Prep by . R.Mani, March 2018

Note On Audit of FOREX Transactions

ADVANCES

COMPLIANCE

- ADVANCES- FOREIGN:
- Is Branch in B or C category
- PCs and PCFCs
- FBP/FBN
- PCs: Given against LCs/confirmed orders

  Whether reported in stock statements

  Whether in rupees/ FC

  Whether margin Collected

  Rate of Interest applied be verified

  Overdue PCs,

  How liquidated- export proceeds or domestic

  Ageing of PCs must

  Extension of PCs, ratification

  ECGC notification – validity

- FBP/FBN: Very important to monitor

  Sanction limit, usance period, D & B Reports/ Mira Inform Reports; counter party

  Rate of Interest be verified, discounting charges, etc

  Bill register for exports, export bills submitted beyond 21 days of shipment

- Verify some Bills transactions--- Varun , X Ltd for bogus exports
- Customs portal ---be verified
- Overdue Bills, crystallization, Bills returned unpaid

  How repaid- domestic/ export proceeds

- ECGC notification, SAL
- If period of Bills extended, has ECGC been notified
- Premium paid to ECGC on pre & post shipment on time,

- Bills for collection- status, delay, noting
- Bills for Collection converted to FBP/FBN
- Forward Contracts- booking, cancellation
- Instances where import LCs availed from one bank, but forward contract not booked
- Forward rates- Current card rates taken, whether concession approved by RO
- UHFC : Unhedged Foreign Currency statements are submitted
- Export remittance received in advance- is it more than 1 year, party not exported the goods, what Action branch has taken

Imports:

- Import remittances made:- Bills of entry, how many B/Es are pending
- ICEGATE – portal , Ruchi Soya ----
- More than 50K USD remittance - 2 officers sign, A-2 forms are signed
- Send sample to Customs Dept for authentication--- now done away with
- Massive fraud in B/Entry
- BOB- fraud /failure of internal controls
- XOS returns, & BEF statements
- R-returns, ECB & WOS/JV, ECB returns, FCGPR , Foreign currency held
- Foreign LCs & BGs
- Import LC devolvement, Foreign BG invoked
- LCs containing onerous clauses.
- KYC of NRE /RFC accounts

LOU & LOC: Sanction terms, period, type of material, (since March 14,2018 RBI has banned the issue of LOUs and LOCs) and SBLCs

- SWIFT:
- Swift fields generation of reports from the same which may include remittance opening of lc , buyers credit and sellers credit explanation how buyers credit is created and so also sellers credit
- One should also touch on country wise exposure fixed by bank's on each country .
- NOSTRO accounts remittances and reconciliation and role of ho account reconciliation role of auditors which should include audit of FEX by central statutory auditors
- LFAR auditor of risk management. System auditor of finacle ,swift audit by branch auditor how such proposals are sanctioned and discretionary powers of the same
- Safe keeping of documents of buyers credit when issued and when reversed in the system.
- Role of foreign banks not seeking confirmation of buyers credit when issued for one year by taking RBI approvals red alert when reversed , why and how and not matched with remittances
- Role of external rating agencies in not looking into the financials closely so also internal rating of the borrower in case of Gitanjali Gems when rating was lowest. Diversion of funds .

Modus Operandi: LOUs issued not entered in CBS

- Funds raised through such LOUs were meant to be used for imports bills payment
- However these were fraudulently used for settling the earlier liabilities of Buyer's credit Facilities allowed by Foreign branches of Indian banks
- As regards FLCs they were opened initially for smaller amounts by creating purported Entries in CBS and sending relevant FLCs through SWIFT messaging system
- It was later on fraudulently increased many times (amount) and amendments issued to said FLCs through SWIFT messages and same were not entered in CBS. The foreign branches discounted the Bills of the beneficiary suppliers

SWIFT Mandatory Controls:

1.0 Restrict Internet Access and Segregate Critical Systems from General IT Environment

Operating System Privileged Account Control

Access to local operating system accounts with system-level administrative rights is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, the accounts are restricted from being accessed.

2. Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security

Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT data flows within the secure zone, and its link to the user PCs.

2.2 Security Updates

All hardware and software inside the secure zone and on user PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.

2.3 System Hardening

Security hardening is conducted on all systems and infrastructure within the secure zone and on user PCs.

3. Physically Secure the Environment

3.1 Physical Security

Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

4. Prevent Compromise of Credentials

4.1 Password Policy

All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts.

4.2 Multi-factor Authentication

Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.

5. Manage Identities and Segregate Privileges

5.1 User Account Management

Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties.

5.2 Token Management

Authentication tokens are managed appropriately during issuance, revocation, use, and storage.

6. Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection

Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.

6.2 Software Integrity

A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications.

6.3 Database Integrity

A database integrity check is performed at regular intervals on databases that record SWIFT transactions.

6.4 Logging and Monitoring

Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs.

7.0 Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning

The organization has a defined cyber incident response plan.

7.2 Security Training and Awareness

Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access.

Three critical agencies: Advocate, Valuer, Rating agency

Fourth is: ----------

Compliance returns/ issues at Branch – income tax, GST, uplinking of returns , Legal Audit, etc

Documentation: In CA office be properly addressed to. Very important