપૂર્ણપણે અલગ રાખો. આને Network Segmentation કહેવામાં આવે છે.

ઉદાહરણ: ધારો કે ABC Urban Co-operative Bank પાસે 10 Branches and 15 ATMs છે. જો ATM અને CBS એક જ LAN પર હોય તો, ATM → Switch → CBS Server, જો કોઈ Hacker ATM માં Malware મૂકી દે, તો Malware સીધો CBS Server સુધી પહોંચી શકે છે. પરંતુ જો અલગ Segmentation હોય ATM Network (VLAN-10) → Firewall → CBS Network (VLAN-20) તો ATM Compromise થાય પણ CBS સુરક્ષિત રહે.

સરળ ઉદાહરણ→ એક હોસ્પિટલમાં Emergency Ward અને Operation Theatre એક જ રૂમમાં રાખવામાં આવતાં નથી. કારણ કે Infection ફેલાઈ શકે. એ જ રીતે ATM Network અને CBS Network અલગ રાખવામાં આવે છે.

ATM એ જાહેર ઉપયોગનું મશીન છે, જ્યારે CBS બેંકનું હૃદય છે. બંનેને એક જ નેટવર્કમાં રાખવું એ જોખમને આમંત્રણ આપવા જેવું છે. જો ATM પર હુમલો થાય તો તેનો અસર CBS સુધી ન પહોંચે, એ માટે RBI એ Network Segmentation ફરજિયાત બનાવ્યું છે.

Information System Auditor સામાન્ય રીતે નીચેના પ્રશ્નો પૂછશે:

- ATM માટે અલગ VLAN છે?
- CBS માટે અલગ VLAN છે?
- Firewall દ્વારા બંને વચ્ચે Access Control છે?
- ATM Network થી સીધું CBS Access થઈ શકે છે?
- Network Diagram ઉપલબ્ધ છે?
- Switch Configuration માં Segmentation દેખાય છે?

જો આ વ્યવસ્થા ન હોય, તો તે Information Security Observation અથવા High Risk Observation બની શકે છે.

2. Secure Configuration

2.1 RBI Requirement

Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

બેંકમાં ઉપયોગમાં લેવાતા દરેક IT સાધન માટે સુરક્ષાના લઘુત્તમ ધોરણો (Baseline Security Standards) નક્કી કરવા, તેનું દસ્તાવેજીકરણ કરવું, તેનો અમલ કરવો અને સમયાંતરે તેની સમીક્ષા કરવી જરૂરી છે.આમાં સમાવેશ થાય છે: Desktop Computers, Laptops, Mobile Devices, Operating Systems, Databases, CBS Software, Internet Banking, Routers, Switches , Firewall, Antivirus, Security Devices,

2.2 Baseline Security એટલે શું?

"દરેક Computer અથવા Server ચાલુ કરતાં પહેલાં તેની સુરક્ષા માટેની લઘુત્તમ જરૂરી સેટિંગ્સ નક્કી કરવી."

જેમ નવી શાખા શરૂ કરતાં પહેલાં Checklist હોય છે, એ જ રીતે નવા Computer માટે પણ Checklist હોવા જોઈએ.

2.3 RBI આ શા માટે કહે છે?

ઘણા Cyber Attack નબળા Configuration ના કારણે થાય છે. ઉદાહરણ: Default Password, Antivirus બંધ, Windows Update ન થયેલ, Firewall Disabled, USB Port ખુલ્લા, આવી નાની ભૂલો Hacker માટે મોટો રસ્તો બની જાય છે.

Example: નવી Branch માં 10 નવા Computers મૂકવામાં આવ્યા.જો કોઈ Standard Configuration ન હોય તો એક Computer માં Antivirus હશે, બીજામાં નહીં. એકમાં Strong Password હશે, બીજામાં Admin/Admin હશે. આ ગંભીર જોખમ છે. એટલે RBI કહે છે- "દરેક Device માટે એકસરખો સુરક્ષા ધોરણ હોવો જોઈએ."

2.4 Baseline Configuration માં શું હોઈ શકે?

i) Strong Password Policy, ii) Antivirus Installed iii) Firewall Enabled iv) Latest Patches v) USB Restricted vi) Auto Screen Lock vii) Encryption Enabled viii) Logging Enabled ix) Default Accounts Disabled

બેંકમાં દરેક Computer સુરક્ષિત હોવો પૂરતો નથી; દરેક Computer એકસરખી રીતે સુરક્ષિત હોવો જોઈએ. Cyber Security નું સૌથી મોટું જોખમ ખોટું Configuration છે. જે રીતે દરેક Branch માં Cash Safe Vault ના કેટલાક Standard હોય છે, તેવી જ રીતે દરેક Computer માટે Security Standard હોવો જોઈએ."

2.5 What Auditor will check?

i) Baseline Configuration Document છે? ii) Review કેટલા સમય પછી થાય છે? iii) Patch Management Policy છે? iv) Hardening Checklist છે? v) Configuration Approval છે?

3. Application Security Life Cycle (ASLC)

ASLC એટલે જ્યારે Software બને છે, તેની શરૂઆતથી લઈને તેનો ઉપયોગ શરૂ થાય ત્યાં સુધી દરેક તબક્કે Security ધ્યાનમાં રાખવી.

3.1 RBI Requirement

Development/Test અને Production Environment અલગ હોવા જોઈએ. અને Testing દરમિયાન સાચા Customer Data નો ઉપયોગ ન કરવો. જો કરવો પડે તો Data Masking કરવું. Software બનાવવા માટે જે Server ઉપયોગમાં લેવાય છે અને બેંકમાં ચાલતું Live CBS બંને અલગ હોવા જોઈએ.

3.2 RBI આ શા માટે કહે છે?

GUJFED

જો Developer સીધું Live CBS માં કામ કરે તોએક નાની Programming ભૂલથી હજારો Accounts પર અસર થઈ શકે.

Example: CBS Vendor નવા Interest Module પર કામ કરે છે. જો સીધું Live CBS માં Testing કરે તો FD Interest ખોટું Calculate થઈ શકે. Customer Accounts બગડી શકે. તેથી પહેલા Test Server પર Testing પછી Production માં અમલ.

3.3 Data Masking શું છે?

Testing માટે સાચા Customer Data નો ઉપયોગ ન કરવો. ઉદાહરણ- સાચું નામ: Ganpatbhai Mistri, Account: 123456789123, Testing માટે નામ: Customer A, Account: XXXXXXXX9123, PAN- ABCDE1234F બદલે ABCDE**F આને Data Masking કહે છે.**

Testing માટે ગ્રાહકનો સાચો ડેટા ક્યારેય વાપરવો નહીં "Developer નું સ્થાન Test Server છે, CBS (Production) Server નહીં.

3.4 Secure Coding

RBI Requirement

Software બનાવતી વખતે Secure Coding, Security Testing, (based on global standard) અને Secure Rollout થવું જોઈએ. Software માત્ર ચાલે એટલું પૂરતું નથી. તે Hacker સામે સુરક્ષિત પણ હોવું જોઈએ.

Secure Coding એટલે શું?

Program લખતી વખતે જ Security Rules નું પાલન કરવું. ઉદાહરણ- ખોટું Coding- Password Plain Text માં Store કરવો. સાચું Coding- Password Encrypt કરવો.

બીજું ઉદાહરણ- User Input ચેક ન કરવો. પરિણામ- SQL Injection Attack.

ત્રીજું ઉદાહરણ- OTP Log File માં લખવો. આ પણ જોખમ.

Security Testing- Software Live કરતાં પહેલાં Ethical Hacker દ્વારા તપાસ.

3.5 Secure Rollout- નવું Version સીધું બધી Branch માં મૂકવું નહીં. પહેલા Pilot Branch પછી ધીમે ધીમે Rollout.

"RBI નું સ્પષ્ટ માનવું છે કે Security by Design, Security by Default અને Security throughout the Life Cycle અપનાવવી જોઈએ."

"નવી શાખા ખોલતાં પહેલાં જેમ Building Plan, Safety અને Security ની ચકાસણી કરીએ છીએ, તેવી જ રીતે નવા Software અથવા IT System ને Live કરતાં પહેલાં તેની સુરક્ષાની સંપૂર્ણ તપાસ કરવી જરૂરી છે. એક નાની Configuration ભૂલ અથવા અસુરક્ષિત Coding આખી બેંકને Cyber Attack માટે ખુલ્લી મૂકી શકે છે."

4. Change Management

4.1 RBI Requirement

"UCBs should have a robust Change Management Process to record and monitor all changes made in the Production Environment. All changes to business applications, technology, service components and IT

facilities should be managed through a proper Configuration Management Process to ensure that the changes are accurate, authorised and secure."

બેંકની **CBS, Internet Banking, Mobile Banking, ATM, Server, Network** અથવા અન્ય **IT** સિસ્ટમમાં કરવામાં આવતા દરેક ફેરફાર **(Change)** માટે એક સુનિશ્ચિત અને લેખિત પ્રક્રિયા હોવી જોઈએ.

દરેક ફેરફાર યોગ્ય મંજૂરી બાદ જ કરવો, તેનો સંપૂર્ણ રેકોર્ડ રાખવો, અમલ પછી તેની ચકાસણી કરવી, જરૂરી હોય તો પાછું જૂનું **Version (Rollback)** લાવી શકાય તેવી વ્યવસ્થા રાખવી.

4.2 Change એટલે શું?

Change એટલે **IT** સિસ્ટમમાં કરવામાં આવતો કોઈપણ ફેરફાર. ઉદાહરણ તરીકે: **CBS** નું નવું **Version Install** કરવું, **Interest Rate Parameter** બદલવો, **Firewall Rule** બદલવી, **Password Policy** બદલવી, **Server Upgrade** કરવું, **ATM Software Update** કરવું, **Mobile Banking** માં નવી સુવિધા ઉમેરવી, **Database Configuration** બદલવી, આ બધું **Change** કહેવાય.

4.3 RBI આ શા માટે કહે છે?

ઘણી વખત **Cyber Incident Hacker** ના કારણે નહીં પરંતુ અનિયંત્રિત **Change** ના કારણે બને છે.એક નાનો ફેરફાર પણ આખી બેંકને અસર કરી શકે છે. તેથી **RBI** કહે છે: "કોઈપણ **Change** વિચાર્યા વગર, પરીક્ષણ કર્યા વગર અથવા મંજૂરી વગર ઉપયોગ **(Production)** માં ન કરવો."

4.4 ઉદાહરણ **1 – CBS Vendor** એ **FD Interest** નું **Parameter** બદલ્યું. **Testing** કર્યા વગર સીધું **Live** કરી દીધું.

પરિણામ: હજારો **FD** પર ખોટું વ્યાજ લાગ્યું. **Customer Complaints** આવી. **Manual Corrections** કરવા પડ્યા.

જો **Change Management Process** હોત, તો આ ભૂલ અટકી શકી હોત.

ઉદાહરણ **2 - IT Engineer** એ **Firewall** માં એક **Rule** કાઢી નાખ્યો. તેના કારણે **Internet Banking** બહારથી ખુલ્લું થઇ ગયું આ નાની ભૂલ મોટો **Cyber Attack** બની શકે.

ઉદાહરણ **3 –** નવી **CBS Version Install** કરતાં પહેલાં **Test Server** પર **Testing, User Acceptance Testing (UAT), Management Approval, Backup, Rollback Plan** હોવા જોઈએ.

4.5 Change Management Process

દરેક **Change** માટે નીચેના પગલાં હોવા જોઈએ:

Step 1 – Change Request, ફેરફાર શા માટે જરૂરી છે?

Step 2 – Risk Assessment, તેની શું અસર થશે?

Step 3 – Approval, યોગ્ય અધિકારીની મંજૂરી.

Step 4 – Testing, Test Server પર પરીક્ષણ.

Step 5 – Backup, જૂનો **Data** અને **Configuration** નો **Backup.**

Step 6 – Implementation, ઉપયોગમાં અમલ.

Step 7 – Verification, બધું યોગ્ય રીતે ચાલે છે કે નહીં તેની તપાસ.

Step 8 – Documentation, ફેરફારનો સંપૂર્ણ Record.

4.6 Configuration Management શું છે?

Configuration Management એટલે બેંકની IT સિસ્ટમમાં શું Installed છે, કયું Version ચાલે છે, કયું Settings છે, તેનો સંપૂર્ણ અને અપડેટ Record રાખવો.

ઉદાહરણ: Server-01, Windows Server 2022, CBS Version 11.3, Firewall Version 5.1, Antivirus Version 8.2, આ બધું Configuration Management નો ભાગ છે.

4.7 RBI "Integrity of Changes" શા માટે કહે છે?

Integrity એટલે ફેરફાર યોગ્ય રીતે થયો છે કે નહીં? કોઈ અનધિકૃત ફેરફાર થયો નથી. કોઈ Malware Install થયું નથી. કોઈ Security Setting Disable થઈ નથી.

4.8 Auditor will check-

Change Management Policy છે? Change Register છે? Change Request Form છે? Management Approval છે? Testing Report છે? Rollback Plan છે? Emergency Change Process છે? Change પછી Post-Implementation Review થાય છે?

4.9 Remember: "IT સિસ્ટમમાં દરેક ફેરફાર સુધારો લાવે એવું જરૂરી નથી; ખોટો ફેરફાર આખી બેંકને મુશ્કેલીમાં મૂકી શકે છે."

"Production Environment કોઈ પ્રયોગશાળા નથી. ત્યાં માત્ર સંપૂર્ણ પરીક્ષણ કરેલા અને મંજૂર થયેલા ફેરફારો જ અમલમાં મૂકવા જોઈએ."

"Change Management નો અર્થ માત્ર Software બદલવો નથી, પરંતુ દરેક ફેરફારને સુરક્ષિત, નિયંત્રિત અને દસ્તાવેજીકૃત રીતે અમલમાં મૂકવો છે."

“બેંકમાં અનધિકૃત IT Change એ અનધિકૃત નાણાકીય વ્યવહાર જેટલો જ ગંભીર જોખમ છે."

"No Testing → No Change, No Approval → No Change, No Documentation → No Change"

5. Periodic Testing (નિયમિત સુરક્ષા પરીક્ષણ)

5.1. Periodically conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of internet facing web/mobile applications, servers and network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.). VA of critical applications and those on DMZ shall be conducted atleast once in every 6 months. PT shall be conducted atleast once in a year.

"કોઈપણ IT સિસ્ટમ સંપૂર્ણપણે સુરક્ષિત નથી. સમય જતાં નવી સુરક્ષા ખામીઓ (Vulnerabilities) શોધાય છે. તેથી નિયમિત પરીક્ષણ કરીને ખામીઓ શોધવી અને સમયસર દૂર કરવી જરૂરી છે."

Vulnerability Assessment (VA) અને Penetration Testing (PT) વચ્ચેનો તફાવત

Vulnerability Assessment (VA)	Penetration Testing (PT)
સુરક્ષાની ખામીઓ શોધે છે	તે ખામીઓનો ઉપયોગ કરીને હુમલો શક્ય છે કે નહીં તેની ચકાસણી કરે છે
Scanner અને Security Tools નો ઉપયોગ	Ethical Hacker દ્વારા હાથથી પરીક્ષણ
"ક્યાં ખામી છે?"	"આ ખામીનો લાભ લઈને સિસ્ટમમાં પ્રવેશ મળી શકે?"
Diagnostic Test	Practical Attack Simulation

VA એટલે ડૉક્ટર દ્વારા શરીરની તપાસ કરીને બીમારી શોધવી.

PT એટલે ડૉક્ટર દ્વારા તપાસવું કે આ બીમારી કેટલી ગંભીર છે અને તેનાથી કેટલું નુકસાન થઈ શકે.

બેંકની તમામ Internet Facing Website, Mobile Banking App, Servers અને Network Components નું સમયાંતરે VA/PT કરવું.

- નવી સિસ્ટમ શરૂ કરતાં પહેલાં
- સિસ્ટમ અમલમાં મૂક્યા પછી
- મોટા ફેરફાર પછી
- સમગ્ર જીવનચક્ર દરમિયાન

Critical Applications અને DMZ માં રહેલી સિસ્ટમનું VA દર 6 મહિને ઓછામાં ઓછું એક વખત કરવું.

Penetration Testing (PT) વર્ષે ઓછામાં ઓછું એક વખત કરવું.

બેંકે પોતાની તમામ મહત્વપૂર્ણ IT સિસ્ટમની નિયમિત સુરક્ષા તપાસ કરાવવી. ખાસ કરીને: Internet Banking, Mobile Banking, CBS, ATM Switch, Web Server, Firewall, DMZ Server, માં રહેલી સુરક્ષા ખામીઓ સમયાંતરે શોધવી.

નવી Cyber Vulnerabilities દરરોજ શોધાય છે. આજે સુરક્ષિત લાગતી સિસ્ટમ 6 મહિના પછી જોખમી બની શકે.

તેથી એક વખત Security Audit કરાવવી પૂરતી નથી.

"VA/PT એ બેંકનું નિયમિત Health Check-up છે. સમયસર તપાસ કરશો તો મોટી Cyber બીમારી અટકાવી શકાય."

"Hacker પહેલાં Vulnerability શોધે તે પહેલાં આપણે શોધી લઈએ, એ જ VA/PT નો હેતુ છે."

5.2 CBS-ASP RBI Requirement: UCBs having their CBS on a shared infrastructure of an Application Service Provider (CBS-ASP) shall get their CBS application including the infrastructure hosting it subjected to VA/PT through the CBS-ASP.

જો CBS કોઈ Application Service Provider (CBS-ASP) ના Shared Infrastructure પર હોસ્ટ થયેલું હોય,

તો તે CBS Application અને Hosting Infrastructure નું VA/PT CBS-ASP દ્વારા કરાવવું જરૂરી છે.

ઘણી UCB પોતાનું CBS પોતાના Data Centre માં ચલાવતી નથી.તે CBS Vendor ના Data Centre પર ચાલે છે.

એવા કિસ્સામાં CBS Vendor એ CBS Application, Server, Database, Hosting Infrastructure, બધાનું VA/PT કરાવવું જરૂરી છે. Outsourcing કરવાથી જવાબદારી સમાપ્ત થતી નથી. સુરક્ષાની અંતિમ જવાબદારી બેંકની જ રહે છે. ABC Bank નું CBS XYZ Technologies ના Data Centre પર ચાલે છે. Vendor VA/PT કરાવે છે.પરંતુ તે Report Bank ના Board અને IT Committee સમક્ષ રજૂ થવી જોઈએ. CBS Vendor પાસે હોસ્ટ થયેલું હોય તો પણ Cyber Security ની જવાબદારી અંતે બેંકની જ રહે છે."

5.3 Application Security Testing: Application security testing of web/mobile applications should be conducted before going live and after every major changes in the applications.

નવી Website અથવા Mobile Banking App Live કરતાં પહેલાં Security Testing કરવી. મોટા Upgrade પછી ફરી Security Testing કરવી. ઉદાહરણ: નવી Mobile Banking App માં UPI Module ઉમેરવામાં આવ્યું. તે સીધું Live કરવું નહીં. પહેલા: Security Testing, VA/PT, User Acceptance Testing (UAT), પછી જ Live કરવું.

"Testing વગર Software ને Live કરવું એટલે બ્રેક ચેક કર્યા વગર કાર ચલાવવી."

5.4 Vulnerabilities નું Remediation: The vulnerabilities detected are to be remedied promptly in terms of the UCB's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

VA/PT દરમિયાન મળેલી ખામીઓ સમયસર દૂર કરવી. માત્ર Report તૈયાર કરવી પૂરતી નથી. ઘણી બેંકો VA/PT તો કરાવે છે, પણ Report Drawer માં મૂકી દે છે. RBI કહે છે:"ખામી શોધવી પૂરતી નથી, તેને સુધારવી પણ જરૂરી છે."

"VA Report પુસ્તક નથી કે શેલ્ફમાં મૂકી દઈએ; તે Action Plan છે."

5.5 Professionally Qualified Teams: Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Top Management.

PT માત્ર Qualified Ethical Hackers દ્વારા જ કરાવવું. RBI આ શા માટે કહે છે? Penetration Testing એ અત્યંત Technical કામ છે. અનુભવ વગર Testing કરવાથી ખામીઓ રહી જાય, ખોટા નિષ્કર્ષ આવે, સિસ્ટમને નુકસાન પણ થઈ શકે.

પછી શું કરવું?

PT Report→ Information Security Team → IT Audit Team → Top Management → Compliance →Closure

What Auditor should check?

VA Report છે? PT Report છે? Reports કેટલા સમયની છે? Critical Vulnerabilities બંધ કરવામાં આવી? Closure Report છે? Board/IT Strategy Committee સમક્ષ રજૂ થઈ? Vendor દ્વારા કરાયેલ VA/PT Report ઉપલબ્ધ છે?

VA/PT નો સંપૂર્ણ Flow

Website / Mobile App / CBS → Vulnerability Assessment (VA) → ખામીઓ મળી → Risk Rating

(Critical / High / Medium / Low) → Remediation → Re-testing→ Penetration Testing → Management Review →Closure

"VA/PT એ Compliance માટેનો ખર્ચ નથી; તે Cyber Attack સામેનું વીમા (Insurance) છે. લાખો રૂપિયાનો હુમલો સમયસર કરાયેલા VA/PT દ્વારા અટકાવી શકાય છે."

"Cyber Security માં સૌથી સસ્તું કામ Vulnerability શોધવાનું છે; સૌથી મોંઘું કામ Hacker હુમલો કર્યા પછી નુકસાન ભરપાઈ કરવાનું છે."

"VA આપણને ખામી બતાવે છે, PT બતાવે છે કે Hacker તે ખામીનો ખરેખર ઉપયોગ કરી શકે છે કે નહીં."

RBI માત્ર VA/PT Report માંગતું નથી; RBI એ પણ જુએ છે કે Report માં દર્શાવેલી દરેક ગંભીર ખામી સમયસર દૂર કરવામાં આવી છે કે નહીં."

6. User Access Control / Management

6.1 RBI Requirement

Provide secure access to the UCB's assets/services from within/outside UCB's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.)

બેંકના તમામ IT સાધનો, સિસ્ટમો અને સેવાઓનો ઉપયોગ બેંકની અંદરથી (Internal Network) અથવા બહારથી (Remote Access) કરવામાં આવે ત્યારે માહિતી સંપૂર્ણપણે સુરક્ષિત રહે તે માટે યોગ્ય સુરક્ષા વ્યવસ્થા હોવી જોઈએ.

માહિતીની સુરક્ષા બે રીતે કરવી જરૂરી છે:

(A) Data at Rest: જે માહિતી Server, Desktop, Laptop, Mobile અથવા Database માં સંગ્રહિત (Stored) છે.

(B) Data in Transit: જે માહિતી એક સ્થળેથી બીજા સ્થળે મોકલાઈ રહી છે.

Data at Rest એટલે શું?

જે માહિતી હાલ ક્યાંક "પડી" છે (Stored છે) તેને Data at Rest કહે છે. ઉદાહરણ: CBS Database, Customer KYC, Fixed Deposit Records, Loan Files, HR Database, Backup Files, Pen Drive, Laptop Hard Disk

RBI શું કહે છે? આ માહિતી Encrypt કરવી.અર્થાત જો Laptop ચોરાઈ જાય, તો પણ કોઈ Data વાંચી ન શકે.

"Locker ચોરાઈ જાય તો પણ જો ચાવી ન હોય તો પૈસા સુરક્ષિત રહે છે. Encryption પણ ડિજિટલ લોકરનું તાળું છે."

Encryption એટલે શું? Encryption એટલે Data ને એવી ભાષામાં ફેરવી દેવો જે માત્ર Authorised User જ વાંચી શકે. ઉદાહરણ: Original- Balance = ₹15,25,000 Encrypt થયા પછી X7@4F#K92AB76... હવે પાસવર્ડ વગર કોઈ વાંચી શકશે નહીં.

Data in Transit એટલે શું? એક જગ્યાએથી બીજી જગ્યાએ મોકલાતી માહિતી. ઉદાહરણ: Branch→CBS Server અથવા Customer Mobile →Internet Banking→ CBS અથવા ATM →Switch CBS

RBI શા માટે કહે છે? જો Data રસ્તામાં Encrypt ન હોય તો Hacker વચ્ચેથી Data ચોરી શકે. આને Man-in-the-Middle Attack કહેવામાં આવે છે.

ઉદાહરણ: ગ્રાહક Mobile Banking કરે છે. જો Connection Secure ન હોય તો User ID, Password, OTP, Account Number બધું Hacker જોઈ શકે.

VPN એટલે શું? Virtual Private Network- Internet ઉપર બનાવેલી સુરક્ષિત ખાનગી ટનલ.

ઉદાહરણ : CEO ઘરે બેઠા CBS Access કરે છે. જો સીધા Internet થી Login કરે છે તો જોખમ.જો VPN દ્વારા Login કરે તો આખો Communication Encrypt થાય. સામાન્ય Internet ખુલ્લો હાઇવે છે તો VPN પોલીસ સુરક્ષાવાળો ખાસ માર્ગ.

Secure Protocols એટલે શું?

આધુનિક સુરક્ષિત Communication Standards.જેમ કે HTTPS, TLS, SSH, SFTP, IPSec, VPN

RBI આ શા માટે કહે છે? આજે Hybrid Working, Mobile Banking, Internet Banking, Cloud Services, Vendor Support વધી ગયા છે. બહારથી Login પણ સુરક્ષિત હોવું જોઈએ.

What IS Auditor checks?

Laptop Encryption છે? Database Encryption છે? Backup Encryption છે? VPN Policy છે? Remote Access Log છે? TLS Certificates Valid છે? HTTPS વપરાય છે? USB Encryption છે? Mobile Device Encryption છે?

Best Practices

Full Disk Encryption, Database Encryption, BitLocker, VPN, HTTPS, TLS 1.3, SSH, SFTP, MFA, Auto Session Timeout, Remote Access Monitoring

સામાન્ય ભૂલો: Laptop Encrypt નથી, Database Plain Text માં, VPN વગર Remote Login, Password Email દ્વારા મોકલવો, Public Wi-Fi પરથી CBS Access, Customer Data USB માં Copy કરવો

"માહિતી બે વખત સૌથી વધુ જોખમમાં હોય છે—જ્યારે તે સંગ્રહિત હોય અને જ્યારે તે એક જગ્યાએથી બીજી જગ્યાએ જઈ રહી હોય. RBI બંને સ્થિતિમાં સુરક્ષા ફરજિયાત બનાવે છે."

"Encryption એટલે ડિજિટલ તાળું. Laptop ચોરાઈ શકે, Hard Disk ખોવાઈ શકે, પરંતુ Encryption હોય તો માહિતી સુરક્ષિત રહે છે."

"VPN વગર જાહેર Internet પરથી CBS Access કરવું એ ખુલ્લા રસ્તે લાખો રૂપિયા લઈને ચાલવા જેવું છે."

બેંકની સૌથી કિંમતી સંપત્તિ હવે Cash નથી, પરંતુ Data છે. તેથી Data સુરક્ષિત રાખવું એ બેંકની પ્રથમ જવાબદારી છે."

યાદ રાખવાનું સૂત્ર: "3E + 2A Rule"

Encrypt → Every → Everywhere

- **At Rest → Encryption**

- **In Transit → Encryption**
- **Remote Access → VPN + MFA**

7. Authentication Framework for Customers

7.0 RBI Requirement

UCBs should have adequate checks and balances to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine/authorised applications and that authentication methodology is robust, secure and centralised.

7.1 બેંકે એવી સુરક્ષિત અને મજબૂત **Customer Authentication System** અમલમાં મૂકવી જોઈએ કે જેથી:

- માત્ર સાચા **(Genuine)** ગ્રાહક જ પોતાના ખાતામાં પ્રવેશ કરી શકે.
- માત્ર બેંકની અધિકૃત **(Authorised) Mobile App** અથવા **Website** મારફતે જ વ્યવહાર થઈ શકે.
- ગ્રાહકોના **Login Credentials (User ID, Password, MPIN, OTP** વગેરે**)** સુરક્ષિત રહે.
- સમગ્ર **Authentication** પ્રક્રિયા કેન્દ્રીય **(Centralised),** વિશ્વસનીય અને સુરક્ષિત હોય.

7.1.2 Authentication એટલે શું**?**

7.1.3 Authentication એટલે કોઈ વ્યક્તિ ખરેખર તે જ વ્યક્તિ છે કે નહીં તેની ઓળખની ખાતરી કરવાની પ્રક્રિયા.

સરળ શબ્દોમાં: **"**જે વ્યક્તિ **Login** કરે છે તે ખરેખર અધિકૃત ગ્રાહક જ છે કે નહીં તેની ચકાસણી કરવી એટલે **Authentication."**

Authentication ના સામાન્ય ઉદાહરણો- ગ્રાહક **Internet Banking** માં **Login** કરે ત્યારે**, Customer ID, Password, OTP** આ ત્રણેય મળ્યા પછી જ **Login** થાય.આ જ **Authentication** છે.

Mobile Banking માં **MPIN, Fingerprint, Face Recognition** આ પણ **Authentication** છે.

7.1.4 Authentication અને **Authorization** વચ્ચેનો તફાવત

Authentication	**Authorization**
તમે કોણ છો?	તમે શું કરી શકો છો?
ઓળખની ચકાસણી	અધિકારની ચકાસણી
Password, OTP	**Fund Transfer, View Only** વગેરે

ઉદાહરણ: **Login** સફળ થયું = **Authentication ,** **₹5** લાખ સુધી **RTGS** કરવાની મંજૂરી = **Authorization**

7.1.5 RBI "Checks and Balances" શા માટે કહે છે**?**

માત્ર **Password** પર આધાર રાખવો પૂરતો નથી. એક કરતાં વધુ સુરક્ષા સ્તરો હોવા જોઈએ. ઉદાહરણ: **Strong Password, OTP, Device Binding, Risk Based Authentication, Session Timeout, Transaction Limit, Behaviour Monitoring**

7.1.6 **Customer Credentials શું છે?**

ગ્રાહકની ગુપ્ત માહિતી: Customer ID, Login Password, Transaction Password, MPIN, OTP, Debit Card PIN, Biometric, Security Questions. આ બધી માહિતી અત્યંત સુરક્ષિત રીતે રાખવી જરૂરી છે.

7.1.7 **RBI આ શા માટે કહે છે?**

જો Login Credentials ચોરાઈ જાય તો Fraudster Login કરી શકે, પૈસા ટ્રાન્સફર કરી શકે, Password બદલી શકે, Loan લઈ શકે. તેથી Credentials ની સુરક્ષા ખૂબ જ મહત્વપૂર્ણ છે.

7.1.8 "Authentication નો અર્થ માત્ર Login કરાવવાનો નથી, પરંતુ સાચો ગ્રાહક જ Login કરે તેની ખાતરી કરવાનો છે."

"Password જાણવો એટલે ગ્રાહક બની જવું નહીં; બેંકે અનેક સ્તરની ઓળખ ચકાસવી જોઈએ."

7.1.9 **Robust Authentication એટલે શું?**

RBI Robust એટલે મજબૂત Authentication કહે છે. તેમાં હોઈ શકે, Strong Password, OTP, Multi-Factor, Authentication (MFA, Device Binding, Biometric, Risk Based Authentication, Transaction Authentication

7.1.10 **Centralised Authentication એટલે શું?**

બેંકની તમામ Digital Services માટે એક જ સુરક્ષિત Authentication System હોવી જોઈએ. ઉદાહરણ: Internet Banking, Mobile Banking, Corporate Banking. બધામાં અલગ અલગ Login System ન હોવી જોઈએ.

7.2 **RBI Requirement**

Implement authentication framework/mechanism to securely verify and identify the applications of UCB to customers (Example: Digital Certificate).

બેંકે એવી વ્યવસ્થા કરવી જોઈએ કે ગ્રાહક પણ ખાતરી કરી શકે કે "હું ખરેખર મારી બેંકની અધિકૃત Website અથવા Mobile App નો જ ઉપયોગ કરી રહ્યો છું."

7.2.1 **RBI આ શા માટે કહે છે?**

આજકાલ Hacker બેંક જેવી જ દેખાતી Website બનાવી દે છે.ઉદાહરણ: સાચું www.abcbank.co.in ખોટું

www.abcbank-secure.com ગ્રાહકને તફાવત સમજાતો નથી.

7.2.2 **Digital Certificate શું છે?**

Digital Certificate એટલે Website નું Digital Identity Card.જેમઆધાર કાર્ડથી વ્યક્તિની ઓળખ થાય,તેમ

Digital Certificate થી Website ની ઓળખ થાય.

7.2.3 **HTTPS અને Lock Symbol**

Browser માં🔒 Lock Symbol અને https:// જો દેખાય તો Website પાસે સામાન્ય રીતે માન્ય SSL/TLS Digital Certificate હોય છે. તેનો અર્થ:

- **Website ની ઓળખ ચકાસવામાં આવી છે.**
- **Browser અને Website વચ્ચેનો Data Encrypt થાય છે.**

7.2.4 What Auditor should check?

MFA અમલમાં છે? Password Policy મજબૂત છે? OTP સુરક્ષિત છે? SSL Certificate Valid છે? Expired Certificate તો નથી? Customer Credentials Encrypt થયેલ છે? Failed Login Monitoring થાય છે? Brute Force Protection છે? Session Timeout છે? Device Registration છે?

Authentication Flow → Customer → User ID→ Password→ OTP / Biometric→ Authentication Server→ Successful Verification → Access Granted

Website Authentication Flow→ Customer Browser→ HTTPS Request→ Digital Certificate Verification→ Certificate Valid→ Encrypted Connection → Secure Banking

7.2.5 "Authentication એટલે ગ્રાહકની ઓળખની ચકાસણી અને Digital Certificate એટલે બેંકની ઓળખની ચકાસણી."

"ગ્રાહક બેંક પર વિશ્વાસ કરે છે, પરંતુ પહેલાં ખાતરી કરવી જોઈએ કે તે ખરેખર બેંકની જ Website અથવા Mobile App સાથે જોડાયેલો છે."

"Cyber Security માં વિશ્વાસ (Trust) શબ્દ પૂરતો નથી; દરેક ઓળખની ચકાસણી (Verification) જરૂરી છે."

"RBI નો હેતુ માત્ર ગ્રાહકની ઓળખ ચકાસવાનો નથી, પરંતુ ગ્રાહક પણ ખાતરી કરી શકે કે તે સાચી બેંક સાથે જ જોડાયેલો છે. એટલે બંને તરફની ઓળખ (Mutual Trust through Authentication) જરૂરી છે."

ઘણા અધિકારીઓ Authentication અને Authorization ને એક જ સમજે છે, જ્યારે તે અલગ છે:

- **Authentication = "તમે કોણ છો?" (Identity Verification)**
- **Authorization = "તમને શું કરવાની મંજૂરી છે?" (Permission/Access Rights)**

8.1 RBI Requirement

Subscribe to Anti-phishing / Anti-Rogue Application services from external service providers for identifying and taking down phishing websites / rogue applications. **છેલ્લા કેટલાક વર્ષોમાં મોટાભાગની બેંકિંગ છેતરપિંડી Phishing Websites અને Fake Mobile Apps દ્વારા થઈ રહી છે. તેથી RBI એ આ નિયંત્રણ ફરજિયાત બનાવ્યું છે.**

8.2 બેંકે એવી વિશેષ Cyber Security Service લેવી જોઈએ કે જે:

- બેંકના નામે બનાવવામાં આવેલી **નકલી Website (Phishing Website)** શોધી શકે.
- બેંકના નામે બનાવવામાં આવેલી **નકલી Mobile Apps (Rogue Applications)** શોધી શકે.
- આવી Website અથવા App ને શક્ય તેટલી ઝડપથી **બંધ (Take Down)** કરાવી શકે.

8.3 Phishing Website એટલે શું?

Phishing Website એ એવી નકલી Website છે જે સાચી બેંકની Website જેવી જ દેખાય છે. ઉદાહરણ: સાચી Website: **www.abcbank.co.in** Fraudster બનાવે: **www.abcbank-india.com** અથવા **www.abcbannk.co.in** અથવા **www.abcbanksecure.in**, ગ્રાહકને લાગે કે આ સાચી Website છે.

8.4 Rogue Application એટલે શું?

Rogue Application એટલે બેંકની અધિકૃત Mobile Banking App જેવી દેખાતીનકલી Mobile App. ઉદાહરણ: Google Play Store બહાર APK File રૂપે મોકલવામાં આવે.ગ્રાહક તેને Install કરે, પછી User ID, Password, MPIN, OTP, બધું Fraudster પાસે પહોંચી જાય.

8.5 Anti-Phishing Service શું કરે?

આ સેવા આખા Internet પર સતત શોધ કરે છે. તે તપાસે છે:

- બેંકના નામે કોઈ નકલી Website છે?
- કોઈએ બેંકનું Logo વાપર્યું છે?
- કોઈ Fake Mobile App બનાવ્યું છે?
- કોઈ Domain ગ્રાહકોને છેતરવા માટે Register થયું છે?

8.6 RBI આ શા માટે કહે છે?

આજના સમયમાં Hacker બેંકના Server પર હુમલો ઓછો કરે છે.તેના બદલે ગ્રાહકને છેતરે છે.કારણ કે ગ્રાહકને છેતરવું બેંક Hack કરવા કરતાં સરળ છે.

ઉદાહરણ : ABC Urban Co-operative Bank ની સાચી Website www.abcbank.co.in છે.Fraudster www.abcbank-help.in બનાવે છે. Google Search માં Advertisement આપે. ગ્રાહક ત્યાં Login કરે. Customer ID, Password, OTP, બધું Hacker પાસે જાય.

8.7 Anti-Phishing Provider શું કરશે?

Website શોધશે, Risk Analyse કરશે, Registrar ને Notice મોકલશે, Hosting Company ને ફરિયાદ કરશે, Website બંધ કરાવશે. આને **Take Down Process** કહે છે.

8.8 Rogue Mobile App Example: Fraudster ABC Bank Mobile.apk નામથી App બનાવે છે. Play Store બહાર WhatsApp દ્વારા મોકલે છે. ગ્રાહક Install કરે છે. તે પછી OTP, SMS, Password, બધું Hacker પાસે જાય છે.

8.9 Anti-Rogue Application Service શું કરે?

Fake Apps શોધે. Play Store Monitor કરે. App Store Monitor કરે. Fake APK શોધે. Google ને Report કરે. App Remove કરાવે.

8.10 RBI "Take Down" શા માટે કહે છે?

માત્ર Website શોધવી પૂરતી નથી. તે બંધ પણ કરાવવી જોઈએ. જેટલો વધુ સમય Website ચાલુ રહેશે, તેટલા વધુ ગ્રાહકો છેતરાશે.

8.11 What Auditor should check?

IS Auditor પૂછશે: Anti-Phishing Service લીધી છે? Fake Domain Monitoring થાય છે? Brand Monitoring થાય છે? Fake App Detection થાય છે? છેલ્લા વર્ષમાં કેટલા Fake Domains મળ્યા? કેટલા બંધ કરાવ્યા? Incident Report છે? Customer Awareness Campaign થાય છે?

"આજનો Hacker બેંકની તિજોરી તોડતો નથી; તે બેંક જેવી દેખાતી Website બનાવીને ગ્રાહકનો વિશ્વાસ તોડે છે."

"સાયબર સુરક્ષા માત્ર પોતાની Website સુરક્ષિત રાખવાથી પૂર્ણ થતી નથી. Internet પર આપણા નામે કોઈ નકલી Website કે App ચાલી રહી નથી તેની સતત દેખરેખ પણ એટલી જ જરૂરી છે."

"Phishing Website શોધવી એ પ્રથમ પગલું છે, પરંતુ તેને ઝડપથી બંધ કરાવવું (Take Down) એ જ સાચી Cyber Security છે."

"બેંકના દરવાજા પર ચોકીદાર રાખવો પૂરતો નથી. જો કોઈ વ્યક્તિ બેંકના નામે સામે જ નકલી શાખા ખોલી દે તો તેને પણ તરત બંધ કરાવવી પડે. Internet પરની Phishing Website અને Rogue Mobile App એ આવી જ 'નકલી શાખાઓ' છે."

"આજના સમયમાં સાયબર સુરક્ષા માત્ર Firewall સુધી મર્યાદિત નથી; Internet પર બેંકના નામ અને પ્રતિષ્ઠાનું રક્ષણ કરવું પણ એટલું જ જરૂરી છે."

9. Data Leak Prevention Strategy

9.1 RBI Requirement

Develop and implement a comprehensive Data Loss/Leakage Prevention (DLP) Strategy to safeguard sensitive (including confidential) business and customer data/information.

બેંકે એવી વ્યાપક **Data Loss Prevention (DLP) Strategy** તૈયાર કરી અને અમલમાં મૂકવી જોઈએ કે જેથી બેંકનો ગોપનીય અને સંવેદનશીલ ડેટા કોઈપણ રીતે ચોરાઈ, લીક થાય અથવા અનધિકૃત વ્યક્તિ સુધી પહોંચે નહીં.

9.1.1 Data Leak એટલે શું?

Data Leak એટલે બેંકની ગોપનીય માહિતી બેંકની બહાર અનધિકૃત રીતે પહોંચી જવી. આ માહિતી ઇરાદાપૂર્વક અથવા અજાણતા પણ બહાર જઈ શકે છે.

9.1.2 Data Leak કેવી રીતે થઈ શકે?

Email દ્વારા, USB Pen Drive દ્વારા , WhatsApp દ્વારા, Personal Gmail પર મોકલીને, Cloud Storage (Google Drive, Dropbox વગેરે) દ્વારા, Print કાઢીને, Mobile Camera થી ફોટો પાડી, Hacker દ્વારા, અસંતુષ્ટ કર્મચારી દ્વારા,

9.1.3 Sensitive Data એટલે શું?

બેંકનો એવો ડેટા કે જે બહાર જાય તો ગ્રાહકો, બેંક અથવા RBI માટે ગંભીર જોખમ ઊભું થાય.

ઉદાહરણ: **Customer Data-** નામ, આધાર નંબર, PAN નંબર, મોબાઇલ નંબર, સરનામું, KYC Documents, Account Number, Transaction History

Business Data- Board Agenda, Audit Report, Inspection Report, Loan Sanction Notes, Interest Rate Strategy, Password Policy, Internal Circulars, Cyber Security Reports

Confidential Data- Passwords, Encryption Keys, Server Configuration, Firewall Rules, Network Diagram

9.1.4 RBI આ શા માટે કહે છે?

આજે Hacker નો મુખ્ય હેતુ: **Data is the New Currency,** ઘણી વખત Hacker પૈસા નથી ચોરતો પણ Customer Database ચોરી જાય છે. પછી Black Market માં વેચે છે, Phishing કરે છે, Identity Theft કરે છે, Loan Fraud કરે છે

Example: એક કર્મચારી Loan Accounts ની Excel File પોતાના Gmail પર ઘરે કામ કરવા માટે મોકલે છે. તેનું Gmail Hack થઈ જાય. હજારો ગ્રાહકોનો Data Internet પર આવી જાય.આને Data Leakage કહે છે.

9.1.5 Data Leak Prevention Strategy માં શું હોવું જોઈએ?

1. Data Classification: બધા Data ને વર્ગીકૃત કરો. જેમ કે: Public, Internal, Confidential, Highly Confidential

2. Access Control: જેને જરૂર હોય તેને જ Data જોવા મળે.

3. Encryption: Data Server માં Store હોય ત્યારે Encrypt કરવો.

4. Encryption During Transmission: Email, VPN, HTTPS, SFTP દ્વારા મોકલવો.

5. USB Control: USB Pen Drive બંધ રાખવી.

6. Email Control: Sensitive Data Personal Gmail પર મોકલી ન શકાય.

7. Printing Control: Sensitive Documents ની Printing Monitor કરવી.

8. Cloud Control: Google Drive, Dropbox, OneDrive, પર Upload ની મંજૂરી નિયંત્રિત કરવી.

9. Monitoring: કોણે કયો Data Copy કર્યો? કોણે Email કર્યો? કોણે Download કર્યો? બધું Monitor કરવું.

9.1.6 Data Leak Prevention (DLP) Software શું કરે?

જો કોઈ કર્મચારી 1000 Customer Records USB માં Copy કરવાનો પ્રયત્ન કરે તો Software તરત Block કરી દેશે.

જો કોઈ PAN Data Email દ્વારા બહાર મોકલે તો Alert Generate થશે.

9.1.7 RBI "Comprehensive Strategy" શા માટે કહે છે?

માત્ર Software ખરીદવાથી કામ નહીં ચાલે. Policy, Technology, People, Training, Monitoring, Audit, બધું મળીને DLP બને છે.

9.2 Vendor Managed Facilities

RBI Requirement

Similar arrangements need to be ensured at Vendor Managed Facilities also.

GUJFED

જો બેંકની IT સિસ્ટમ Vendor, CBS-ASP, Cloud, Data Centre, દ્વારા સંચાલિત થતી હોય તો ત્યાં પણ Data Leak Prevention ની સમાન વ્યવસ્થા હોવી જોઈએ.

9.2.1 RBI આ શા માટે કહે છે?

Outsourcing કરવાથી જવાબદારી પૂરી થતી નથી. Customer Data Vendor પાસે હોયતો પણ તેની સુરક્ષા માટે બેંક જ જવાબદાર છે.

Example: CBS Vendor પાસે 10 લાખ Customer Records છે. Vendor ના કર્મચારીએ Data Copy કરી દીધો. જવાબદાર કોણ? RBI અનુસાર **બેંક પણ જવાબદાર છે.**

9.2.2 Vendor Agreement માં શું હોવું જોઈએ?

NDA, Encryption, Access Control, Audit Rights, Data Backup, Data Deletion, Data Return Policy, Incident Reporting, Cyber Security Audit

9.2.3 What Auditor should ask?

DLP Policy છે? Data Classification છે? Encryption છે? USB Block છે? Email Monitoring છે? Cloud Upload Control છે? Vendor પાસે DLP છે? DLP Alerts Monitor થાય છે? Data Leak Incident Register છે?

9.2.4 DLP Process

Sensitive Data→ Classification→ Access Control→ Encryption → Monitoring → Email / USB / Cloud Check → Leak Attempt→ DLP Software Detect→ Block→ Alert→ Investigation

9.2.5 "આજના સમયમાં બેંકની સૌથી મૂલ્યવાન સંપત્તિ તેની ઇમારત કે ફર્નિચર નહીં, પરંતુ ગ્રાહકોનો ડેટા છે."

"સાયબર સુરક્ષા એટલે માત્ર Hacker ને રોકવું નહીં; બેંકનો ડેટા ખોટા હાથમાં ન જાય તેની ખાતરી કરવી પણ એટલી જ મહત્વપૂર્ણ છે."

9.2.6 "એક Customer નો આધાર નંબર, PAN અને મોબાઇલ નંબર પણ Cyber Criminal માટે સોનાથી વધુ કિંમતી હોઈ શકે છે."

"Outsourcing કરી શકાય છે, પરંતુ જવાબદારી Outsource કરી શકાતી નથી. Vendor પાસે રહેલો ગ્રાહકનો ડેટા પણ બેંકની જ જવાબદારી છે."

યાદ રાખવાનું સૂત્ર

"Protect Data, Protect Customer, Protect Reputation."

10. Audit Logs

10.1 RBI Requirement

Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

બેંકની તમામ મહત્વપૂર્ણ IT સિસ્ટમમાં વપરાશકર્તાઓ (Users) દ્વારા કરવામાં આવેલી દરેક મહત્વપૂર્ણ પ્રવૃત્તિ (User Activity) ની **સ્વયંસંચાલિત નોંધ (Audit Log)** રાખવી જોઈએ. જો ભવિષ્યમાં કોઈ Cyber Fraud અથવા Cyber Attack થાય, તો આ Audit Logs ના આધારે તેની તપાસ (Forensic Investigation) કરી શકાય.

10.1.1 Audit Log એટલે શું?

Audit Log એટલે **કોણે? ક્યારે? કયા Computer પરથી? શું કર્યું?** તેનો આપોઆપ તૈયાર થતો રેકોર્ડ. **"Audit Log એ IT સિસ્ટમની ડિજિટલ ડાયરી (Digital Diary) છે."**

10.1.2 Audit Log માં શું નોંધાય? ઉદાહરણ- Login, Logout, Failed Login, Password બદલવો, Customer Account જોવું, Transaction કરવી, Loan Approval, Interest Rate બદલવો, User Creation, User Deletion, ATM Switch Access, Database Access, Firewall Configuration Change, etc.

ઉદાહરણ: Date : 10-07-2026, Time : 10:15 AM, User ID : BM001, Branch : Paldi Branch, Activity : Cash Credit Limit Approved, Amount : ₹10,00,000, IP Address : 10.20.15.18, Status : Successful, આ જ Audit Log છે.

10.1.3 RBI આ શા માટે કહે છે?

જો Fraud થાય તો સૌથી પહેલો પ્રશ્ન પૂછાય છે: કોણે કર્યું? ક્યારે કર્યું? ક્યાંથી Login થયું? કયા User ID થી થયું? કેટલા વાગ્યે થયું? આ બધા જવાબ Audit Log માંથી મળે છે.

10.1.4 **Audit Log ક્યાં ક્યાં રાખવા?**

CBS, Internet Banking, Mobile Banking, ATM, Firewall, Router, Switch, Database, Windows Server, Linux Server, Active Directory, VPN, Email Server.

10.1.5 Forensic Audit શું છે?

Forensic એટલે સાયબર ગુનાની વૈજ્ઞાનિક તપાસ. જેમ Crime Scene પર Fingerprints તપાસવામાં આવે છે તે જ રીતે Cyber Crime માં Audit Logs તપાસવામાં આવે છે.

10.1.6 "Audit Log એ Cyber Crime નું CCTV Camera છે."

"CCTV વગર ચોર શોધવો મુશ્કેલ હોય છે, તેવી જ રીતે Audit Log વગર Cyber Criminal શોધવો લગભગ અશક્ય છે."

10.1.7 Log Retention

Audit Logs કેટલા સમય સુધી રાખવા? તે Policy અનુસાર નક્કી કરવું. ઘણી બેંકો Regulatory Requirement પ્રમાણે રાખે છે.

10.2 RBI Requirement

An alert mechanism should be set to monitor any change in the log settings.

જો કોઈ વ્યક્તિ Audit Log ની Settings માં ફેરફાર કરે, અથવા Logging બંધ કરે, અથવા Log Delete કરવાનો પ્રયત્ન કરે, તો તરત Alert Generate થવો જોઈએ.

10.2.1 RBI આ શા માટે કહે છે?

Hacker નું પ્રથમ કામ શું હોય? પોતાના પુરાવા (Evidence) નષ્ટ કરવાના. તેથી Hacker Log Delete કરે છે. Logging બંધ કરે છે. Log File બદલે છે. RBI કહે છે આવું થાય તો તરત Alert આવવો જોઈએ. **Example:** એક Administrator Logging Disable કરે છે. સિસ્ટમ તરત IT Security Team ને Email મોકલે છે. અથવા SMS Alert આપે છે.

10.2.2 **Alert ક્યારે આવવો જોઈએ?**

Logging બંધ થાય, Log File Delete થાય, Log Size અચાનક ઘટે, Time બદલે, Log Retention Policy બદલાય, Audit Configuration બદલાય, **SIEM નો ઉપયોગ,** મોટી બેંકો SIEM (Security Information and Event Management) વાપરે છે. SIEM બધા Logs એક જગ્યાએ ભેગા કરે છે. અને શંકાસ્પદ ઘટના થાય તો તરત Alert આપે.

10.2.3 What Auditor will ask?

Audit Logging Enabled છે? Logs Tamper Proof છે? Logs Delete કરી શકાય? Failed Login Logs છે? Admin activities Log થાય છે? Log Review થાય છે? SIEM છે? Log Retention Policy છે? Alert Mechanism છે? શું Logs ની **દૈનિક અથવા નિયમિત સમીક્ષા** થાય છે? Critical Events પર **Alert** આવે છે? મળેલા Alerts પર સમયસર **કાર્યવાહી** થાય છે? Audit Logs નો ઉપયોગ **Fraud Detection** અને **Cyber Incident Investigation** માટે થાય છે?

10.2.4 "Audit Log એ બેંકની IT સિસ્ટમનું CCTV Camera છે. Camera બંધ હશે, Recording જ નથી, **તો ગુનેગાર શોધવો મુશ્કેલ બની જશે."**

"Cyber Security માં સૌથી મહત્વનો પુરાવો Audit Log છે. તેથી તેને સુરક્ષિત રાખવો અને તેની સાથે કોઈ ચેડાં ન થાય તેની સતત દેખરેખ રાખવી જરૂરી છે."

"જો Hacker સૌથી પહેલાં કોઈ વસ્તુ નષ્ટ કરવાનો પ્રયત્ન કરે તો તે Audit Logs છે, કારણ કે તેમાં તેના ગુનાના પુરાવા હોય છે."

"Audit Logs માત્ર Record નથી; તે Cyber Security નું Evidence, Monitoring Tool અને Investigation નો આધારસ્તંભ છે."

11. Incident Response and Management

11.1 RBI Requirement

Put in place an effective Incident Response Programme. UCBs must have a mechanism/resources to take appropriate action in case of any cyber security incident. They must have written Incident Response Procedures including the roles of staff/outsourced staff handling such incidents.

Cyber Attack થશે કે નહીં તે આપણા હાથમાં નથી, પરંતુ હુમલો થયા પછી આપણે કેટલી ઝડપથી અને અસરકારક રીતે પ્રતિસાદ આપીએ છીએ તે આપણા હાથમાં છે. આ જ Cyber Resilience નો આધાર છે.

11.1.2 દરેક UCB પાસે **Cyber Security Incident Response Programme** હોવો જોઈએ.

જો કોઈ Cyber Security ઘટના બને, તો બેંક પાસે:

- તરત કાર્યવાહી કરવાની વ્યવસ્થા હોવી જોઈએ.
- જરૂરી સાધનો (Resources) ઉપલબ્ધ હોવા જોઈએ.
- લેખિત **Incident Response Procedure (SOP)** હોવી જોઈએ.
- કોણ શું કરશે તેની જવાબદારીઓ સ્પષ્ટ હોવી જોઈએ.
- Vendor અથવા Outsourced Staff ની જવાબદારીઓ પણ નક્કી કરેલી હોવી જોઈએ.

11.1.3 Incident એટલે શું?

Incident એટલે કોઈપણ એવી ઘટના જે બેંકની માહિતી, સિસ્ટમ અથવા સેવાઓની સુરક્ષાને અસર કરે.

ઉદાહરણ: Ransomware Attack, Phishing Attack, Malware Infection, ATM Hacking, CBS Server Crash, Data Leakage, Internet Banking બંધ થઈ જવી, Unauthorized Login, DDOS Attack, Customer Data Theft, etc.

11.1.4 Incident Response એટલે શું?

Incident Response એટલે Cyber Attack થયા પછી ઝડપી, વ્યવસ્થિત અને નિયંત્રિત રીતે નુકસાન ઘટાડવાની પ્રક્રિયા. "Incident Response એટલે આગ લાગ્યા પછી ગભરાવું નહીં, પરંતુ Fire Drill મુજબ કામ કરવું."

11.1.5 RBI આ શા માટે કહે છે?

ઘણી બેંકો પાસે Firewall, Antivirus અને Security Software હોય છે. પરંતુ હુમલો થાય ત્યારે:

- કોણ નિર્ણય લેશે?
- કોણ Vendor ને ફોન કરશે?
- RBI ને કોણ જાણ કરશે?
- CERT-In ને કોણ Report કરશે?
- ગ્રાહકોને કોણ માહિતી આપશે?

તે નક્કી નથી હોતું. આથી RBI કહે છે: **"Attack પહેલાં તૈયારી રાખો." Written Incident Response Procedure.** દરેક બેંક પાસે લખેલી SOP હોવી જોઈએ.

11.1.6 Incident Response Programme ના 6 તબક્કા

1. Preparation (તૈયારી)-	હુમલો થાય તે પહેલાં તૈયારી. Policy, SOP, Incident Response Team, Contact List, Training, Cyber Drill
2. Detection (ઓળખ)-	Incident ની ઓળખ કરવી, ઉદાહરણ- Firewall Alert, SIEM Alert, Antivirus Alert Customer Complaint
3. Containment (નિયંત્રણ)	Attack ફેલાય નહીં તે માટે અસરગ્રસ્ત સિસ્ટમને અલગ કરવી. Infected Computer ને Network માંથી Disconnect કરવો.

GUJFED

4. Eradication (સમસ્યા દૂર કરવી)- Malware દૂર કરવું. Password Reset કરવો. Security Patch લગાવવી.

5. Recovery (ફરી કાર્યરત કરવું)- Backup Restore કરવો. CBS ફરી શરૂ કરવું. Internet Banking ચાલુ કરવી.

6. Lessons Learned (શીખવું)- આ હુમલો કેમ થયો? ભવિષ્યમાં કેવી રીતે અટકાવવો?

11.1.7 **Incident Response Team (IRT)**

ટીમમાં સામાન્ય રીતે: CEO, IT Head, Information Security Officer, CBS Vendor Representative, Network Engineer, Legal Officer, Compliance Officer.

"સાયબર હુમલા સમયે સૌથી મોટું જોખમ હુમલો નહીં, પરંતુ ગભરાટ (Panic) છે. Incident Response Plan ગભરાટને નિયંત્રિત કરે છે."

"જે બેંક હુમલા પહેલાં તૈયારી કરે છે, તે હુમલા પછી ઝડપથી ઉભી થઈ શકે છે."

11.2 RBI Requirement:

UCBs are responsible for meeting the requirements prescribed for Incident Management and BCP/DR even if their IT infrastructure, systems or applications are managed by third-party vendors/service providers.

જો બેંકની IT સિસ્ટમ, CBS, Data Centre અથવા Applications કોઈ Vendor સંચાલિત કરતો હોય, તો પણ Incident Management અને BCP/DR માટેની સંપૂર્ણ જવાબદારી બેંકની જ રહેશે.

11.2.1 BCP અને DR શું છે?

BCP (Business Continuity Plan)- કોઈપણ મોટી વિપત્તિ પછી પણ બેંકની જરૂરી સેવાઓ ચાલુ રાખવાની યોજના.

DR (Disaster Recovery)- મુખ્ય Data Centre બંધ થઈ જાય તો બીજા સ્થળેથી સિસ્ટમ ફરી શરૂ કરવાની વ્યવસ્થા.

11.2.2 RBI આ શા માટે કહે છે?

ઘણી બેંકો કહે છે- "CBS Vendor સંભાળે છે." RBI કહે છે: **"Vendor સંભાળી શકે, પરંતુ જવાબદારી બેંકની જ રહેશે."**

Example- બેંકનું CBS Cloud પર છે. Vendor ના Data Centre માં આગ લાગી. CBS બંધ થઈ ગયું. RBI પૂછશે:

DR Site હતી? Recovery Time Objective (RTO) કેટલું હતું? કેટલા સમયમાં સેવા ફરી શરૂ થઈ? ગ્રાહકોને કેવી રીતે સેવા આપી? જવાબદારી Vendor ની નહીં,બેંકની ગણાશે.

11.2.3 Vendor Agreement માં શું હોવું જોઈએ?

Incident Reporting Time, 24×7 Support, Escalation Matrix, BCP Testing, DR Drill, RTO / RPO, Cyber Incident Notification, Audit Rights, SLA

11.2.4 What Auditor will check?

Incident Response Policy છે? Incident Response Team છે? Incident Register છે? CERT-In Reporting થાય છે? Cyber Drill થાય છે? Table-top Exercise થાય છે? BCP Test થાય છે? DR Drill થાય છે? Vendor SLA માં Incident Response છે? ✓ RTO/RPO નિર્ધારિત છે?

11.2.5 Incident Response Flow

Cyber Attack→ Detection→ Incident Declared→ Incident Response Team Activated→ Containment→ Investigation→ Recovery→CERT-In / RBI Reporting→Lessons Learned→ Improved Security Controls

11.2.6 "Vendor પાસે CBS હોસ્ટ કરાવવાથી જવાબદારી પૂરી થતી નથી. RBI ની નજરે ગ્રાહકના ડેટા અને બેંકિંગ સેવાઓ માટે અંતિમ જવાબદારી બેંકના Board અને Management ની જ રહે છે."

Incident Management, Business Continuity અને Disaster Recovery માટે અંતિમ જવાબદારી બેંકની જ રહે છે.

"Prepare Before the Attack, Respond During the Attack, Recover After the Attack, Learn for the Future."

"સાયબર હુમલો અટકાવવો શ્રેષ્ઠ છે; પરંતુ હુમલો થયા પછી ઝડપથી ઊભા થવું એ જ સાચી Cyber Resilience છે."

GUJFED