ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ
প্রধান কার্যালয়, বিডিবিএল ভবন (লেভেল-১৪)
৮, রাজউক এভিনিউ, ঢাকা-১০০০।
হিউম্যান রিসোর্স ম্যানেজমেন্ট ডিপার্টমেন্ট

তারিখঃ ১৫ পৌষ ১৪২৮ / ৩০ ডিসেম্বর ২০২১

প্রজ্ঞাপন নং- ২৫/২০২১

কর্পোরেশনের পরিচালনা বোর্ডের ১৮.১১.২০২১ তারিখে অনুষ্ঠিত ৬০৪তম সভায় "ICT Audit ম্যানুয়াল" অনুমোদিত হয়েছে। পরিচালনা বোর্ড কর্তৃক অনুমোদিত "ICT Audit ম্যানুয়াল" সকলের অবগতির জন্য এতৎসঙ্গে জারি করা হলো।

০২। কর্পোরেশনের IT কার্যক্রম পরিচালনার ক্ষেত্রে "ICT Audit ম্যানুয়াল" অনুসরণের জন্য অনুরোধ জানানো হলো।

০৩। কর্তৃপক্ষের অনুমোদনক্রমে এ প্রজ্ঞাপন জারি করা হলো।

(বিভাস সাহা)
উপ-মহাব্যবস্থাপক

বিতরণ (জ্যেষ্ঠতার ক্রমানুসারে নয়):

১. সহকারী মহাব্যবস্থাপক/সিনিয়র সিস্টেম এনালিস্ট, আইসিবি।
২. উপ-মহাব্যবস্থাপক/সিস্টেম ম্যানেজার, আইসিবি।
৩. মহাব্যবস্থাপক-এর সচিবালয়, আইসিবি, প্রধান কার্যালয়, ঢাকা।
৪. উপ-ব্যবস্থাপনা পরিচালক-এর সচিবালয়, আইসিবি, প্রধান কার্যালয়, ঢাকা।
৫. ব্যবস্থাপনা পরিচালক-এর সচিবালয়, আইসিবি, প্রধান কার্যালয়, ঢাকা।
৬. চেয়ারম্যান-এর সচিবালয়, আইসিবি, প্রধান কার্যালয়, ঢাকা।
৭. প্রধান নির্বাহী কর্মকর্তা, আইসিবি সাবসিডিয়ারি কোম্পানিসমূহ।
৮. আইসিবি কর্মকর্তা সমিতি, আইসিবি, প্রধান কার্যালয়, ঢাকা।
৯. আইসিবি কর্মচারী ইউনিয়ন, আইসিবি, প্রধান কার্যালয়, ঢাকা।
১০. অফিস কপি।

অনুলিপি (কর্পোরেশনের ওয়েবসাইটে প্রকাশের প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য):

সিনিয়র সিস্টেম এনালিস্ট, প্রোগ্রামিং ডিপার্টমেন্ট, আইসিবি, প্রধান কার্যালয়, ঢাকা।

ICT AUDIT ম্যানুয়াল

ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ

INVESTMENT CORPORATION OF BANGLADESH

ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ

প্রেক্ষাপট

প্রতিটি প্রতিষ্ঠানের সার্বিক কার্যক্রমে জবাবদিহিতা নিশ্চিতকরণের লক্ষ্যে নিরীক্ষা গুরুত্বপূর্ণ ভূমিকা পালন করে। প্রতিষ্ঠান এর প্রয়োজনীয়তার আলোকে যথাসময়ে যথামাত্রায় যথানিয়মাচার পরিপালনপূর্বক সম্পাদিত কার্যাবলী নিরীক্ষার মাধ্যমে যাচাই-বাছাই করা হয়। সাধারণত সম্পাদিত কার্যাবলীতে নিয়ন্ত্রণকারী কর্তৃপক্ষ কর্তৃক প্রজ্ঞাপিত বিধিবিধান/নীতিমালা অনুসরণের বিষয়টি নিরীক্ষা দ্বারা সুষ্ঠু ও সুক্ষ্মভাবে পর্যবেক্ষণ করা হয়ে থাকে। পরিপালন/অনুসরণে নিরীক্ষার বিষয়গুলো পর্যবেক্ষণের জন্য একটি সুনির্দিষ্ট গাইডলাইন প্রয়োজন। উদ্ভাবনী প্রযুক্তি বাস্তবায়ন যে কোন প্রতিষ্ঠানের কর্মকান্ডে ব্যবহৃত প্রক্রিয়াসমূহের দক্ষতা উন্নত করতে এবং প্রাতিষ্ঠানিক সক্ষমতা বৃদ্ধি করতে সহায়তা করলেও, তথ্যপ্রযুক্তিগত দুর্বলতা নিয়ন্ত্রিত পদ্ধতিতে নিয়ন্ত্রণ করা প্রয়োজন। সে লক্ষ্যে প্রতিষ্ঠানের তথ্যপ্রযুক্তি নির্ভর কার্যাবলীর নিয়ন্ত্রণ এবং মূল্যায়নের জন্য ICT AUDIT ম্যানুয়াল এর প্রয়োজন।

ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ ১৯৭৬ সালে যাত্রা শুরুর পর থেকে পুঁজিবাজার উন্নয়ন ও শিল্পোন্নয়নের মাধ্যমে দেশের অর্থনৈতিক উন্নয়নে গুরুত্বপূর্ণ ভূমিকা পালন করে আসছে। সময়ের পরিক্রমায় এ প্রতিষ্ঠানের কার্যক্রম বিস্তৃত হয়েছে এবং একই সাথে আর্থিক কার্যক্রমে ঝুঁকির মাত্রাও বৃদ্ধি পেয়েছে। বর্তমানে বিশ্বব্যপী দক্ষ ঝুঁকি ব্যবস্থাপনা ও উন্নত সেবা-নিশ্চিতকরণে তথ্য ও যোগাযোগ প্রযুক্তি (ICT) ব্যবস্থা খুবই গুরুত্বপূর্ণ যা প্রতিষ্ঠানের ব্যবস্থাপনার মৌলিক উপাদান এবং প্রতিষ্ঠানের কার্যাবলী গতিশীল ও নিরাপদভাবে সম্পাদনে কার্যকর ভূমিকা রাখে। আইসিবির কার্যক্রম পরিচালনায় তথ্য প্রযুক্তি নির্ভরশীলতা ব্যাপকহারে বৃদ্ধি পেয়েছে এবং তথ্য প্রযুক্তির অবিচ্ছিন্ন বিকাশ বিভিন্নভাবে প্রতিষ্ঠানের কাজ করার পদ্ধতিকে বদলে দিয়েছে । বর্তমানে কর্পোরেশনের সুষ্ঠু ব্যবস্থাপনা ও উন্নত সেবা নিশ্চিতকরণে তথ্য প্রযুক্তির ভূমিকা অপরিসীম। তথ্য-প্রযুক্তির সঠিক প্রয়োগ, তথ্য প্রযুক্তিগত অবকাঠামো, নীতি এবং কার্যাবলীর মূল্যায়ণের জন্য তথ্য প্রযুক্তিগত নিরীক্ষা অত্যন্ত অপরিসীম। সে লক্ষ্যে তথ্য প্রযুক্তি নির্ভর কার্যাবলী এবং ঝুঁকি নির্ধারণ সঠিকভাবে যাচাই এবং চিহ্নিত ঝুঁকি হ্রাসকরণের মাধ্যমে কর্পোরেশনের কার্যক্রম গতিশীল, সুশৃঙ্খল ও যুগোপযোগীকরণের লক্ষ্যে "ICT AUDIT ম্যানুয়াল" প্রণয়ন করা হয়েছে । সহজ এবং ঝামেলামুক্ত তথ্য ও যোগাযোগ প্রযুক্তি নির্ভর আর্থিক কার্যক্রম পরিচালনায় আইসিবির রেফারেন্স এবং নির্দেশিকা হিসেবে ম্যানুয়ালটি গুরুত্বপূর্ন ভূমিকা পালন করবে ।

List of Abbreviation /Acronyms

2-FA - Two Factor Authentication
ACL - Access Control List
AC- Audit Committee
ACBOD- Audit Committee of Board of Directors
ADC- Alternative Delivery Channels
ADP- Automated Data Processing
AIPS- Automated Information Processing Systems
AMC - Annual Maintenance Contract
AML - Anti-Money Laundering
ATM- Automated Teller Machine
BCP - Business Continuity Plan
BRP - Backup and Restore Plan
BSEC - Bangladesh Securities and Exchange Commission
CAAT - Computer Assisted Auditing Techniques
CCTV - Close Circuit Television
CDC - Central Data Center
CD ROM - Compact Disk Read Only Memory
CGEIT - Certified in the Governance of Enterprise IT
IT CIA- Certified Internal Auditor/ Confidentiality, Integrity and Availability
CIS- Continuous and Intermittent Simulation
CFSA-Certified Financial Services Auditor
CFE-Certified Fraud Examiner
CISA - Certified Information Systems Auditor
CISM - Certified Information Security Manager
CISSP - Certified Information Systems Security Professional
COB - Close of Business
CRISC - Certified in Risk and Information Systems Control
DC - Data Center
DCFCL - Departmental Control Function CheckList
DNS - Domain Name System
DDoS - Distributed Denial of Service
DOS - Denial of Service
DR - Disaster Recovery

DRP - Disaster Recovery Plan/Database Restore Plan
DRS - Disaster Recovery Site
DSL- Digital Subscriber Link
E-mail - Electronic Mail
EDP - Electronic Data Processing
EoD - End of Day
ICT - Information and Communication Technology
ICTP-ICT Policy
IP - Internet Protocol
IPS - Intrusion Prevention System
IS - Information Systems
ISACA - Information Systems Audit and Control Association
ISDN - Integrated Services Digital Network
IT - Information Technology
ITF-Integrated Test Facility
LAN - Local Area Network
MAN- Metropolitan Area Network
PDA - Personal Digital Assistant
PIN - Personal Identification Number
PKI - Public Key Infrastructure
SAN - Storage Area Network
SCARF/EAM-Systems Control Audit Review File and Embedded Audit Modules
SDLC - Software Development Life Cycle
SLA - Service Level Agreement
SSH - Secured Shell
SSL - Secured Socket Layer
SQL- Structured Query Language
TCP - Transmission Control Protocol
UAT - User Acceptance Test
UPS - Uninterrupted Power Supply
VLAN - Virtual Local Area Network
VPN - Virtual Private Network
WAN - Wide Area Network

ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ
ICT AUDIT ম্যানুয়াল

সূচিপত্র

অধ্যায়-০১

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা (ICT Audit)

১.১। ভূমিকা :

বর্তমান সময়ের আধুনিক, জটিল, উদ্ভাবনী এবং উচ্চ প্রতিযোগীতামূলক পরিবেশে ব্যবসা পরিচালনাকারী কোনো প্রতিষ্ঠানের জন্য তথ্য ও যোগাযোগ প্রযুক্তি (ICT) একটি অত্যন্ত গুরুত্বপূর্ণ প্রাণশক্তি। সমসাময়িক কালে ইন্টারনেট ও ইন্ট্রানেট ব্যবস্থার মাধ্যমে বিশ্বজুড়ে আন্তঃসংযুক্ত এবং ক্রমশ প্রসারমান পরিবেশে বিভিন্নরকম উচ্চমাত্রার সাইবার হুমকিতে থাকা প্রতিনিয়ত ঝুঁকিপুর্ণ পরিস্থিতিতে একটি প্রতিষ্ঠানকে সফলভাবে টিকে থাকার এবং ব্যবসায়িকভাবে অগ্রসর হবার জন্য আধুনিক ও যুগোপযোগী তথ্য ও যোগাযোগ প্রযুক্তি ব্যবস্থা অতীব প্রয়োজনীয় উপাদান।

কর্পোরেশনের বেশিরভাগ কর্মকান্ডই বর্তমানে তথ্য ও যোগাযোগ প্রযুক্তি এর সহায়তায় পরিচালিত হয়ে থাকে। পুর্বের কাগজ ভিত্তিক পদ্ধতির কর্মকান্ড বর্তমানে স্বয়ংক্রিয় তথ্য প্রযুক্তির ব্যবহারের মাধ্যমে অনেকখানি কমে এসেছে। এখন কর্পোরেশনের বেশিরভাগ তথ্যই ইলেক্ট্রনিক পদ্ধতিতে ইনপুট, প্রক্রিয়াকরণ ও সংরক্ষণ করা হয়ে থাকে। কম্পিউটার নেটওয়ার্ক এর মাধ্যমে কম্পিউটার/ডিভাইস সমুহের মধ্যে তথ্যের আদান প্রদান হয়ে থাকে। বর্তমান দুনিয়ায় তথ্য কে ব্যবসার সবচেয়ে গুরুত্বপুর্ণ এবং ঝুঁকিপূর্ণ উপাদানগুলোর মধ্যে অন্যতম হিসেবে বিবেচনা করা হয়ে থাকে। বৈশ্বিক ব্যবসায়িক পরিবেশ ক্রমবর্ধমানভাবে আন্তঃসংযুক্ত হয়ে পড়ছে এবং নিয়মিত তথ্যের আদান প্রদান ঘটছে। এর ফলে স্বাভাবিকভাবেই তথ্য ও যোগাযোগ প্রযুক্তি সংক্রান্ত হুমকি ও ঝুঁকি ক্রমশ বেড়ে চলেছে। এছাড়া কর্পোরেশন তার গ্রাহক, কর্মচারী, সেবাসমূহ, ব্যবসায়ীক কর্মকান্ড, লেনদেন ইত্যাদি বিভিন্ন গোপনীয় এবং মূল্য সংবেদনশীল তথ্যাদি ধারণ করে থাকে।

অতএব, উদ্ভাবনী এবং উচ্চ প্রতিযোগীতামূলক বৈশ্বিক পরিবেশে টেকসই ও যুগোপযোগী ব্যবসা পদ্ধতি নিশ্চিত, ব্যবসায়িক ঝুঁকি হ্রাস , ব্যবসায় নতুন সুযোগ তৈরী, মুনাফা এবং সুনাম বৃদ্ধি করতে কর্পোরেশনের তথ্য ও যোগাযোগ প্রযুক্তির ব্যবস্থার আধুনিকায়ন, নিয়মিত হালনাগাদকরণ এবং এতদসংক্রান্ত অভ্যন্তরীন নিয়ন্ত্রণ ও পরিপালন ব্যবস্থা প্রতিষ্ঠা করা অত্যন্ত গুরুত্বপুর্ণ বিষয়।

(ICT) অডিট হলো এমন একটি প্রক্রিয়া যা এ বিষয়ে তথ্য উপাত্ত সংগ্রহ এবং যাচাই করে একটি প্রতিষ্ঠানের কম্পিউটার ব্যবস্থার সকল আইন ও নিয়ম-নীতি মেনে প্রতিষ্ঠানটির লক্ষ্য অর্জনের উদ্দেশ্যে পরিচালিত কর্মকান্ড তথা সম্পদ সমুহের সঠিক ব্যবস্থাপনা করছে কি না, সঠিকতা ও অখন্ডতা রক্ষা করছে কি না, এবং ঝুঁকি হ্রাসকল্পে যথাযথ সুরক্ষা ব্যবস্থা স্থাপন ও ব্যবস্থাপনা করছে কি না তা যাচাই করে দেখা। একটি প্রতিষ্ঠানের তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার প্রাথমিক লক্ষ্য হলো তথ্য ও যোগাযোগ প্রযুক্তি সম্পর্কিত ঝুঁকি ও নিরাপত্তা ত্রুটি সমূহ নির্ধারণ এবং সম্ভাব্য সমাধানের সুপারিশ প্রদান করা। কর্পোরেশনের তথ্য ও যোগাযোগ প্রযুক্তি সংক্রান্ত ঝুঁকি ব্যবস্থাপনা এবং তথ্য ও যোগাযোগ প্রযুক্তি ব্যবস্থা সমূহের নিরাপত্তা ত্রুটি সমূহ নির্ধারণ এবং যথাযথ পরিচালনা নিশ্চিতকরণের লক্ষ্যে কর্পোরেশনে আইসিটি অডিট ব্যবস্থা প্রতিষ্ঠা করতে হবে ।

১.২। সংজ্ঞা :

তথ্য ও যোগাযোগ প্রযুক্তি (ICT) :

তথ্য ও যোগাযোগ প্রযুক্তির পূর্নাঙ্গ রূপ হলো ইনফরমেশন এন্ড কমিউনিকেশন টেকনোলজি । যোগাযোগ প্রযুক্তি ব্যবহার করে তথ্য পাওয়ার পদ্ধতি ই হলো তথ্য ও যোগাযোগ প্রযুক্তি (ICT) । এটি তথ্য প্রযুক্তির (IT) অনুরূপ। ইন্টারনেট, কম্পিউটার, ওয়্যারলেস নেটওয়ার্ক, সেল ফোন এবং তথ্য যোগাযোগের অন্যান্য প্রযুক্তিসমূহ এর অন্তর্ভূক্ত।

নিরীক্ষা (Audit):

নিরীক্ষা হলো পদ্ধতি (system) নিয়ন্ত্রণ, প্রতিষ্ঠিত নীতিমালার পরিপালন, পরিচালন প্রক্রিয়া যাচাইয়ের জন্য নথি-পত্র ও কর্মকান্ডের একটি স্বাধীন ও নিরপেক্ষ মূল্যায়ন ,পরীক্ষণ ,নিয়ন্ত্রণ, নীতিমালা ও পদ্ধতির ক্ষেত্রে প্রয়োজনীয় পরিবর্তন আনয়নের সুপারিশ করা। নিরীক্ষা কোন প্রতিষ্ঠানের কার্যাবলী সংক্রান্ত তথ্য যাচাই অন্তে মতামত সহকারে সংশ্লিষ্ট কর্তৃপক্ষের নিকট উপস্থাপন করে। এই ম্যানুয়ালে নিরীক্ষা বলতে তথ্য প্রযক্তিগত নিরীক্ষা কে বুঝাবে।

তথ্য ও যোগাযোগ প্রযুক্তি (ICT Audit) নিরীক্ষা :

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষণ, স্বয়ংক্রিয় উপাত্ত প্রক্রিয়াকরণ (Automatic Data Process) নিরীক্ষণ , বৈদ্যুতিক উপাত্ত প্রক্রিয়াকরণ (Electronic data processing)নিরীক্ষণ হলো প্রাথমিকভাবে একটি তথ্য প্রযুক্তি স্থাপনার মধ্যে সিস্টেমের নিয়ন্ত্রণ অবস্থা পরীক্ষা করা। এটি একটি প্রতিষ্ঠানের তথ্য প্রযুক্তি অবকাঠামো, অনুশীলন ও কার্যক্রমের উপযুক্ততা ও যথার্থতা মূল্যায়নের প্রক্রিয়া। কম্পিউটার পদ্ধতি রক্ষা ও উপাত্তের সঠিকতা বজায় রাখে কিনা তা যাচাই করার মাধ্যমে কার্যকরভাবে ও দক্ষতার সাথে একটি প্রতিষ্ঠানের লক্ষ্য অর্জনের পথকে সুগম করার জন্য তথ্য প্রযুক্তি নিরীক্ষার উদ্ভব। তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা হলো পদ্ধতি নিয়ন্ত্রণের পর্যাপ্ততা নিরুপন, প্রতিষ্ঠিত নীতিমালা ও পরিচালন প্রক্রিয়ার পরিপালন নিশ্চিতকরণ এবং প্রয়োজনীয় পরিবর্তনের সুপারিশ করার লক্ষ্যে রেকর্ড ও কর্মকান্ডের স্বাধীন মূল্যায়ন ও পরীক্ষণ।

১.৩। ম্যানুয়ালের উদ্দেশ্য:

- অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণের জন্য একটি নির্দেশিকা (Handbook) তৈরী করা।
- অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষক দলের দায়িত্ব চিহ্নিত করা;
- অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার সমস্যা চিহ্নিতকরণ এবং সমাধানের দিক নির্দেশনা প্রদান করা;
- ঝুঁকি নিরূপণের মাধ্যমে অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার বাৎসরিক পরিকল্পনা কর্মসূচি উপস্থাপন করা;
- নিয়মতান্ত্রিক নমুনা বাছাই (Sampling) এর ধারণা তৈরি করা;
- নিরীক্ষার কার্যকারিতা বাড়াতে রিপোর্টিং ও মনিটরিং পদ্ধতির মান নির্ধারণ করা;
- অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা দলের সক্ষমতা বাড়াতে কর্মলক্ষ্য (Roadmap) নির্ধারণ করা;

১.৪। ম্যানুয়ালের কার্যপরিধি:

এই ম্যানুয়েলের কার্যপরিধি আইসিটি নিরীক্ষার কার্যক্রম/সীমানা নির্ধারণ করবে। আইসিটি নিরীক্ষার পরিধি নির্ধারন করা নিরীক্ষা কার্যক্রমের একটি অংশ। এছাড়া আইসিটি নিরীক্ষা কার্যক্রম কতদিন যাবৎ কোথায় ও কি উদ্দেশ্যে সম্পাদিত হবে তা এই ম্যানুয়ালের মাধ্যমে সজ্ঞায়িত হবে। এই ম্যানুয়ালের বিধি বিধান নিম্নোক্ত কর্মকান্ডের সঙ্গে সঙ্গতি রেখে কর্পোরেশনের সর্বত্র ও সকল কর্মচারীর ক্ষেত্রে প্রযোজ্য হবেঃ

১. কর্পোরেশনের কার্যক্রমের সাথে সঙ্গতি রেখে তথ্য ও যোগাযোগ প্রযুক্তি এর ব্যবহার ও নিয়ন্ত্রন ;

২. প্রযুক্তির অপব্যবহারের মাধ্যমে কর্পোরেশনের ঝুঁকি ও ঝুঁকির মাত্রা নির্ধারণ;

৩. তথ্য ও যোগাযোগ প্রযুক্তি কাজে ব্যবহৃত সরঞ্জামাদি (হার্ডওয়্যার ও সফটওয়্যার) রক্ষনাবেক্ষণ ও ব্যবস্থাপনা;

৪. সফটওয়্যার উন্নয়ন ও আনুষঙ্গিক কর্মকান্ড সম্পাদন।

১.৫। ম্যানুয়ালের গুরুত্ব/প্রয়োজনীয়তা:

নতুন তথ্য প্রযুক্তির উন্নয়নের সাথে সাথে এতদসংশ্লিষ্ট একাধিক হুমকি ও ঝুঁকিরও উদ্ভব ঘটেছে। বর্তমানে এসব ঝুঁকির মাত্রা বিপদজনক পর্যায়ে পৌঁছেছে। ফলে প্রতিষ্ঠানের মধ্যে তথ্য পদ্ধতির (System) অভ্যন্তরীণ নিয়ন্ত্রণ প্রতিষ্ঠা করা প্রয়োজন হয়ে পড়েছে। আইসিবি ও তার গ্রাহকদের উন্নততর সেবা দেয়ার লক্ষ্যে সফটওয়্যারে আধুনিক তথ্য প্রযুক্তির ব্যবহার নিশ্চিত করেছে । তথ্য পদ্ধতির ব্যবস্থাপনায় আইসিবি আইসিটি পলিসি প্রণয়ন করেছে। এ বিষয়ে সময়ে সময়ে ব্যবস্থাপনা কর্তৃপক্ষ কর্তৃক নির্দেশনাসমূহ এবং তথ্য ও যোগাযোগ ঝুঁকি ব্যবস্থাপনা ও নিয়ন্ত্রণের জন্য বাংলাদেশ সরকারের আইসিটি এ্যাক্ট, বিআরপিডি সার্কুলার এবং বাংলাদেশ ব্যাংক-এর "গাইডলাইন্স অন আইসিটি সিকিউরিটি ফর ব্যাংকস এন্ড নন-ব্যাংক ফিনান্সিয়াল ইন্সটিটিউশন্স ২০১৫" রয়েছে । তথ্য ও যোগাযোগ প্রযুক্তির অভ্যন্তরীণ নিয়ন্ত্রণ ও নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে আইসিবির তথ্য পদ্ধতি নিরীক্ষা ও পরিদর্শন করে। এক্ষেত্রে উল্লিখিত নীতিমালা, নির্দেশিকা, প্রচারিত বিজ্ঞপ্তি ও আইনের সাথে তথ্য ও যোগাযোগ পদ্ধতির পরিচালনা যেন সংগতিপূর্ণ হয় সেজন্য তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণকে বিষয়টি নিশ্চিত করবেন। দক্ষতার সাথে কার্যকরভাবে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা ও পরিদর্শন কার্যক্রম পরিচালনার জন্য আইসিটি ম্যনুয়াল তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকদের নির্দেশনাও প্রদান করবে।

অধ্যায়-২
তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার (ICT Audit) ধারনা

প্রাথমিকভাবে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা হল তথ্য ও যোগাযোগ প্রযুক্তি স্থাপনার মধ্যে পদ্ধতি নিয়ন্ত্রণের একটি পরীক্ষা, যা একটি প্রতিষ্ঠানের তথ্য ও যোগাযোগ কাঠামো, এর চর্চা পরিচালনার উপযুক্ততা ও গ্রহণযোগ্যতা মূল্যায়নের প্রক্রিয়া। তথ্য পদ্ধতি সম্পদের সুরক্ষা ও উপাত্তের সঠিকতা রক্ষা করে কিনা তা মূল্যায়নের মাধ্যমে কোনো প্রতিষ্ঠানকে কার্যকরভাবে ও দক্ষতার সাথে তার লক্ষ্য অর্জনে সহায়তা করতে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার ধারনার উদ্ভব হয়েছে । তাই তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা হলো পদ্ধতি নিয়ন্ত্রণের পর্যাপ্ততা নিরূপণ, প্রতিষ্ঠিত নীতিমালা ও পরিচালন প্রক্রিয়ার পরিপালন নিশ্চিতকরণ এবং নিয়ন্ত্রণ, নীতিমালা বা প্রক্রিয়ার মধ্যে প্রয়োজনীয় পরিবর্তনের সুপারিশ করার লক্ষ্যে রেকর্ড ও কর্মকান্ডের স্বাধীন মূল্যায়ন ও পরীক্ষণ।

এছাড়া তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা হল কারিগরি উপকরণ ও দক্ষতা ব্যবহার করে একটি পদ্ধতির পর্যাপ্ততা ও কার্যকারিতা যাচাই করা । এটি ব্যবসায়ে প্রযুক্তি ব্যবহারে উদ্ভূত দুর্বলতা নিয়ন্ত্রণ ও ঝুঁকি চিহ্নিতকরণে ব্যবস্থাপনা কর্তৃপক্ষের তথ্য পদ্ধতির উপর নির্ভরযোগ্যতা বাড়ায় এবং নিয়ন্ত্রণকে শক্তিশালী করার উপায় নির্ধারণ করে, যা কোনো প্রতিষ্ঠানের ব্যবসায়িক উদ্দেশ্য অর্জনে সহায়তা করে ।

২.১ নিরীক্ষার ধরন :

অভ্যন্তরীণ ও বহিঃস্থভাবে সম্পাদন করা যায় এমন বিভিন্ন নিরীক্ষা নিম্নে উল্লেখ করা হলো এবং নিম্নলিখিত প্রতিটি বিষয়ের সাথে সম্পর্কিত নিরীক্ষণ প্রক্রিয়া সম্পর্কে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকের ধারণা থাকা জরুরী:

আর্থিক নিরীক্ষা (Financial Audit): আর্থিক নিরীক্ষার উদ্দেশ্য হল একটি প্রতিষ্ঠানের আর্থিক প্রতিবেদনের সঠিকতা, স্বচ্ছতা ও বস্তুনিষ্ঠতা মূল্যায়ন করা। আর্থিক নিরীক্ষায় প্রায়শই বিস্তারিত ও ব্যাপক পরীক্ষণের প্রয়োজন পড়ে। এ ধরনের নিরীক্ষা তথ্যের বস্তুনিষ্ঠতা ও বিশ্বাসযোগ্যতা বাড়ায়।

পরিচালনগত নিরীক্ষা (Operational Audit): পরিচালন ব্যবস্থাকে সাশ্রয়ী, দক্ষ, নিরাপদ ও কার্যকর করার লক্ষ্যে একটি বিদ্যমান প্রক্রিয়া বা ক্ষেত্রের অভ্যন্তরীণ নিয়ন্ত্রণ কাঠামা মূল্যায়নের পরিচালনগত নিরীক্ষা করা হয় । এ্যাপ্লিকেশন নিয়ন্ত্রণের তথ্য পদ্ধতি নিরীক্ষা অথবা লজিক্যাল সিকিউরিটি সিস্টেমস অডিট-পরিচালনগত নিরীক্ষার উদাহরণ।

সমন্বিত নিরীক্ষা (Integrated Audit): সমন্বিত নিরীক্ষা হল আর্থিক ও পরিচালনগত নিরীক্ষার সমন্বিত পদক্ষেপ। একটি প্রতিষ্ঠানের অর্থনৈতিক তথ্য, সম্পদ সুরক্ষা, দক্ষতা এবং পরিপালনের সাথে সম্পৃক্ত সামগ্রিক উদ্দেশ্য মূল্যায়নে এ নিরীক্ষা সম্পাদন করা হয় । সমন্বিত নিরীক্ষা অভ্যন্তরীণ বা বহিঃস্থ নিরীক্ষকগণের দ্বারা সম্পাদন করা যেতে পারে এবং এতে অভ্যন্তরীণ নিযন্ত্রণের পরিপালন পরীক্ষা ও ব্যাপক নিরীক্ষণ প্রক্রিয়া যুক্ত থাকতে পারে ।

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা (ICT Audit): তথ্য ও যোগাযোগ ব্যবস্থা এবং সংশ্লিষ্ট উৎসসমূহ পর্যাপ্তভাবে সম্পদ সুরক্ষা, উপাত্ত ও পদ্ধতির শুদ্ধতা বজায় রাখা, প্রাসঙ্গিক ও নির্ভরযোগ্য তথ্য প্রদান, কার্যকরভাবে প্রতিষ্ঠানের লক্ষ্য অর্জন, সম্পদের সুষ্ঠু ব্যবহার এবং অভ্যন্তরীণ নিয়ন্ত্রণ কার্যকর করার মাধ্যমে ব্যবসার গ্রহণযোগ্য নিশ্চয়তা প্রদান করে কিনা তা নির্ধারণে এই প্রক্রিয়া প্রমাণক সংগ্রহ ও মূল্যায়ন করে। এর মাধ্যমে পরিচালনগত ও নিয়ন্ত্রণগত উদ্দেশ্য অর্জিত হবে এবং অনাকাঙ্খিত ঘটনা রোধ অথবা চিহ্নিত করা এবং নির্দিষ্ট সময় অন্তর তা সংশোধন করা । সংক্ষেপে, সেটাই তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা যা স্বয়ংক্রিয় তথ্য প্রক্রিয়াকরণ ব্যবস্থা, সংশ্লিষ্ট অস্বয়ংক্রিয় প্রক্রিয়া এবং উভয়ের একাঙ্গীভূতকরনের বিষয়টি পুণর্বিক্ষণ ও পূর্ণ অথবা আংশিক মূল্যায়ন করে ।

বিচারিক নিরীক্ষা (Forensic Audit): প্রথাগতভাবে, প্রতারণা ও অপরাধ উদঘাটন ও প্রকাশ এবং এর ফলো-আপের জন্য পরিচালিত বিশেষায়িত নিরীক্ষাকেই বিচারিক নিরীক্ষা হিসেবে সংজ্ঞায়িত করা হয়। আইনশৃঙ্খলা রক্ষাকারী বাহিনী ও বিচারিক কর্তৃপক্ষের যাচাই বাছাই এর জন্য প্রমাণ খুঁজে বের করাই এ ধরনের নিরীক্ষার প্রাথমিক উদ্দেশ্য। সাম্প্রতিক বছরগুলোতে কর্পোরেট প্রতারণা ও সাইবার অপরাধ-সংশ্লিষ্ট তদন্তের জন্য বিচারিক পেশাজীবিগণকে নিয়োজিত করা হচ্ছে। কোনো ক্ষেত্রে কম্পিউটার সম্পদের অপব্যবহার হয়ে থাকলে যথাযথ কর্তৃপক্ষের কাছে প্রতিবেদন উপস্থাপনের জন্য সম্ভাব্য অপরাধমূলক কর্মকান্ডের তথ্য সংগ্রহে অধিক তদন্তের প্রয়োজন পড়ে। ইলেক্ট্রনিক যন্ত্রপাতি যেমনঃ কম্পিউটার, ল্যাপটপ, সেলুলার ফোন, পার্সোনাল ডিজিটাল এ্যাসিস্ট্যান্টস (PDAs), ডিস্কস, সুইচ, রাউটার, হাব এবং অন্যান্য ইলেক্ট্রনিক যন্ত্রপাতি কম্পিউটার বিচারিক তদন্তের অন্তর্ভুক্ত ।

২.২ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার উদ্দেশ্যঃ

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা অন্যান্য নিরীক্ষার মত নয় যদিও এটি অন্যান্য নিরীক্ষার ক্ষেত্রে গুরুত্বপূর্ণ মান বহন করে। তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার মূল উদ্দেশ্য হচ্ছে তথ্য প্রযুক্তি পরিচালনে অভ্যন্তরীণ নিয়ন্ত্রণ ব্যবস্থা মূল্যায়ন করা এবং এর দুর্বলতা চিহ্নিত করা। করপোরেশন ও এর গ্রাহকের স্বার্থ রক্ষা করা খুবই গুরুত্বপূর্ণ। বর্তমান সময়ে হ্যাকাররা খুব শক্তিশালী তাই কর্পোরেশনের সম্পদ রক্ষা এবং অনুমোদিত পক্ষগুলোকে তথ্য সরবরাহ করার জন্য আইএস অপারেশন সংরক্ষণ করা খুবই গুরুত্বপূর্ণ। সাধারণ নিরীক্ষণের উদ্দেশ্যসমূহকে কীভাবে নির্দিষ্ট আইএস নিয়ন্ত্রণে রূপান্তরিত করা যায় সে সম্পর্কে আইএস অডিটরের ধারণা থাকা উচিত। তথ্য পদ্ধতি নিরীক্ষা পরিকল্পনায় নিরীক্ষার উদ্দেশ্য নির্ধারণ একটি জটিল প্রক্রিয়া।

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার মূল্যায়ন প্রক্রিয়ায় নিম্নোক্ত বিষয়গুলো নিশ্চিত করতে হবে :

(ক) সম্পদের সুরক্ষা নিশ্চিত করা। 'সম্পদ' যা নিম্ন ধরনের সম্পদের অন্তর্ভূক্ত:

- **প্রযুক্তি (Technology)**- হার্ডওয়্যার, অপারেটিং সিস্টেম, ডাটাবেজ ম্যানেজমেন্ট সিস্টেম (DBS), নেটওয়ার্ক, মাল্টিমিডিয়া ইত্যাদি প্রযুক্তির আওতাভূক্ত;
- **উপাত্ত (Data)**- ব্যাপক অর্থে উপাত্তের উদ্দেশ্য হল বহিঃস্থ এবং অভ্যন্তরীণ, বিন্যস্ত ও অবিন্যস্ত, চিত্র, শব্দ, পদ্ধতি (System), দলিলায়ন (Documentation) ইত্যাদি;
- **প্রয়োগ পদ্ধতি(Application system)** - ম্যানুয়াল ও নির্ধারিত প্রক্রিয়ার সমন্বিত রূপই প্রয়োগ পদ্ধতি;
- **সুবিধা**- তথ্য পদ্ধতিকে সুরক্ষা দেয়ার জন্য অভ্যন্তরীণ উৎসের সরবরাহ;
- **জনবল**- পরিকল্পনা, সংগঠিত করা, অর্জন, অর্পণ, সহায়তা এবং তথ্য ব্যবস্থা ও সেবা পর্যবেক্ষণে কর্মীর দক্ষতা, সচেতনতা এবং উৎপাদনশীলতা ইত্যাদি।।

(খ) উপাত্ত বা তথ্যে নিম্নবর্ণিত গুণাবলী নিশ্চিত করাঃ

- **সাশ্রয়**- যথাযথভাবে সম্পদ ব্যবহারের মাধ্যমে সর্বোচ্চ লক্ষ্য অর্জনের জন্য কর্মী, প্রক্রিয়া ও ব্যবস্থা নিয়ে কাজ করা;
- **দক্ষতা**- স্বল্পতম সম্পদ ব্যবহারের মাধ্যমে প্রতিষ্ঠানের চাহিদানুসারে গুণগত ও পরিমানগত তথ্য সরবরাহ;
- **কার্যকারিতা**- উর্ধ্বতন কর্তৃপক্ষ ও ব্যবহারকারীদের সামগ্রিক উদ্দেশ্য পূরণের জন্য ব্যবসা প্রক্রিয়ায় প্রাসঙ্গিক এবং যথাসময়ে সরবরাহকৃত সঠিক, সামঞ্জস্যপূর্ণ ব্যবহারযোগ্যভাবে তথ্য সরবরাহ করতে তথ্য ও যোগাযোগ ব্যবস্থা নিয়ে কাজ করা;
- **গোপনীয়তা**- অননুমোদিতভাবে স্পর্শকাতর তথ্য প্রকাশ রোধ করা;
- **অখন্ডতা**- সংরক্ষিত উপাত্তের সঠিকতা ও সামঞ্জস্যতা এ দুটি ডাটা রেকর্ডের হালনাগাদকরণের মধ্যে যেকোন পরিবর্তনের অনুপস্থিতিকে নির্দেশ করে;
- **পর্যাপ্ততা**- ব্যবসা প্রক্রিয়ায় চাহিদা মত প্রয়োজনাতিরিক্ত তথ্য প্রাপ্তি সম্পর্কিত এবং সম্পদের সুরক্ষা সংশ্লিষ্ট;
- **পরিপালন**- ব্যবসা প্রক্রিয়ার সাথে সংশ্লিষ্ট আইন, বিধি-বিধান এবং চুক্তিভিত্তিক ব্যবস্থা তথা বাইরে থেকে আরোপিত ব্যবসায়িক মানদন্ড পরিপালনের সাথে এটি সম্পৃক্ত । এর অর্থ হল পদ্ধতিকে অবশ্যই কর্পোরেশনের আইন, বিধি-বিধান এবং শর্তের আওতায় পরিচালনা করা। প্রতিষ্ঠানের কর্মকান্ড যাতে নিয়ন্ত্রণকারী কর্তৃপক্ষের আইনের সাথে সংগতিপূর্ণ হয় সে বিষয়টি তথ্য প্রযুক্তি নিরীক্ষককে দেখতে হবে;
- **তথ্যের নির্ভরযোগ্যতা ও নিরাপত্তা**- প্রতিষ্ঠান পরিচালনা এবং এর নিরাপত্তায় ব্যবস্থাপনা কর্তৃপক্ষের প্রয়োজন, আর্থিক তথ্য ব্যবহারকারীদের জন্য আর্থিক প্রতিবেদন প্রদান এবং আইন ও বিধি-বিধান পরিপালনের বিষয়টি দেখার লক্ষ্যে নিয়ন্ত্রণকারী কর্তৃপক্ষের কাছে প্রতিবেদন উপস্থাপনার্থে সঠিক তথ্য সরবরাহের সাথে এটি জড়িত ।

বিদ্যমান আইন পরিপালনের মাধ্যমে কর্পোরেশনের আর্থিক এবং পরিচালন দক্ষতা নিশ্চিত করার কাঙ্খিত লক্ষ্য অর্জনে তথ্য যোগাযোগ প্রযুক্তি প্রক্রিয়া / তথ্য ও যোগাযোগ উৎস যৌথভাবে কাজ করছে কিনা তা খতিয়ে দেখাই তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা।

২.৩ তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষার গুরুত্ব/প্রয়োজনীয়তা :

- বর্তমানে, প্রতিযোগিতায় টিকে থাকতে প্রতিষ্ঠানগুলো প্রযুক্তিগত পরিবর্তনের সাথে খাপ খাইয়ে নিচ্ছে। প্রতিযোগীতামূলক সুবিধা গ্রহণ, পরিচালন উৎকর্ষ অর্জন এবং কখনো কখনো বিভিন্ন শাখাকে সম্পৃক্ত করার মত নানা কারণে তারা বিভিন্ন প্রযুক্তি সংযোজন করছে । এটা তাদের পরিচালন দক্ষতা বৃদ্ধি করছে। প্রতিষ্ঠানে প্রযুক্তির প্রয়োগ অনেক ঝুঁকির জন্ম দেয় যা ব্যবসার জন্য ক্ষতিকারক হতে পারে। এ কারণে তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষার প্রয়োজন রয়েছে।
- তথ্য ও যোগাযোগ প্রযুক্তির (ICT) ব্যাপক সুবিধার বিষয়টি অনুধাবন করতে পেরে অনেক প্রতিষ্ঠান তথ্য ও যোগাযোগ প্রযুক্তির খাতে প্রচুর অর্থ ব্যয় করছে । এর উদ্দেশ্য এটা নিশ্চিত করা প্রয়োজন যে তাদের তথ্য ও যোগাযোগ পদ্ধতি নির্ভরযোগ্য, সুরক্ষিত এবং সাইবার-আক্রমণে ঝুঁকিপূর্ণ (vulnerable) নয়।
- আইসিটি নিরীক্ষণ গুরুত্বপূর্ণ কারণ এটি তথ্য ও যোগাযোগ প্রযুক্তি (ICT)- র পর্যাপ্ত নিরাপত্তা, ব্যবহারকারীদের নির্ভরযোগ্য তথ্য সরবরাহ এবং তাদের কাঙ্খিত সুবিধা অর্জনে নিশ্চয়তা প্রদান করে। উপাত্ত পরিবর্তন (tampering), উপাত্ত হারানো

বা তথ্য ফাঁস হওয়া, সেবা বিঘ্নিত হওয়া এবং তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতির দুর্বল ব্যবস্থাপনার ঝুঁকি কমাতেও তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষা সহায়তা করে।

২.৪ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার প্রকারভেদ:

তথ্য ও উপাত্তের যথাযথ ব্যবহার ও নিরাপত্তা, ডাটা প্রসেসিং ব্যয়, সিস্টেম পরিচালনা, প্রযুক্তির ব্যবহার এবং সুপরিকল্পিত নিয়ন্ত্রণ ইত্যাদি আইসিটি অডিটের বিবেচ্য বিষয়। কাজের ধরন অনুযায়ী আইসিটি অডিট বিভিন্ন প্রকার হতে পারে। যেমনঃ

সিস্টেম এবং এপ্লিকেশন অডিটঃ বিদ্যমান সিস্টেমের পদ্ধতি ও এপ্লিকেশনগুলোর যথাযথতা, কার্যকারিতা, দক্ষতা, নির্ভরযোগ্যতা, সময়োপযোগীতা, নিরাপত্তা সার্বিকভাবে নিয়ন্ত্রিত কিনা তার মূল্যায়ন হল সিস্টেম এবং এপ্লিকেশন অডিট।

সিস্টেম ডেভেলপমেন্ট অডিটঃ কর্পোরেশনের উদ্দেশ্য বাস্তবায়নের নিমিত্ত প্রস্তুতকৃত সিস্টেমগুলো বিভিন্ন নিয়ন্ত্রণকারী কর্তৃপক্ষের নির্দেশনা এবং সিস্টেম উন্নয়নের নূন্যতম মান বা স্ট্যান্ডার্ড বজায় রেখে বিদ্যমান বা নতুন উন্নয়নকৃত সিস্টেমগুলো চলমান রয়েছে কিনা তার মূল্যায়ন হল সিস্টেম ডেভেলপমেন্ট অডিট।

ইনফরমেশন প্রসেসিং ফ্যাসিলিটিস অডিটঃ স্বাভাবিক ও অস্বাভাবিক পরিস্থিতিতে নিয়মতান্ত্রিক, সঠিক, সময়োপযোগী এবং সাশ্রয়ীভাবে সিস্টেম চলমান রয়েছে কিনা তার মূল্যায়ন হল ইনফরমেশন প্রসেসিং ফ্যাসিলিটিস অডিট।

ইন্টারনেট, সার্ভার এবং এক্সট্রানেটস অডিটঃ নিরীক্ষা পদ্ধতি যা প্রতিষ্ঠানের চাহিদা মত সঠিক ও নিরবিচ্ছিন্ন তথ্য সরবরাহ নিশ্চিত করতে ক্লয়েন্ট ও সার্ভারের মধ্যে সংযোগকারী নেটওয়ার্কের নিয়ন্ত্রণ ও কার্যক্রম নিশ্চিত করে।

ম্যানেজমেন্ট অব আইটি এবং এন্টারপ্রাইজ আর্কিটেকচার অডিটঃ নিরীক্ষা পদ্ধতি যা প্রতিষ্ঠানের ডাটা প্রসেসিং এ দক্ষ ও উপযুক্ত আইটি পরিবেশ নিশ্চিত করতে প্রস্তুতকৃত আইটি স্ট্রাকচার ও পদ্ধতির নিয়ন্ত্রণ নিশ্চিত করে।

টেকনোলজি ইনোভেশন প্রসেস অডিটঃ নিরীক্ষা পদ্ধতি যা নতুন প্রজেক্ট উদ্ভাবনে ব্যবহৃত টেকনোলজির ঝুঁকির মাত্রা নিরূপণ এবং বিদ্যমান সিস্টেমের সাথে সামঞ্জস্যতা ও সময়োপযোগীতা নিশ্চিত করে।

ইনোভেটিভ কম্পারিজন এবং পজিশন অডিটঃ নিরীক্ষা পদ্ধতি যা প্রতিযোগিদের তুলনায় কোন প্রতিষ্ঠানের উদ্ভাবনী কাজে দক্ষতা ও সক্ষমতা যাচাই করে। এটি প্রতিষ্ঠানের বিদ্যমান প্রযুক্তিকে যাচাই করে এবং নতুন প্রযুক্তি সংযোজনের বিষয়ে মতামত প্রদান করে।

২.৫ তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষকের কর্তব্যঃ

আইসিটি নিরীক্ষকগণ প্রতিষ্ঠানের আইসিটি সিস্টেমের নিরাপত্তা, গুনগতমান ও আবশ্যিকভাবে পরিপালনীয় বিষয়গুলো উর্ধতন কর্তৃপক্ষ(বোর্ড) সমীপে উপস্থাপন করবে। টেকনিক্যাল কাজে যথার্থ দক্ষতাসহ নিরীক্ষকের সাধারণ গুনাবলী হিসেবে পেশাদারিত্ব ও স্বাধীনভাবে মত প্রকাশের সাহসিকতা থাকা প্রয়োজন।

একজন আইসিটি নিরীক্ষকের দায়িত্ব নিম্নরূপ হতে পারেঃ

- প্রতিষ্ঠানের কম্পিউটার সিস্টেম এবং কারিগরী দিকগুলো নিরীক্ষা করা। এছাড়া কম্পিউটারের ডাটাগুলোর নিরাপত্তা নিশ্চিত করে স্বচ্ছতা, সঠিকতা, নিখুতভাবে নিরূপন করা।
- ডাটার সঠিকতা ও নির্ভূলতা নিরূপণ, ডাটা ব্যাকআপ এবং ডিজাস্টার রিকভারী পর্যবেক্ষণ, ডাটা সেন্টারের কার্যক্রম, ডাটা কমিউনিকেশন এবং এক্সেস কন্ট্রোল, ডাটাবেইজ অ্যাডমিনিস্ট্রেশন এবং ইউজার কন্ট্রোল সিস্টেম নিরীক্ষা করা;
- কর্তৃপক্ষ বা রেগুলেটরী অথরিটির নির্দেশে বিশেষ রিভিউ, অনুসন্ধান বা নিরীক্ষা কার্য পরিচালনা করা;
- ইনফরমেশন সিস্টেম নিরীক্ষা ব্যবস্থাপনার পরিকল্পনা করা, নিরীক্ষা ও নিরীক্ষকের কাজের লক্ষ্য ও পরিধি নির্ধারণ করা। এছাড়া নিরীক্ষা পদ্ধতির (নিরীক্ষা প্রক্রিয়া, কৌশল ও ব্যবহৃতব্য টুলস) বিষয়ে কর্তৃপক্ষের নিকট সুপারিশ উপস্থাপন করা;
- নিরীক্ষা কার্যক্রমের সাথে সঙ্গতি রেখে প্রতিষ্ঠানের আইসিটি সিস্টেমের উন্নয়নের বিষয়ে সুপারিশ প্রদান করা;
- নিরীক্ষা কার্যক্রমের আওতা ও ক্ষেত্র চিহ্নিতকরন ও নির্ধারণ এবং ব্যয়, সময় ও গুণগতমানের নিরিখে উক্ত বিষয়ের ঝুঁকির মাত্রা নিরূপণ করা;
- নিরীক্ষক দলের অংশ হিসেবে আইসিটি নিরীক্ষা কাজে নিরীক্ষা কর্মীদের কারিগরী সহায়তা ও দিক নির্দেশনা প্রদান করা;
- নিরীক্ষা কার্যক্রম পরিচালনার নিমিত্ত প্রতিষ্ঠানের কার্যক্রমের সাথে সঙ্গতি রেখে নতুন নতুন প্রযুক্তির কারিগরি জ্ঞান ও দক্ষতা অর্জন করা।

২.৬ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকের প্রয়োজনীয় যোগ্যতা:

একজন তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষকের যেসব বিষয়ে জ্ঞান থাকতে হবে তা নিম্নে উল্লেখ করা হলো:

- একটি সমন্বিত তথ্য ব্যবস্থা/পদ্ধতির (system) নিরীক্ষা কর্মসূচির কর্মকান্ড, পরিচালনা ও রক্ষণাবেক্ষণ;
- তথ্য ব্যবস্থা/পদ্ধতি নিরীক্ষা ও নিয়ন্ত্রণের নীতি ও চর্চা;
- ব্যবসায় কম্পিউটার ব্যবহার, মেইনফ্রেম সিস্টেম এবং সংশ্লিষ্ট তথ্য পদ্ধতি প্রযুক্তি যথা: লোকাল এরিয়া নেটওয়ার্ক (LAN), মেট্রোপলিটান এরিয়া নেটওয়ার্ক (MAN), ওয়াইড এরিয়া নেটওয়ার্ক (WAN), ক্লায়েন্ট সার্ভার সিস্টেম ইত্যাদি সংক্রান্ত নীতি ও চর্চা;
- তথ্য ব্যবস্থা/পদ্ধতি প্রক্রিয়া ও নিয়ন্ত্রণ বিশ্লেষণের পদ্ধতি ও কৌশল;
- তথ্য নিরাপত্তা ও প্রবেশাধিকার নিয়ন্ত্রণ, উপাত্তের নির্ভুলতা, ব্যাকআপ ও দুর্যোগ ব্যবস্থাপনা, ডাটাবেজ ব্যবস্থাপনা, লোকাল এরিয়া নেটওয়ার্ক এবং ডাটা কমিউনিকেশনস, ক্লায়েন্ট সার্ভার সিস্টেম সংশ্লিষ্ট কার্যাবলী, পরিচালন ও কর্মকান্ডের নীতি ও চর্চা;
- ISACA নিরীক্ষার মত তথ্য ব্যবস্থা নিরীক্ষা মানদন্ড ও নিশ্চয়তা মানদন্ড এবং নির্দেশনাসমূহ;
- পরিসংখ্যনগত নমুনা বাছাই ও প্রত্যাগতি বিশ্লেষণ (regression analysis) এর মত প্রাগ্রসর গাণিতিক ও পরিমানগত বিশ্লেষণ পদ্ধতি;
- সংশ্লিষ্ট জাতীয় ও আন্তর্জাতিক আইন ও বিধি-বিধান;
- ব্যবস্থাপনা নীতি ও কৌশল;
- ব্যবসা ও নিরীক্ষা সংক্রান্ত নৈতিকতাসমূহ ইত্যাদি।

একজন তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষকের যেসব বিষয়ের উপর দক্ষতা থাকা দরকার তা হলঃ

- স্বাধীনভাবে তথ্য ব্যবস্থা নিরীক্ষা সম্পাদন করা;
- বিভাগের নীতি ও পদ্ধতির ব্যাখ্যা প্রদান ও কার্যকর করতে বাধ্য করা;
- পরিসংখ্যানগত, অর্থনৈতিক ও অন্যান্য গাণিতিক বিশ্লেষণ করা;
- ঝুঁকি বিশ্লেষণ ও অগ্রাধিকারের ভিত্তিতে নিরীক্ষার বিষয় নির্বাচন করা;
- নিরীক্ষিত কর্মকান্ডের পরিবেশ ও চাহিদা বুঝতে পারা;
- নিরীক্ষা ফলাফলের পরিণাম এবং এর প্রভাব বুঝতে পারা;
- দূরদর্শী, রক্ষণযোগ্য ও সময়োচিত সিদ্ধান্ত গ্রহণ;
- নিরীক্ষা ফলাফলের বস্তুগত নির্ভরতা বিচার বিবেচনা করা;
- তথ্য ব্যবস্থা নিরীক্ষায় চুক্তি, আইন, বিধি-বিধানের অনুসরণ;
- মৌখিক ও লিখিত নির্দেশাবলী অনুধাবন ও অনুসরণ করতে পারা;
- মৌখিক ও লিখিত উভয় ক্ষেত্রে পরিস্কারভাবে ও সংক্ষেপে যোগাযোগ করা ;
- কর্ম সম্পাদন প্রক্রিয়ায় চুক্তিবদ্ধ সকলের সাথে কার্যকর কর্ম-সম্পর্ক স্থাপন ও বজায় রাখা ইত্যাদি ।

একজন তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকের সার্টিফাইড ইনফরমেশন সিস্টেম অডিটর (CISA), সার্টিফাইড ইনফরমেশন সিকিউরিটি ম্যানেজার (CISM), সার্টিফাইড ইন দা গভর্নেন্স অব এন্টারপ্রাইজ আইটি (CGEIT), সার্টিফাইড ইন রিস্ক এন্ড ইনফরমেশন সিস্টেম কন্ট্রোল (CRISC) এর মত আন্তর্জাতিক মানের পেশাগত সনদপত্র থাকা বাঞ্ছনীয় ।

অধ্যায়-৩

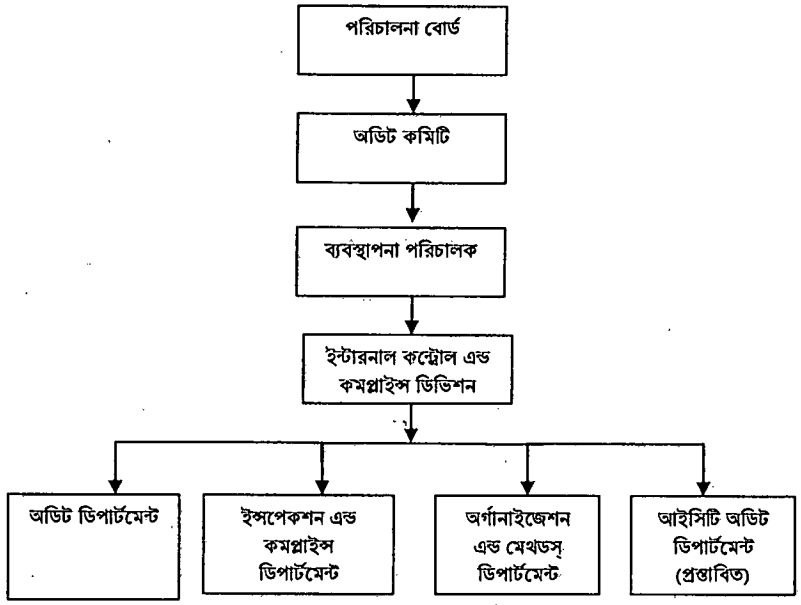
তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার পরিকল্পনা (ICT Audit Planning)

৩.১ নিরীক্ষা প্রণালী

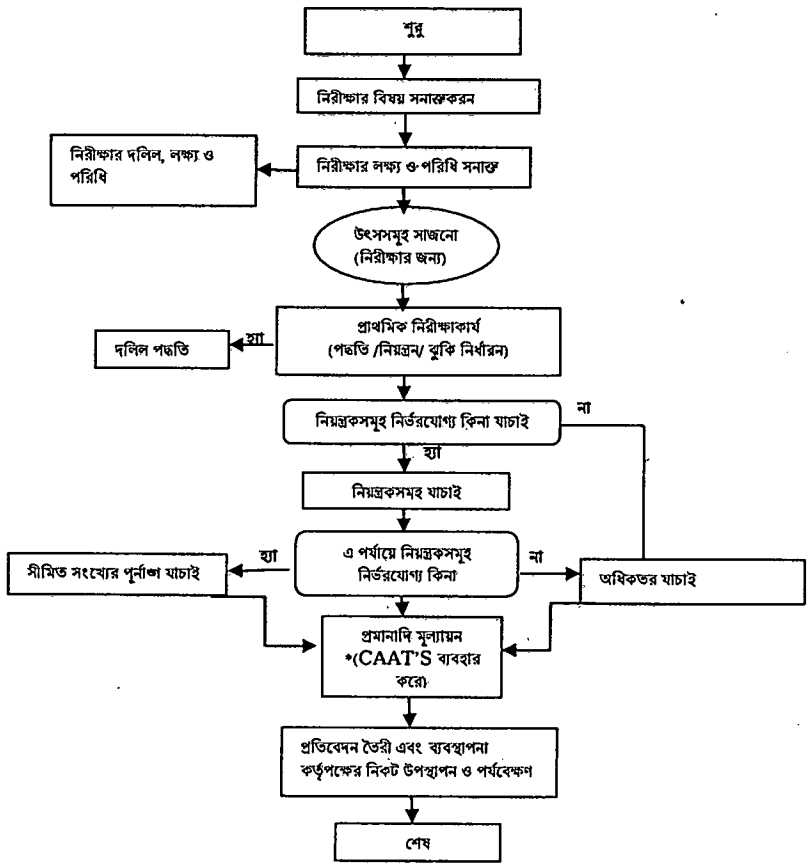
- বিদ্যমান তথ্য প্রযুক্তির সিস্টেমের পরিবেশে ঝুঁকির বিষয়গুলো চিহ্নিত করা ও এ ধরনের ঝুঁকি প্রতিকারের জন্য অগ্রাধিকার ভিত্তিক তালিকা তৈরি করা;
- পরিচালনা পর্ষদের অনুমোদিত বিদ্যমান আইসিটি পলিসি অনুযায়ী তথ্য ও যোগাযোগ প্রযুক্তি (ICT) বাস্তবায়ন করা হচ্ছে কিনা তা দেখা;
- যথাযথ পরিচর্যা এবং তথ্য ও যোগাযোগ প্রযুক্তি (ICT) সম্পদের অপব্যবহার/ভুল ব্যবহার, কম্পিউটার সংশ্লিষ্ট অপরাধ রোধ করে ঝুঁকি দূর করতে তথ্য প্রযুক্তি নীতি ও অন্যান্য প্রাসঙ্গিক নির্দেশিকায় নির্ধারিত নিয়ন্ত্রণ ব্যবস্থা কঠোরভাবে পরিপালন করা হয় কিনা তা যাচাই করা;
- বর্ণিত নিয়ন্ত্রণ ব্যবস্থার পরিপালন নিশ্চিত করার লক্ষ্যে নিয়ন্ত্রণের মাত্রা যাচাই ও মতামত পেশ করা ইত্যাদি।

৩.২ নিরীক্ষার প্রাতিষ্ঠানিক কাঠামো

আইসিবির পূর্ণাঙ্গ ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স (ICC) কাঠামো



৩.৩। নিরীক্ষা প্রক্রিয়ার ফ্লো চার্ট



*CAAT'S- Computer Assisted Audit Techniques and tools

৩.৪। নিরীক্ষা প্রক্রিয়ার ধাপ বা পর্যায়:

নিরীক্ষা পর্যায়	বিবরণ
নিরীক্ষার বিষয়	নিরীক্ষার ক্ষেত্র চিহ্নিত করা
নিরীক্ষার উদ্দেশ্য	নিরীক্ষার উদ্দেশ্য চিহ্নিত করা। উদাহরণস্বরূপ, সফটওয়্যার সোর্স কোড একটি সু-সংজ্ঞায়িত এবং নিয়ন্ত্রিত পরিবেশে সম্পন্ন হয় কিনা তা নির্ধারণ করা।
নিরীক্ষার পরিধি	একটি নির্দিষ্ট সময়ের জন্য প্রতিষ্ঠানের সুনির্দিষ্ট পদ্ধতি, কার্যাবলী অথবা ইউনিট চিহ্নিত করে পর্যালোচনার জন্য অর্ন্তভূক্ত করা।
প্রাক-নিরীক্ষা পরিকল্পনা	• প্রয়োজনীয় কারিগরি দক্ষতা ও সম্পদ চিহ্নিত করা । • পরীক্ষা বা পর্যালোচনার জন্য ফাংশনাল ফ্লো চার্ট, নীতিমালা, মানদন্ড ও নির্দেশিকা, প্রক্রিয়া ও পূর্ববর্তী নিরীক্ষা কার্যক্রমের কাগজপত্রের মত তথ্য সূত্র চিহ্নিত করা। • নিরীক্ষার স্থান বা সুযোগ সুবিধা চিহ্নিত করা

নিরীক্ষার পদ্ধতি এবং উপাত্ত সংগ্রহের ধাপ	• নিয়ন্ত্রণ যাচাই ও পরীক্ষার জন্য নিরীক্ষা প্রক্রিয়া চিহ্নিত করা ও নির্বাচন করা । • সাক্ষাৎকারের জন্য ব্যক্তি বিশেষের তালিকা করা । • পর্যালোচনার জন্য বিভাগীয় নীতিমালা, মানদন্ড ও নির্দেশিকা নির্বাচন ও প্রাপ্তি। • নিয়ন্ত্রণ পরীক্ষা ও যাচাই এর জন্য নিরীক্ষা উপকরণ ও পদ্ধতি তৈরি করা।
পরীক্ষা অথবা পর্যালোচনার ফলাফল মূল্যায়নের পদ্ধতি	• পর্যালোচনার ফলাফল থেকে তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, মানদন্ড ও নির্দেশিকার বিচ্যুতি/লঙ্ঘন চিহ্নিত করা । • এর সাথে সম্পর্কিত ঝুঁকির মাত্রা চিহ্নিত করা ।
নিরীক্ষা প্রতিবেদন প্রস্তুতকরণ	• নিরীক্ষা প্রতিবেদনের কাঠামো নির্ধারণ । • যথাসময়ে পূর্নাঙ্গ ,বস্তুনিষ্ঠ , স্পষ্ট এবং সংক্ষিপ্ত প্রতিবেদন প্রস্তুতকরন । • প্রাপ্ত ফলাফলের উপযুক্ততা/সঠিকতা পর্যালোচনা ও মূল্যায়ন। • প্রয়োজনীয় সুপারিশ প্রদান।
ব্যবস্থাপনা কর্তৃপক্ষের সাথে যোগাযোগের পদ্ধতি	• তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষক নিরীক্ষায় প্রাপ্ত ফলাফল সংশ্লিষ্ট ডিভিশনের প্রধানের কাছে রিপোর্ট করবে। নিরীক্ষায় প্রাপ্ত ফলাফলের গুরুত্ব বিবেচনা করে উর্ধ্বতন কর্তৃপক্ষের কাছে রিপোর্ট প্রেরণ করতে হবে ।

৩.৫। তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা টিম:

৩.৫.১ টিম গঠন:

একটি প্রতিষ্ঠানে একটি নির্দিষ্ট অথবা একগুচ্ছ উদ্দেশ্য বাস্তবায়নের জন্য সংশ্লিষ্ঠ বিষয়ে দক্ষ/পারদর্শী কিছু সংখ্যক কর্মীর সমন্বয়ে টিম গঠন করা হয়ে থাকে। আইসিবির তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা কার্যক্রম পরিচালনায় ব্যবস্থাপনা কর্তৃপক্ষের অনুমোদনক্রমে কর্পোরেশনের বিভিন্ন ডিপার্টমেন্ট/শাখা/সাবসিডিয়ারি কোম্পানী হতে সংশ্লিষ্ট বিষয়ে দক্ষ এবং অভিজ্ঞ কর্মচারীর সমন্বয়ে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা টিম গঠন করা যেতে পারে। ব্যবস্থাপনা কর্তৃপক্ষের নির্দেশক্রমে নিরীক্ষা টিমের দলনেতা টিমকে কাজে নিয়োজিত করবেন এবং টিমের সদস্যদের জবাবদিহিতা দলনেতার কাছে থাকবে যিনি কার্যকরভাবে দলের দায়িত্ব পালন নিশ্চিত করার জন্য নিয়োজিত থাকবেন।

৩.৫.২ টিমের ভূমিকা:

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা টিমের প্রধান ভূমিকা ও দায়িত্ব নিম্নে উল্লেখ করা হলঃ

- ঝুঁকি ব্যবস্থাপনা, নিয়ন্ত্রণ এবং পরিচালন ব্যবস্থা মূল্যায়ন ও এগুলো কাঙ্খিতভাবে কাজ করছে মর্মে যুক্তিসংগত নিশ্চয়তা প্রদান করা এবং প্রতিষ্ঠানকে এর উদ্দেশ্য ও লক্ষ্য অর্জনে সক্ষম করা
- ঝুঁকি ব্যবস্থাপনার ক্ষেত্রে অভ্যন্তরীণ নিয়ন্ত্রণ ঘাটতির বিষয়ে উর্ধ্বতন কর্তৃপক্ষের কাছে রিপোর্ট করা এবং দক্ষতা ও কার্যকারিতা উভয় বিচারে প্রতিষ্ঠানের কর্মকান্ডের মান উন্নয়নে সুপারিশ প্রদান করা;
- তথ্যের নিরাপত্তা এবং সম্পৃক্ত ঝুঁকি প্রবণতা নিরূপণ করা;
- নিয়ন্ত্রক বিধি-বিধান পরিপালন কর্মসূচির মূল্যায়ন করা;
- প্রতিষ্ঠানের প্রতারণা-বিরোধী কর্মকান্ডে সহায়তা করা ।

৩.৫.৩ টিমের ধারাবাহিকতা ও মূল্যায়ন:

নিরীক্ষা টিম গঠনে টিমের ভারসাম্যপূর্ণ ধারাবাহিকতা বজায় রাখতে হবে যা নিরীক্ষা প্রক্রিয়ায় তথ্যের গরমিল কমাতে এবং নিরীক্ষা কার্যক্রমের অগ্রগতিতে গুরুত্বপূর্ণ ভূমিকা পালন করবে।

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা কার্যক্রম পরিচালনায় নিরীক্ষা টিমের মূল্যায়ন অত্যন্ত গুরুত্বপূর্ণ । নিরীক্ষা টিমের মূল্যায়ন টিমের শক্তি ও দুর্বলতা চিহ্নিত করে শক্তি বৃদ্ধির মাধ্যমে দুর্বলতা কাটিয়ে ওঠার উপায় বের করতে সহায়তা প্রদান করবে। এ ধরনের মূল্যায়নে প্রাপ্ত ফলাফল নিরীক্ষা টিমকে নিরীক্ষা পদ্ধতি ও প্রক্রিয়ার যথার্থতা এবং নিরীক্ষা কর্মকান্ডের মান নিয়ন্ত্রণ পরিপালনে উৎসাহিত করে।

নিরীক্ষা প্রতিবেদন প্রদানের পর সমাপনী সভায় সর্বসম্মত মূল্যায়ন প্রদান করতে হবে এবং প্রতিষ্ঠানের নিরীক্ষা কর্মকান্ডের কার্য-সম্পাদন মানের উপর ভিত্তি করে কর্মীদের যথার্থ স্বীকৃতি দিতে হবে ।

৩.৫.৪ প্রশিক্ষণ, উন্নয়ন ও নিয়ন্ত্রণ:

একজন তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষককে নিরীক্ষা কার্যক্রম চালাতে প্রয়োজনীয় আবশ্যিক জ্ঞান, দক্ষতা ও সামর্থ্য প্রদর্শনের যোগ্যতা থাকতে হবে। সে লক্ষ্যে প্রতিষ্ঠানকে তাদের তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণের প্রশিক্ষণের ব্যবস্থা করতে হবে যা তাদের নিরীক্ষা কার্যক্রম, ঝুঁকি মূল্যায়ন এবং নিরীক্ষা পরিকল্পনার মত কর্মকান্ড-সম্পাদনে সহায়তা প্রদান করবে। এছাড়া পেশাগত সনদপত্র অর্জনের মাধ্যমে পেশাদারিত্ব ও বিশ্বাসযোগ্যতা বাড়াতে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণকে নিম্নে বর্ণিত সনদগুলো অর্জনে সহায়তা করতে হবে :

- সার্টিফাইড ইনফরমেশন সিস্টেমস অডিটর (CISA)
- সার্টিফাইড ইনফরমেশন সিস্টেমস সিকিউরিটি প্রফেশনাল (CISSP)
- সার্টিফাইড ইনফরমেশন সিস্টেমস সিকিউরিটি ম্যানেজার (CISM)
- সার্টিফাইড ইন দা গভর্নেন্স অব এন্টারপ্রাইজ আইটি (CGEIT)
- সার্টিফাইড ইন রিস্ক এন্ড ইনফরমেশন সিস্টেমস কন্ট্রোল (CRISC)
- সার্টিফাইড ইন্টারনাল অডিটর (CIA)
- সার্টিফাইড ফাইনান্সিয়াল সার্ভিসেস অডিটর (CFSA)
- সার্টিফাইড ফ্রড এক্সজামিনার (CFE)

অধ্যায়-৪

তথ্য ও যোগাযোগ প্রযুক্তি ঝুঁকি ব্যবস্থাপনা (ICT Risk Management)

৪.১ ঝুঁকি ব্যবস্থাপনা:

ঝুঁকি বলতে কর্ম প্রক্রিয়ায় কোন ঘাটতির ফলে কোন ধরনের ভুল, ত্রুটি, অনিয়ম, অসংগতি, জালিয়াতি বা প্রতারণা সংঘটনের সম্ভাবনাকে বোঝায়। কার্যকর ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার তথ্য সার্থক নিরাপত্তা কর্মসূচির গুরুত্বপূর্ণ উপাদান। একটি উন্নয়নশীল দেশের পুঁজিবাজার, অর্থবাজার, বিনিয়োগ ব্যাংকিং-এ নেতৃস্থানীয় প্রতিষ্ঠান হিসেবে আইসিবি-কে সকল প্রকার ব্যবসায়ের অভ্যন্তরীণ ও বাহ্যিক কর্ম পরিবেশের আর্থিক/অনার্থিক ঝুঁকিসমূহসহ বিভিন্ন পদ্ধতিগত ঝুঁকিসমূহ প্রতিনিয়ত ব্যবস্থাপনা করতে হয়। শুধু তথ্য সম্পদই নয় বরং প্রতিষ্ঠানকে এবং এর উদ্দেশ্য বাস্তবায়নের সামর্থ্যকে রক্ষা করাই ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার প্রধান লক্ষ্য। ঝুঁকি ব্যবস্থাপনা তিনটি প্রক্রিয়ার সমন্বয় যার ভিত্তি বিভিন্ন আইন, বিধি-বিধান ও নির্দেশিকার উপর প্রতিষ্ঠিত। প্রক্রিয়া তিনটি হল- ঝুঁকি নিরূপণ, ঝুঁকি নিরসন এবং মূল্যায়ন ।

৪.২ ঝুঁকি নিরূপণ

ঝুঁকি ব্যবস্থাপনা পদ্ধতির প্রথম প্রক্রিয়া হল ঝুঁকি নিরূপণ । সম্ভাব্য ঝুঁকির মাত্রা এবং তথ্য ও যোগাযোগ প্রযুক্তি (ICT) পদ্ধতির সাথে সংশ্লিষ্ট ঝুঁকি নির্ধারণে প্রতিষ্ঠানগুলো ঝুঁকি নিরূপণ করে। এ প্রক্রিয়ার ফলাফল ঝুঁকি নিরসন প্রক্রিয়ায় ঝুঁকি হ্রাস অথবা দূরীকরণে যথাযথ সহায়তা করে ।

ঝুঁকি নিরূপণ পদ্ধতি নয়টি প্রাথমিক ধাপকে অন্তর্ভুক্ত করে যা হলো-

ধাপ ১- পদ্ধতির বৈশিষ্ট্য প্রদান (system characterization)।
ধাপ ২- হুমকি চিহ্নিত করণ (Threat Identification)।
ধাপ ৩- দুর্বলতা চিহ্নিতকরণ (Vulnerability Identification)।
ধাপ ৪- নিয়ন্ত্রণ বিশ্লেষণ (Control Analysis)।
ধাপ ৫- সম্ভাব্যতা নির্ধারণ (Probability Determination)
ধাপ ৬- প্রভাব বিশ্লেষণ (Impact analysis) ।
ধাপ ৭- ঝুঁকি নির্ধারন (Risk Determination) ।
ধাপ ৮- নিয়ন্ত্রণ সুপারিশ (Control Recommendations) ।
ধাপ ৯- ফলাফল লিপিবদ্ধকরণ (Result Documentation) ।

ধাপ ১- পদ্ধতির বৈশিষ্ট্য প্রদান(system characterization):

তথ্য ও যোগাযোগ প্রযুক্তি (ICT) পদ্ধতির ঝুঁকি নিরূপণের প্রথম ধাপ হল কাজের সুযোগ নির্ধারণ করা। এ ধাপে সম্পদ ও পদ্ধতি গঠিত হওয়ার তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতির সীমানা চিহ্নিত করা হয় । এ পদ্ধতির বৈশিষ্টমন্ডিতকরণ ঝুঁকি নিরূপণ কাজের সুযোগ প্রতিষ্ঠা করে। পাশাপাশি এটি পরিচালনগত অনুমোদন (বা স্বীকৃতি) সীমানা নির্ধারণ এবং ঝুঁকি সংজ্ঞায়িত করনে প্রয়োজনীয় তথ্য (যথা- হার্ডওয়্যার, সফটওয়্যার, সিস্টেম কানেক্টিভিটি এবং দায়িত্বপ্রাপ্ত বিভাগ বা সহায়ক ব্যক্তি সম্পর্কে) প্রদান করে।

ধাপ ২- হুমকি চিহ্নিত করণ (Threat Identification):

একটি হুমকি তার নির্দিষ্ট হুমকি উৎসের নির্দিষ্ট দুর্বলতার সফল সদ্ব্যবহার করে। সিস্টেমের দুর্বলতা হচ্ছে এমন একটি দুর্বলতা যা আকস্মিকভাবে অথবা উদ্দেশ্যপ্রণোদিতভাবে সিস্টেমের নিরাপত্তা বিনষ্ট করতে পারে। একটি হুমকি উৎস ততক্ষন পর্যন্ত কোনও ঝুঁকি উপস্থিত করে না যতক্ষন না তার কোন দুর্বলতার সদ্ব্যবহার হয়। হুমকির সম্ভাবনা নির্ধারণের জন্য অবশ্যই হুমকির উৎস, সম্ভাব্য দুর্বলতা এবং বিদ্যমান নিয়ন্ত্রণগুলি বিবেচনায় নিতে হবে ।

১) হুমকির উৎস চিহ্নিতকরণ : কোনো পরিস্থিতি বা ঘটনা যা একটি তথ্য ও যোগাযোগ প্রযুক্তি (ICT) পদ্ধতির ক্ষতি করার সক্ষমতা রাখে তাকেই হুমকির উৎস বলে সংজ্ঞায়িত করা হয় । প্রাকৃতিক, মানবসৃষ্ট বা পরিবেশগত বিষয়গুলোই সাধারণত হুমকির উৎস।

২) হুমকির উৎস:

উৎস	বিবরণ
প্রাকৃতিক হুমকি	বন্যা, ভূমিকম্প, টর্ণেডো, ভূমিধ্বস, তুষারপাত/ধ্বস, বৈদ্যুতিক ঝড়, অগ্নিকান্ড এবং এ ধরনের অন্যান্য ঘটনা।
মানবসৃষ্ট হুমকি	মানুষের দ্বারা সংঘটিত ঘটনা যেমন-অনিচ্ছাকৃত কর্ম (ভুল তথ্য ইনপুট) এবং উদ্দেশ্যমূলক কর্ম (নেটওয়ার্ক ভিত্তিক আক্রমণ, মেলওয়্যার ছড়ানো) ইত্যাদি
পরিবেশগত হুমকি	দীর্ঘ সময় বিদ্যুৎ না থাকা, দূষণ, রাসায়ণিক দ্রব্য, তরল পদার্থ চুইয়ে পড়া ইত্যাদি।

৩) **প্রেরণা ও কার্যাবলী:** প্রণোদনা ও আক্রমণের জন্য প্রয়োজনীয় সম্পদ মানুষকে ব্যাপক হুমকির উৎসে পরিণত করে। বর্তমান সময়ের এমন কিছু সাধারণ মানবসৃষ্ট হুমকি, তাদের সম্ভাব্য প্রেরণা এবং পদ্ধতি বা হুমকিমূলক কার্য যার দ্বারা সে আক্রমণ চালাতে পারে তা নিম্নের ছকে তুলে ধরা হলঃ

উৎস	উদ্দেশ্য	কার্যাবলী
হ্যাকার, ক্রাকার	চ্যালেঞ্জ, অহংবোধ, বিদ্রোহ।	হ্যাকিং; সোসাল ইঞ্জিনিয়ারিং।
অপরাধী	অননুমোদিতভাবে তথ্য ধ্বংস করা ও উপাত্ত পরিবর্তন; অবৈধভাবে তথ্য প্রকাশ; আর্থিক লাভ।	কম্পিউটার সংশ্লিষ্ট অপরাধ (যথা-সাইবার স্টকিং, সাইবার বুলিং); প্রতারণামূলক কাজ (যথা-পুন:প্রদর্শন, ছদ্মবেশ, আড়িপাতা); অবৈধভাবে বিক্রি ; স্পোফিং; সিস্টেমে অনধিকার প্রবেশ।
সন্ত্রাসী	ব্লাকমেইল; ধ্বংস; এক্সপ্লোয়েশন; প্রতিশোধ।	সাইবার বম্বিং; তথ্য যুদ্ধ; সিস্টেমে আক্রমন (যথা-DoS, DDoS); সিস্টেমে অণুপ্রবেশ; সিস্টেমে অবৈধ হস্তক্ষেপ।
গুপ্তচরবৃত্তি	অর্থনৈতিক ও প্রতিযোগিতামূক সুবিধা।	আর্থিক সুবিধা গ্রহন কার্য; তথ্য চুরি; ব্যক্তিগত গোপনীয়তায় অনধিকার প্রবেশ; সোসাল ইঞ্জিনিয়ারিং; ব্যক্তিগত গোপনীয়তায় অনধিকার প্রবেশ; সামাজিক কৌশল; সিস্টেমে অনুপ্রবেশ (শ্রেণীকৃত তথ্য, স্বত্বমূল এবং/অথবা প্রযুক্তি সংশ্লিষ্ট তথ্য)
নিজস্ব জনবল (দুর্বল প্রশিক্ষণ প্রাপ্ত, হতাশ, বঞ্চিত, বিদ্বেষপরায়ণ, অমনোযোগী, অসৎ অথবা চাকুরিচ্যুত কর্মী)	অতিউৎসাহ, অহংবোধ, বুদ্ধিমত্তা; আর্থিক লাভ; প্রতিশোধ; অনিচ্ছাকৃত ভুল-ভ্রান্তি; প্রতারণা ও চুরি (যথা- ভুল ডাটা এন্ট্রি, প্রোগ্রামিং-এ ভুল)।	কোনো কর্মীকে আঘাত; ব্লাকমেইল; স্বত্বমূলক তথ্য সন্ধান; কম্পিউটারের অপব্যবহার; প্রতারণা ও চুরি; অবৈধভাবে তথ্য বিক্রি; ভুল ডাটা এন্ট্রি; ক্ষতিকর কোড (যথা-ভাইরাস, লজিক বম্ব, ট্রোজান হর্স); ব্যক্তিগত তথ্য বিক্রি; সিস্টেম বাগস; সিস্টেমে অনধিকার প্রবেশ; সিস্টেম সেবোটেজ

ধাপ ৩- আক্রম্যতা চিহ্নিতকরণ (Vulnerability Identification):

আক্রম্যতা হ'ল সিস্টেম সুরক্ষা পদ্ধতি, ডিজাইন, বাস্তবায়ন বা অভ্যন্তরীণ নিয়ন্ত্রণগুলির একটি ত্রুটি বা দুর্বলতা যা ব্যবহার করা যেতে পারে। আকস্মিকভাবে অথবা উদ্দেশ্যপ্রণোদিতভাবে সিস্টেমের নিরাপত্তা বিনষ্ট করতে এবং এর ফলে সিস্টেম এর সুরক্ষা ব্যাহত বা সিস্টেমের সুরক্ষা নীতির লঙ্ঘন হতে পারে।

ধাপ ৪- নিয়ন্ত্রণ বিশ্লেষণ (Control Analysis):
একটি সিস্টেমের আক্রম্যতা আঘাত হানার সম্ভাবনা কমাতে অথবা দূরীভূত করতে প্রতিষ্ঠান কর্তৃক বাস্তবায়িত অথবা বাস্তবায়নাধীন নিয়ন্ত্রণ বিশ্লেষণ এ ধাপের লক্ষ্য ।

নিয়ন্ত্রণ পদ্ধতি :- প্রযুক্তিগত এবং অপ্রযুক্তিগত উভয় পদ্ধতিই নিরাপত্তা নিয়ন্ত্রণের অন্তর্ভুক্ত। প্রযুক্তিগত নিয়ন্ত্রণ হল এমন রক্ষাকবচ যা কম্পিউটার হার্ডওয়্যার, সফটওয়্যার অথবা ফার্মওয়্যারে অন্তর্ভুক্ত করা হয় যেমন - প্রবেশ নিয়ন্ত্রণ কৌশল, সনাক্তকরণ ও প্রমাণীকরণ প্রক্রিয়া, এনক্রিপশন (সাধারণ ভাষাকে কোডে রূপান্তর করে তথ্য গোপন করা) পদ্ধতি, অভিপ্রায় নিরুপণ সফটওয়্যার ইত্যাদি। ব্যবস্থাপনা ও পরিচালনা নিয়ন্ত্রণ যেমন- নিরাপত্তা নীতিমালা, পরিচালন প্রক্রিয়া এবং কর্মীর ভৌত ও পরিবেশগত বিষয় অপ্রযুক্তিগত নিয়ন্ত্রণের অন্তর্ভুক্ত।

নিয়ন্ত্রণের শ্রেণীবিভাগ:- অভ্যন্তরীণ নিয়ন্ত্রণ কার্যক্রম এবং সহায়ক প্রক্রিয়া হয় ম্যানুয়াল অথবা স্বয়ংক্রিয় কম্পিউটার তথ্য দ্বারা পরিচালিত। নিম্নে বর্ণিত বৈশিষ্ট্যাবলীসহ নিয়ন্ত্রণের শক্তি মূল্যায়নে নিয়ন্ত্রণের যেসব বিষয় বিবেচনায় নেয়া উচিত সেগুলোকে প্রতিরোধমূলক, সনাক্তকরণমূলক ও সংশোধনমূলক হিসেবে শ্রেণীকরণ করা হয়ঃ

শ্রেণী	বিবরণ
প্রতিরোধমূলক	• সংঘটিত হওয়ার আগে সমস্যা চিহ্নিত করা • পরিচালনা ও যোগান(ইনপুট) উভয় পর্যবেক্ষণ • সংঘটিত হওয়ার আগে সম্ভাব্য সমস্যা চিহ্নিতকরণের চেষ্টা ও সমন্বয় • ভুল, বর্জন অথবা বিদ্বেষপ্রসূত কাজ সংঘটন প্রতিরোধ।
সনাক্তকরণমূলক	• ভুল, বর্জন অথবা বিদ্বেষপ্রসূত কাজ সনাক্তকরণ ও রিপোর্ট করতে নিয়ন্ত্রণ এর ব্যবহার
সংশোধনমূলক	• হুমকির প্রভাব হ্রাসকরণ • সনাক্তকৃত নিয়ন্ত্রণের মাধ্যমে উদঘাটিত সমস্যার সমাধান • সমস্যার কারণ চিহ্নিতকরণ • সমস্যা থেকে উদ্ভূত ভুল সংশোধন • ভবিষ্যতে সমস্যার সংঘটন হ্রাস প্রক্রিয়াকরণ ব্যবস্থার পরিমার্জন।

ধাপ ৫- সম্ভাব্যতা নির্ধারণ (Probability Determination) :

সামগ্রিক সম্ভাব্যতা এর গুণমান প্রাপ্তির জন্য যা সম্ভাব্য দুর্বলতা সম্পর্কিত হুমকির পরিবেশের মধ্যে ব্যবহারের সম্ভাবনা নির্দেশ করে; নিম্নলিখিত প্রশাসনিক কারণগুলি অবশ্যই বিবেচনা করা উচিত :

- হুমকির উৎস প্রেরণা ও সামর্থ্য
- ভেদ্যতার প্রকৃতি
- বর্তমান নিয়ন্ত্রণের অস্তিত্ব ও কার্যকারিতা

একটি জ্ঞাত হুমকির উৎসের সম্ভাব্য আক্রমণ চালানোর সম্ভাবনাকে উচ্চ, মধ্যম ও নিম্ন এ তিন ভাবে বর্ণনা করা যেতে পারে। নিম্নের ছকে এ তিন ধরনের সম্ভাব্যতা পর্যায় উল্লেখ করা হলঃ

পর্যায়	সম্ভাবনা/সম্ভাব্যতা সংজ্ঞা
উচ্চ	হুমকির উৎস উচ্চ প্রেরণা প্রাপ্ত ও যথেষ্ট সক্ষম এবং আক্রমণের চেষ্টা ও ভেদ্যতা প্রতিরোধে নিয়ন্ত্রণ অকার্যকর ।
মধ্যম	হুমকির উৎস প্রেরণা প্রাপ্ত ও সক্ষম কিন্তু ভেদ্যতা প্রতিরোধে নিয়ন্ত্রণ ব্যবস্থা রয়েছে যা আক্রমণের চেষ্টায় বাধা দেবে।
নিম্ন	হুমকির উৎসের প্রেরণা বা সামর্থ্যের অভাব আছে অথবা প্রতিরক্ষা ব্যবস্থা যথা স্থানে রয়েছে যা স্বয়ংক্রিয় প্রতিরোধ করবে অথবা প্রচন্ডভাবে বাধা দেবে ।

ধাপ ৬- প্রভাব বিশ্লেষণ (Impact analysis):

ঝুঁকির মাত্রা পরিমাপে পরবর্তী প্রধান ধাপ হল একটি দূর্বলতা থেকে উদ্ভূত হুমকিসমূহের বিরূপ প্রভাব নিরূপণ। তিনটি নিরাপত্তা লক্ষ্য তথা নির্ভুলতা, পর্যাপ্ততা ও গোপনীয়তা এর যে কোনো একটি অথবা এদের সমন্বিত অবস্থার যে কোন একটি যথাযথভাবে অর্জিত না হলে নিরাপত্তা বিষয়ের বিরূপ প্রভাব বর্ণনা করা সম্ভব। প্রতিটি নিরাপত্তা লক্ষ্য এবং তা যথাযথভাবে অর্জিত না হলে তার পরিনতি বা প্রভাবের সংক্ষিপ্ত বর্ণনা নিম্নে ব্যাখ্যা করা হলোঃ

আর্থিক ক্ষতির পরিমাণ, সিস্টেম মেরামত খরচ অথবা সফল হুমকি কর্মাকান্ডের ফলে সৃষ্ট সমস্যাসমূহ সমাধানের জন্য গৃহীত প্রয়োজনীয় পদক্ষেপসমূহের দ্বারা পরিমানগতভাবে কিছু বাস্তবসম্মত প্রভাবের পরিমাপ নির্ধারণ করা যেতে পারে। অন্যান্য প্রভাবসমূহ (যেমন-জনগণের আস্থা হারানো, বিশ্বাসযোগ্যতা নষ্ট, প্রতিষ্ঠানের স্বার্থের ক্ষতি) কোনো নির্দিষ্ট একক দ্বারা পরিমাপ করা যায় না তবে উচ্চ, মধ্যম ও নিম্ন গুনসম্পন্ন প্রভাব হিসেবে বিবেচনা বা বর্ণনা করা যায়। প্রভাবের শ্রেণীগত বৈশিষ্ঠের কারণে শুধুমাত্র উচ্চ, মধ্যম ও নিম্ন এই তিন গুণগত পর্যায়কেই চিহ্নিত ও বর্ণনা করা হলোঃ

পর্যায়	প্রভাব
উচ্চ	উচ্চ পর্যায় বলতে (১) উল্লেখযোগ্য পরিমান সম্পদ বা সংস্থানের ব্যাপক ব্যয়বহুল ক্ষতি; (২) প্রতিষ্ঠানের উদ্দেশ্য, সুনাম বা স্বার্থ ব্যাপকভাবে বিঘ্নিত, ক্ষতিগ্রস্থ বা বাধাগ্রস্থ হওয়া; অথবা (৩) লোকবলের মৃত্যু বা মারাত্মকভাবে আহত হওয়া ইত্যাদি বোঝায়।
মধ্যম	মধ্যম পর্যায় বলতে (১) সম্পদ বা সংস্থানের ব্যয়বহুল ক্ষতি; (২) প্রতিষ্ঠানের উদ্দেশ্য, সুনাম বা স্বার্থ বিঘ্নিত, ক্ষতিগ্রস্থ বা বাধাগ্রস্থ হওয়া; অথবা (৩) লোকবলের আহত হওয়া ইত্যাদি বোঝায়।
নিম্ন	নিম্ন পর্যায় বলতে (১) কিছু সম্পদ বা সংস্থানের ক্ষতি; অথবা (২) প্রতিষ্ঠানের উদ্দেশ্য, সুনাম বা স্বার্থে উল্লেখযোগ্য প্রভাব পড়া ইত্যাদি বোঝায়।

ধাপ ৭- ঝুঁকি নিরূপণ (Risk Determination):

তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতির ঝুঁকির মাত্রা নিরূপণ এ ধাপের উদ্দেশ্য। একটি নির্দিষ্ট আক্রম্যতা ঝুঁকি নির্ধারণকে নিম্নে বর্ণিত বিষয়ের কার্যাবলী হিসেবে প্রকাশ করা যেতে পারে-

- একটি জ্ঞাত হুমকি উৎসের চেনা ভেদ্যতা প্রচেষ্টার সম্ভাব্যতা;
- হুমকি-উৎসের সফল ভেদ্যতার প্রভাবের মাত্রা;
- ঝুঁকি হ্রাস বা দূরীকরণে পরিকল্পিত বা বিদ্যমান নিয়ন্ত্রণের পর্যাপ্ততা।।

ঝুঁকি পরিমাপে একটি ঝুঁকি পরিমাপক কাঠামো এবং একটি ঝুঁকি-মাত্রা পরিমাপক কাঠামো অবশ্যই উদ্ভাবন করতে হবে।

ঝুঁকি-মাত্রা পরিমাপক কাঠামো:- উদ্দেশ্যঝুঁকি (mission risk) হল হুমকির সম্ভাবনা ও হুমকির প্রভাবের জন্য নির্ধারিত মানের গুণফল। হুমকির সম্ভাবনা ও হুমকির প্রভাবের শ্রেণীতে প্রদেয় ভরণের (inputs) উপর ভিত্তি করে কিভাবে সামগ্রিক ঝুঁকি মান (risk ratings) নির্ধারণ করা হয় তা নিচের ছকে তুলে ধরা হল। নিচের ছাঁচটি (matrix) হুমকির সম্ভাব্যতা (উচ্চ, মধ্যম ও নিম্ন) এবং হুমকি প্রভাবের (উচ্চ, মধ্যম ও নিম্ন) একটি ৩ X ৩ ম্যাট্রিক্স (matrix)।

নিচের নমুনা ছকে কিভাবে সামগ্রিক উচ্চ, মধ্যম ও নিম্ন মাত্রার ঝুঁকি নিরূপণ করা হয় তা দেখানো হল। এসব ঝুঁকির মাত্রা অথবা মান নির্ধারণ বিষয়কেন্দ্রিক হতে পারে। এ বিবেচনার যৌক্তিকতা প্রতিটি হুমকি সম্ভাব্যতার মাত্রা ও প্রতিটি সম্ভাব্য প্রভাবের গুরুত্ব বিচারে ব্যাখ্যা করা যেতে পারে। উদাহরণস্বরূপ:-

- প্রতিটি হুমকি সম্ভব্যতার উচ্চ মাত্রার জন্য ১.০, মধ্যম মাত্রার জন্য ০.৫ এবং নিম্ন মাত্রার জন্য ০.১ সম্ভাবনা নির্ধারণ;
- প্রতিটি উচ্চ মাত্রার প্রভাবের জন্য ১০০, মধ্যম মাত্রার জন্য ৫০ এবং নিম্ন মাত্রার জন্য ১০ মান নির্ধারণ।

হুমকির সম্ভাবনা (সম্ভাব্যতা)	প্রভাব		
	নিম্ন (১০)	মধ্যম (৫০)	উচ্চ (১০০)
উচ্চ (১.০)	নিম্ন (১০×১.০=১০)	মধ্যম (৫০) (৫০×১.০=৫০)	উচ্চ (১০০) (১০০×১.০=১০০)
মধ্যম (০.৫)	নিম্ন (১০×০.৫=৫)	মধ্যম (৫০) (৫০×০.৫=২৫)	উচ্চ (১০০) (১০০×০.৫=৫০)
নিম্ন (০.১)	নিম্ন (১০×০.১=০১)	মধ্যম (৫০) (৫০×০.১=৫)	উচ্চ (১০০) (১০০×০.১=১০)

ঝুঁকির মাত্রাঃ উচ্চ (>৫০ থেকে ১০০); মধ্যম (>১০ থেকে ৫০); নিম্ন (>১ থেকে ১০);

ঝুঁকির মাত্রার বিবরণ:- নিচের ছকে উপরে চিত্রিত ছক এর বিবরণ দেয়া হল। এই ঝুঁকি পরিমাপক উচ্চ, মধ্যম ও নিম্ন মানসহ জ্ঞাত ভেদ্যতার (vulnerability) ক্ষেত্রে একটি তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতি, সুবিধা বা প্রক্রিয়া কতটুকু ঝুঁকিপূর্ণ তা তুলে ধরা হল। প্রতিটি ঝুঁকির ক্ষেত্রে উধর্বতন ব্যবস্থাপনা কর্তৃপক্ষ, প্রতিষ্ঠানের মালিককে অবশ্যই যে ব্যবস্থা গ্রহণ করতে হবে তা নিম্নের ছকে তুলে ধরা হলো:-

ঝুঁকির মাত্রা	ঝুঁকির মাত্রার বিবরণ ও প্রয়োজনীয় পদক্ষেপ।
উচ্চ	যদি কোনো পর্যবেক্ষণ বা প্রাপ্ত ফলাফলকে উচ্চ ঝুঁকি বলে মূল্যায়ন করা হয় সেখানে একটি সংশোধনীমূলক জোরালো পদক্ষেপ গ্রহণের প্রয়োজন পড়বে। এ ক্ষেত্রে একটি বিদ্যমান ব্যবস্থা কার্যক্রম অব্যাহত রাখতে পারে, তবে যত শীঘ্র সম্ভব একটি সংশোধনীমূলক কর্মপরিকল্পনা অবশ্যই গ্রহণ করতে হবে।
মধ্যম	কোনো পর্যবেক্ষণকে মধ্যম ঝুঁকি হিসেবে চিহ্নিত করা হলে সেখানে একটি সংশোধনীমূলক ব্যবস্থা গ্রহণের প্রয়োজন হবে এবং একটি নির্দিষ্ট সময়ের মধ্যে এ ব্যবস্থা কার্যকর করার জন্য অবশ্যই একটি পরিকল্পনা করতে হবে।
নিম্ন	কোনো পর্যবেক্ষণকে নিম্ন ঝুঁকি হিসেবে চিত্রিত করা হলে সেখানে সংশোধনীমূলক ব্যবস্থার প্রয়োজন আছে কিনা তা নির্ধারণ করতে হবে অথবা সে ঝুঁকি গ্রহণের সিদ্ধান্ত নিতে হবে।

ধাপ ৮: নিয়ন্ত্রণ সুপারিশ (Control Recommendations) :
সুপারিশকৃত নিয়ন্ত্রণের লক্ষ্য হল তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতি ও এর উপাত্তের ঝুঁকির মাত্রা একটি গ্রহণযোগ্য পর্যায়ে নামিয়ে আনা। চিহ্নিত ঝুঁকি হ্রাসে বা দূরীকরণে নিয়ন্ত্রণ ও বিকল্প সমাধান সুপারিশের ক্ষেত্রে নিম্নের বিষয়গুলো বিবেচনায় নিতে হবেঃ

- সুপারিশকৃত বিকল্পের কার্যকারিতা (যথা- সিস্টেম উপযোগিতা);
- আইন ও বিধি-বিধান;
- প্রাতিষ্ঠানিক নীতিমালা;
- পরিচালনগত প্রভাব;
- নিরাপত্তা ও নির্ভরযোগ্যতা।

ধাপ ৯: ফলাফল লিপিবদ্ধকরণ(Result Documentation):
ঝুঁকি মূল্যায়ন শেষে হুমকির উৎস ও ভেদ্যতা (vulnerability) চিহ্নিত করা, ঝুঁকি নিরূপণ এবং সুপারিশকৃত নিয়ন্ত্রণ আরোপ করা এর ফলাফল আনুষ্ঠানিক রিপোর্ট বা ব্রিফিং এ নথিভূক্ত করতে হবে।

৪.৩ ঝুঁকি হ্রাসকরণ:
ঝুঁকি ব্যবস্থাপনার দ্বিতীয় প্রক্রিয়া ঝুঁকি হ্রাসকরণ। ঝুঁকি নিরূপণ প্রক্রিয়া থেকে এর গুরুত্ব নির্ধারণ, মূল্যায়ন এবং সুপারিশকৃত যথাযথ ঝুঁকি হ্রাসকারী নিয়ন্ত্রণ চালুকরণ এর অন্তর্ভুক্ত।

৪.৪ ঝুঁকি নিরসন উপায় :
প্রতিষ্ঠানের ঝুঁকি হ্রাসে উধর্বতন ব্যবস্থাপনা কর্তৃপক্ষ কর্তৃক ব্যবহৃত একটি নিয়মতান্ত্রিক পদ্ধতি হল ঝুঁকি নিরসন। নিম্নোক্ত যে কোনো ঝুঁকি নিরসন বিকল্পের মাধ্যমে ঝুঁকি হ্রাস করা যায়:

ঝুঁকি ধারণা- সম্ভাব্য ঝুঁকি মেনে নিয়ে তথ্য ও যোগাযোগ প্রযুক্তি পদ্ধতি পরিচালনা অব্যাহত রাখা অথবা ঝুঁকিকে একটি গ্রহণযোগ্য মাত্রায় নামিয়ে আনতে নিয়ন্ত্রণ আরোপ করা।

ঝুঁকি এড়ানো- ঝুঁকির কারণ এবং/অথবা ফলাফল দূর করে ঝুঁকি এড়ানো (যথা- সিস্টেমের কিছু কাজ অথবা ঝুঁকি চিহ্নিত হলে সিস্টেম বন্ধ করে দেয়া)।

ঝুঁকি সীমিতকরণ- হুমকির আক্রমণের ক্ষতিকর প্রভাব হ্রাসে নিয়ন্ত্রণ আরোপ করে ঝুঁকি সীমিত করা।

ঝুঁকি পরিকল্পনা- ঝুঁকির গুরুত্ব নির্ধারণ, নিয়ন্ত্রণ বাস্তবায়ন ও বজায় রাখতে ঝুঁকি দূরীকরণ পরিকল্পনার মাধ্যমে ঝুঁকি ব্যবস্থাপনা।

গবেষণা ও স্বীকৃতি- ভেদ্যতা (vulnerability) বা ত্রুটি স্বীকার ও একটি সংশোধনে গবেষণার মাধ্যমে নিয়ন্ত্রণ নির্ধারণ করে ক্ষতির ঝুঁকি কমিয়ে আনা।

ঝুঁকি স্থানান্তর- ক্ষতি পূরণে বীমা করার মত অন্যান্য বিকল্প ব্যবহার করে ঝুঁকি স্থানান্তর করা।

৪.৫ ঝুঁকি নিরসন কৌশল:

উর্ধ্বতন কর্তৃপক্ষ, প্রতিষ্ঠান প্রধান সম্ভাব্য ঝুঁকি ও সুপারিশকৃত নিয়ন্ত্রণ জেনে কখন, কোন কোন পরিস্থিতিতে পদক্ষেপ নিতে হবে এবং ঝুঁকি নিরসনে এবং প্রতিষ্ঠান রক্ষায় কখন এসব নিয়ন্ত্রণ আরোপ করতে হবে তা ঝুঁকি নিরসন কৌশলের মাধ্যমে নির্ধারন করবেন।

- **যখন ত্রুটি বা দুর্বলতা বিদ্যমান থাকে:** ত্রুটি বা দুর্বলতা কমাতে নিশ্চত কৌশল বাস্তবায়ন।
- **যখন আক্রম্যতা (vulnerable) প্রচেষ্টা চলমান:** আক্রমণ হ্রাস অথবা ঠেকাতে লেয়ারড প্রটেকশন, স্থাপনাগত নকশা এবং পরিচালনাগত নিয়ন্ত্রণ প্রয়োগ করা।
- **সম্ভাব্য লাভের তুলনায় যখন আক্রমণকারীর ব্যয় কম হয়:** আক্রমণকারীর ব্যয় বাড়িয়ে আক্রমণকারীর প্রেরণা হ্রাসে প্রতিরোধমূলক ব্যবস্থা গ্রহণ (যেমন- পদ্ধতি ব্যবহারকারী কি পেতে পারে এবং করতে পারে তা নির্ধারণ করার মত পদ্ধতি নিয়ন্ত্রণ ব্যবহার)।
- **যখন ক্ষতি অনেক বেশী:** আক্রমণের তীব্রতা সীমিত করতে নকশা নীতি, স্থাপত্য নকশা এবং প্রযুক্তিগত ও অপ্রযুক্তিগত সুরক্ষা ব্যবহার করে ক্ষতির সম্ভাবনা কমিয়ে আনা।

৪.৬ ঝুঁকি মূল্যায়ন ও নিরূপণ:

ঝুঁকি ব্যবস্থাপনা একটি চলমান ও বিবর্তনশীল প্রক্রিয়া। এ অংশে উত্তম অনুশীলন ও একটি চলমান ঝুঁকি মূল্যায়ন ও নিরূপণ প্রক্রিয়ার প্রয়োজনীয়তা এবংএকটি সফল ঝুঁকি ব্যবস্থাপনা কর্মসূচির সাথে জড়িত বিষয়ের উপর গুরুত্বারোপ করা হয়েছে।

৪.৬.১ উত্তম নিরাপত্তা অনুশীলন:

শুধু আইন অথবা বিধি-বিধানের বাধ্যবাধকতার জন্যই নয় বরং একটি ভাল অনুশীলন এবং প্রতিষ্ঠানের ব্যবসায়িক উদ্দেশ্য সহায়ক বলে ঝুঁকি ব্যবস্থাপনা এবং তথ্য ও যোগাযোগ প্রযুক্তির SDLC প্রতিটি ধাপে সংযোজন করা দরকার। এখানে উল্লেখ করা প্রয়োজন যে, তথ্য ও যোগাযোগ প্রযুক্তি সিস্টেম-এ SDLC এর পাঁচটি পর্যায় রয়েছে। এগুলো হলো: শুরু করা, উন্নয়ন বা অধিগ্রহণ, বাস্তবায়ন, পরিচালনা বা রক্ষণাবেক্ষণ এবং অপসারণ এর যে কোনো পর্যায়ের জন্যই মূল্যায়ন করা হোক না কেন ঝুঁকি ব্যবস্থাপনা পদ্ধতি একই। তদুপরি, প্রতিষ্ঠানের ঝুঁকি নিরূপণ ও দূরীকরণে একটি সুনির্দিষ্ট কর্মসূচি থাকা উচিত। অধিকন্তু নীতিমালা ও নতুন প্রযুক্তির উদ্ভাবনে ফলে তথ্য ও যোগাযোগ প্রযুক্তি সিস্টেম এ এবং প্রক্রিয়াকরণ পরিবেশে বড় পরিবর্তনের পর্যায়ক্রমিক সম্পাদিত প্রক্রিয়াও যথেষ্ট নমনীয় হওয়া বাঞ্ছনীয়।

৪.৬.২ সফলতার চাবি-কাঠি:

একটি সফল ঝুঁকি ব্যবস্থাপনা কার্যক্রম পাঁচটি বিষয়ের উপর নির্ভর করে। যথা-

(১) উধর্বতন ব্যবস্থাপনা কর্তৃপক্ষের প্রত্যয়;
(২) আইসিটির পূর্ণ সমর্থন ও অংশ গ্রহণ;
(৩) ঝুঁকি নিরূপণকারী দলের সামর্থ্য (যার অবশ্যই একটি নির্দিষ্ট ক্ষেত্র ও সিস্টেমে ঝুঁকি ব্যবস্থাপনা পদ্ধতি প্রয়োগের দক্ষতা, প্রতিষ্ঠানের ঝুঁকি চিহ্নিত করা এবং প্রতিষ্ঠানের চাহিদানুযায়ী ব্যয় সাশ্রয়ী সুরক্ষা দিতে হবে);
(৪) ব্যবহারকারী সুবিধাভোগীদের সচেতনতা ও সহযোগিতা (যারা অবশ্যই নিয়ম অনুসরণ করবে এবং তাদের প্রতিষ্ঠানের উদ্দেশ্য সুরক্ষায় আরোপিত নিয়ন্ত্রণ পরিপালন করবে) এবং
(৫) অব্যাহতভাবে আইসিটি সংশ্লিষ্ট কর্মসূচির ঝুঁকি মূল্যায়ন ও নিরূপণ।

অধ্যায়-৫
তথ্য ও যোগাযোগ প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষা

৫.১। তথ্য প্রযুক্তি নিয়ন্ত্রন:

বর্তমানে আর্থিক প্রতিষ্ঠানের কার্যক্রম পরিচালনায় তথ্য প্রযুক্তির ব্যবহার ব্যাপক হারে বৃদ্ধি পাওয়ায় পদ্ধতিসমূহকে পর্যাপ্তভাবে নিয়ন্ত্রণ সুরক্ষা প্রদান, রেকর্ডসমূহ সঠিকভাবে রক্ষণাবেক্ষণ করা এবং ঝুঁকি গ্রহণযোগ্যভাবে হ্রাস করার জন্য তথ্য প্রযুক্তির নিয়ন্ত্রণ অত্যন্ত গুরুত্বপূর্ন। তথ্য প্রযুক্তির নিয়ন্ত্রন হলো এমন একটি প্রক্রিয়া বা নীতিমালা যা একটি প্রতিষ্ঠানে ব্যবহৃত তথ্য প্রযুক্তি গুলিকে এমনভাবে পরিচালনা করে যা যথার্থ , তথ্য নির্ভর এবং সংগঠন প্রযোজ্য আইন ও বিধিবিধান মেনে চলার মাধ্যমে প্রতিষ্ঠানের কাঠমোর স্বচ্ছতা এবং যথার্থতা নিশ্চিত করে । এটি প্রতিষ্ঠানের অভ্যন্তরীণ নিয়ন্ত্রনের একটি উপসেট । তথ্য প্রযুক্তির নিয়ন্ত্রনের লক্ষ্যসমূহ গোপনীয়তা, অখন্ডতা এবং ডাটা উপলভ্যতা এবং ব্যবসায়িক উদ্যোগের তথ্য প্রযুক্তিগত পদ্ধতির সাথে সম্পর্কিত।
যে সকল ম্যানুয়াল এবং প্রোগ্রামড নীতিমালা /পদ্ধতি তথ্য সম্পদের সুরক্ষা, এর রেকর্ডের যথার্থতা, নির্ভরযোগ্যতা নিশ্চিত করে তা তথ্য প্রযুক্তি নিয়ন্ত্রণের অর্ন্তভূক্ত । তথ্য প্রযুক্তির নিয়ন্ত্রণ সাধারনত তিনটি শেণীতে ভাগ করা যেতে পারে:-

সাধারণ নিয়ন্ত্রণ (General control):

সাধারণ নিয়ন্ত্রণ হলো তথ্য প্রযুক্তি কাঠামোর মৌলিক নিয়ন্ত্রণ। এটি তথ্য প্রযুক্তি দ্বারা উৎপন্ন ডাটার নির্ভরযোগ্যতা , সিস্টেমের স্বয়ংক্রিয় পরিচালনা এবং নির্ভরযোগ্য আউটপুট নিশ্চিত করে। নিয়ন্ত্রণ ক্যাটাগরিতে তথ্য প্রযুক্তিগত নীতি, পদ্ধতি, মান, অপারেশনাল, প্রোগ্রাম, ডাটা নিয়ন্ত্রণ এবং আদানপ্রদান , প্রযুক্তিগত সহায়তা নীতি এবং পদ্ধতি, হার্ডওয়্যার সফটওয়্যারের বিকাশ, দুর্যোগ পুনরুদ্ধার/ ব্যাকআপ পদ্ধতি, ইভেন্ট ম্যানেজমেন্ট অন্তর্ভুক্ত রয়েছে।

অ্যাপ্লিকেশন নিয়ন্ত্রণ (Application control):

অ্যাপ্লিকেশন নিয়ন্ত্রণগুলিকে লেনদেন প্রক্রিয়াজাতকরন নিয়ন্ত্রণ অথবা "ইনপুট-প্রসেসিং-আউটপুট" নিয়ন্ত্রণ বলে। এটি সম্পূর্নরূপে স্বয়ংক্রিয় আউটপুট মাধ্যমে ইনপুট থেকে ডেটা সম্পূর্ন ও সঠিক প্রক্রিয়াকরন নিশ্চিত করতে ব্যবহৃত হয়। এই নিয়ন্ত্রণগুলি নির্দিষ্ট অ্যাপ্লিকেশনটির ব্যবসায়ের উদ্দেশ্য অনুসারে পরিবর্তিত হয়। এই নিয়ন্ত্রণগুলি অ্যাপ্লিকেশনগুলির মধ্যে ব্যবহৃত ডেটার গোপনীয়তা এবং সুরক্ষা নিশ্চিত করতে সহায়তা করতে পারে। অ্যাপ্লিকেশন ক্যাটাগরিতে সম্পূর্নতা পরীক্ষা, বৈধতা পরীক্ষা, সনাক্তকরণ, প্রমাণীকরণ, অনুমোদন, ইনপুট নিয়ন্ত্রণ এবং ফরেনসিক নিয়ন্ত্রণ অন্তর্ভুক্ত রয়েছে।

নির্দিষ্ট নিয়ন্ত্রণ (Specific control): নির্দিষ্ট নিয়ন্ত্রণের মধ্যে অর্ন্তভূক্ত নেটওয়্যার্ক, ইন্টারনেট, ইন্ড ইউজার কমপিউটিং এবং তথ্য প্রযুক্তি নিরাপত্তা।

এই কাঠামোর অধীনে স্বতন্ত্র কম্পিউটার নিয়ন্ত্রণ দুই ভাবে শ্রেণীবিন্যাস করা যায়:

প্রোগ্রামড:- প্রোগ্রামড নিয়ন্ত্রণ হলো পূর্বনির্ধারিত প্রোগ্রাম অনুসারে কোনও অবজেক্টের অপারেশন মোডের নিয়ন্ত্রণ।

ম্যানুয়াল:- ম্যানুয়াল নিয়ন্ত্রণ হলো ব্যক্তি দ্বারা ম্যানুয়ালি সঞ্চালিত নিয়ন্ত্রণ। এটি নিয়ন্ত্রণের অন্তর্নির্মিত অভাব এর জন্য ক্ষতিপূরণমূলক কাজ হিসাবে সজ্ঞায়িত করা যায়।

- প্রোগ্রামড নিয়ন্ত্রণ যতবেশি কার্যকর হয়, ম্যানুয়াল নিয়ন্ত্রণ ততকম ব্যবহার করা হয়।
- প্রোগ্রামড এবং ম্যানুয়াল নিয়ন্ত্রণের মধ্যে ভারসাম্য যতবেশি হয় তথ্য ও যোগাযোগ প্রযুক্তির নিয়ন্ত্রণ ততোবেশি কার্যকর হয়।
- নিয়ন্ত্রণ কে প্রতিরোধমূলক, ডিটেকটিভ বা সংশোধক হিসাবে শ্রেণীবদ্ধ করা যেতে পারে।
- তথ্য প্রযুক্তির নিরীক্ষণটি প্রোগ্রামড এবং প্রতিরোধমূলক নিয়ন্ত্রণের প্রয়োগকে উৎসাহ প্রদান করে।

৫.২। নিয়ন্ত্রন ব্যর্থতার ফলাফল:

তথ্য প্রযুক্তির নিয়ন্ত্রন ব্যর্থতা গুলি হলো:-

- ব্যবসায়িক উদ্দেশ্য অনুসারে কম্পিউটার অ্যাপ্লিকেশনের অনুপযুক্ততা;
- অননুমোদিত তথ্য সংক্রান্ত পরিবর্তন;
- তথ্যের অখন্ডতা হ্রাস;
- অননুমোদিত ভাবে তথ্য সংক্রান্ত প্রবেশ এবং তথ্য উন্মোচন;
- ধারাবাহিক ভাবে সেবাপ্রদানের অভাব;
- উন্নয়নমূলক সম্পদ/ সংস্থানের অপচয়।

৫.৩। তথ্য প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষা পরিচালনা:

তথ্য ও যোগাযোগ প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষা প্রাথমিক ভাবে ঝুঁকি ও পদ্ধতি ভিত্তিক। তথ্য ও যোগাযোগ প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার ধাপগুলি বর্ননা করা হলো:

ক) একটি প্রাথমিক জরিপ পরিচালনা করা যা:

- পদ্ধতি/সিস্টেম এবং এর সীমাবদ্ধতা সম্পর্কে বিস্তারিত ধারনা প্রদান করে;
- মূল ঝুঁকিপূর্ণ ক্ষেত্রগুলি চিহ্নিত করা।

খ) সম্ভাব্য ঝুঁকিসমূহ মূল্যায়ন।

গ) ঝুঁকি বিশ্লেষণের ফলাফলের ভিত্তিতে তথ্য ও যোগাযোগ প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার বিশদ পরিকল্পনা ।

ঘ) নিয়ন্ত্রণের উদ্দেশ্য এবং প্রত্যাশিত নিয়ন্ত্রণগুলি সনাক্তকরণ।

ঙ) প্রকৃত নিয়ন্ত্রনের বিপরীতে প্রত্যাশিত নিয়ন্ত্রন নথিভূক্তকরণ ।

চ) একটি প্রাথমিক মূল্যায়ন পরিচালনা।

ছ) নিরীক্ষা কার্যক্রম যাচাই এবং পরিকল্পনা করা।

জ) ক্লায়েন্টের সাথে সুপারিশগুলি সম্মতিকরন।

ঝ) যথাযথ বিবরণী।

৫.৩.১ প্রাথমিক জরিপ পরিচালনা:

- যে কোন প্রতিষ্ঠানের তথ্য ও যোগাযোগ প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার কর্মপরিকল্পনায় প্রতিষ্ঠানের সমগ্রিক তথ্য ও যোগাযোগ পদ্ধতির প্রাথমিক মূল্যায়নের উল্লেখযোগ্য বিষয়গুলি হলো:-
  - কম্পিউটার ফাংশনসমূহের সংগঠন;
  - কম্পিউটার হার্ডওয়্যার এবং সফটওয়্যারের ব্যবহার;
  - অ্যাপ্লিকেশন প্রক্রিয়াজাতকরণ এবং তাদের আপেক্ষিক তাৎপর্য;
  - বিদ্যমান অ্যাপ্লিকেশনের পরিবর্তন, নতুন অ্যাপ্লিকেশনের বিকাশের পদ্ধতি/প্রক্রিয়াসমূহ;

- প্রাথমিক সমীক্ষা মূল্যায়নের জন্য যেসব ভিত্তি সরবরাহ করবে তা হলো:-
  - তথ্য ও যোগাযোগ প্রযুক্তির প্রাসঙ্গিক নিরীক্ষা পদ্ধতির সাথে সংশ্লিষ্ট ঝুঁকিসমূহ;
  - অভ্যন্তরীন নিরীক্ষা প্রক্রিয়া যাচাই এবং কমার্শিয়াল অডিটর দ্বারা পরীক্ষার মান উন্নয়নে CAATs (Computer Assisted Audit Techniques and tools) এর সক্ষমতা;
  - তথ্য ও যোগাযোগ প্রযুক্তিবিহীন নিরীক্ষার মূলনীতি সম্পর্কে ধারনা (যেমন দুর্বল নিয়ন্ত্রণ কমার্শিয়াল অডিটর দ্বারা আরও স্থিতিশীল কাজের প্রয়োজনীয় পরামর্শ প্রদান করে)

৫.৩.২ কম্পিউটারাইজড পদ্ধতি/পরিবেশ/সিস্টেম এ ঝুঁকির মূল্যায়ন :

- তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষণের সংস্থান সর্বাধিক ঝুঁকিপূর্ণ অঞ্চলে পরিচালিত হওয়া প্রয়োজন যা প্রতিষ্ঠানের নিরীক্ষার মতামতকে সমর্থন প্রদান করে।
- কম্পিউটারাইজড পদ্ধতিতে ঝুঁকি বিশ্লেষণের অংশ হিসাবে ব্যবহারের জন্য ঝুঁকির কোনও নির্দিষ্ট সেট না থাকলেও নিম্নলিখিত ঝুঁকির নিয়ামকসমূহ উল্লেখযোগ্য:
  - সিস্টেম দ্বারা প্রক্রিয়াজাত লেনদেনের মান;
  - সিস্টেমটি সঠিকভাবে পরিচালনার উপর প্রতিষ্ঠান কতটা নির্ভরশীল;
  - স্থিতিশীলতা, দুর্বল নিয়ন্ত্রণের কোনও ইতিহাস, পরিচিত সিস্টেমের দুর্বলতা, অভ্যন্তরীণ নিয়ন্ত্রণের প্রয়োজনীয় স্তর, জটিলতা ইত্যাদি ক্ষেত্রে সিস্টেমের দুর্বলতা;
  - যখন প্রতিষ্ঠানের গোপনীয় তথ্য প্রকাশিত হয় , প্রতিষ্ঠানের ক্ষতি হয় অথবা সিস্টেমে কোন ব্যর্থতা থাকে সেক্ষেত্রে প্রতিষ্ঠানের ঝুঁকিসমুহের নিজস্ব মূল্যায়ন কার্যক্রম পরিচালনা করা ।

৫.৩.৩ তথ্য প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার নির্দিষ্ট পরিকল্পনা:

- প্রাথমিক সমীক্ষার ফলাফলের উপর নির্ভর করে আইসিটি নিরীক্ষকগণ সিদ্ধান্ত গ্রহন করেন তারা নিরীক্ষা সংক্রান্ত মতামত প্রদান করবেন অথবা প্রয়োজনীয় সিদ্ধান্ত গ্রহনের জন্য পরবর্তী পর্যায়ে নিরীক্ষার কাজ চালিয়ে যাবেন।

তথ্য প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার পরিকল্পনা অত্যন্ত সতর্কতার সাথে করা উচিত, যেমন:-

- নিরীক্ষার ক্ষেত্রগুলি এত বিস্তৃত এবং অবান্তর হওয়া উচিত নয় যাতে তা ব্যর্থতার সম্ভাব্যতা, বিশ্বাসযোগ্যতার হ্রাস এবং নীতিভ্রষ্টতা কে বাড়িয়ে দেয়।
- অপরিকল্পিত কাজের দ্বারা পরিকল্পিত কাজ যাতে ক্ষতিগ্রস্থ না হয়।
- তথ্য প্রযুক্তি নিয়ন্ত্রিত নিরীক্ষার পরিকল্পনা করার সময় সাধারণত নিরীক্ষক দ্বারা যে তথ্য প্রযুক্তি নিয়ন্ত্রন এবং নিরীক্ষা জ্ঞানের মাধ্যমে তথ্য প্রযুক্তি সংক্রান্ত নিরীক্ষা কাজ সম্পন্ন করা যেতে পারে তার সম্পূর্ণ স্বীকৃতি দিতে হবে।
- নিরীক্ষা প্রক্রিয়ার সংহতকরণকে প্রচারের লক্ষ্যে যৌথ কম্পিউটার এবং আর্থিক নিরীক্ষণ ইনপুটকে উৎসাহিত করা প্রয়োজন।

৫.৩.৪ বিভিন্ন ধরণের কম্পিউটার নিয়ন্ত্রিত নিরীক্ষা:-

- কম্পিউটার ইনস্টলেশন এর সাধারণ নিয়ন্ত্রণ পর্যালোচনা;
- তথ্য ও যোগাযোগ প্রযুক্তির সুবিধাসমূহ সংগ্রহ;
- বিদ্যমান কম্পিউটার অ্যাপ্লিকেশনসমূহের পর্যালোচনা;
- নতুন অ্যাপ্লিকেশনের উন্নয়ন এবং পরিবর্ধন;
- ডেটা রূপান্তর পর্যালোচনা।

৫.৩.৫ সিস্টেম বেজড অডিট পদ্ধতি (SBA):

সিস্টেম বেজড অডিট হলো এমন একটি প্রক্রিয়া যা নিরীক্ষিত বিষয়ের অভ্যন্তরীন নিয়ন্ত্রন পদ্ধতির উপর নির্ভর করে থাকে। বেশিরভাগ কম্পিউটার নিয়ন্ত্রিত পর্যালোচনা সংক্রান্ত কাজ সিস্টেম বেজড অডিট (SBA) ব্যবহার করে চালানো হয়ে থাকে।

সিস্টেম বেজড অডিট (SBA) এর ধাপসমূহ:

ধাপ-১: নিরীক্ষার সুযোগ নিশ্চিতকরণ;

ধাপ-২: নিরীক্ষার বিষয়ের সাথে পরিচয় ;

ধাপ-৩: পূর্বের নিরীক্ষা পেপার পর্যালোচনা;

ধাপ-৪: প্রাথমিক পর্যালোচনা;

- নিরীক্ষণের পদ্ধতি
- কর্মীদের বরাদ্দ
- সময়
- দায়িত্বশীল কর্মকর্তার সাথে সাক্ষাৎ

ধাপ-৫: প্রাক নিরীক্ষা কাজ;

- বিশ্লেষণমূলক পর্যালোচনা
- একত্রিত রেকর্ডসমূহ কেন্দ্রিয়ভাবে পরীক্ষা করা
- CAATs এর ব্যবহার , যেখানে উপর্যুক্ত

ধাপ-৬: সিস্টেমটি নির্ধারণ করা এবং রেকর্ড করা;

- সিস্টেম ডকুমেন্টেশন প্রস্তুত বা আপডেট করা
- ওয়াক-থ্রু পরীক্ষা করা

ধাপ-৭: নিয়ন্ত্রণগুলি সনাক্ত করা এবং প্রাথমিক মূল্যায়ন সম্পাদন করা;

ধাপ-৮: নিয়ন্ত্রণ পরীক্ষা পরিকল্পনা এবং সঞ্চালন;

ধাপ-৯: পরীক্ষার ফলাফল মূল্যায়ন (সিস্টেম অপারেশনের মূল্যায়ন) এব সিস্টেমের দুর্বলতা পরীক্ষা , যদি প্রয়োজন হয়;

ধাপ-১০: সিস্টেমের দুর্বলতা পরীক্ষার ফলাফল মূল্যায়ন;

ধাপ-১১: প্রতিবেদনে নিরীক্ষণ সংক্রান্ত কাজের ফলাফলগুলি সংক্ষিপ্ত করে আলোচনার জন্য একটি খসড়া প্রস্তুত করা;

ধাপ-১২: দায়িত্বশীল ব্যবস্থাপকের সাথে অনুসন্ধান এবং সুপারিশ নিয়ে আলোচনা করা এবং পদক্ষেপে সম্মত হওয়া;

ধাপ-১৩: নিরীক্ষা প্রতিবেদন বা পরিচালনা সংক্রান্ত চিঠি চূড়ান্ত করা;

ধাপ-১৪: নিরীক্ষা পত্রের পর্যালোচনা ও মূল্যায়ন;

- মান নিয়ন্ত্রন পর্যালোচনা
- নিরীক্ষা কার্যক্রম সংশোধন
- আইটেম অনুসরণ করা।

৫.৩.৬ কম্পিউটার সহায়ক নিরীক্ষণ কৌশল এবং সরঞ্জাম (CAATs):

Computer Assisted Audit Techniques and tools (CAATs) হলো এমন সকল প্রক্রিয়া যার মাধ্যমে কম্পিউটারের সহায়তায় নিরীক্ষণ পদ্ধতির কার্য সম্পাদন করা হয়। CAATs কোনও সিস্টেমে অভ্যন্তরীণ নিয়ন্ত্রণের ক্রিয়াকলাপ পরীক্ষা করার পাশাপাশি অ্যাকাউন্টসমূহের একটি সেটে নিরীক্ষার মতামতকে সমর্থন করার জন্য লেনদেন পরীক্ষা করা উভয়ই হতে পারে। (CAATs) এর মাধ্যমে কোন নমুনা সাধারনভাবে নিরীক্ষা করতে যে সময় প্রয়োজন তার চেয়ে অনেক কম সময়ে নমুনাটির ১০০% নিরীক্ষা করা যেতে পারে। যা একই সময়ে আর্থিক স্তরের নিরীক্ষা কাজের আর্থিক গুণমান এবং দক্ষতা উভয়ই বাড়িয়ে তোলে।

CAATs ব্যবহারের সুবিধাসমূহ:

- ব্যাপক পরিসরে নিরীক্ষা কার্যক্রম পরিচালনা;
- গ্রহনযোগ্য নিরীক্ষা পদ্ধতি;
- আধুনিক নিরীক্ষা পদ্ধতি;
- কম ব্যয়বহুল নিরীক্ষা পদ্ধতি।

CAATs মূলত দুইভাগে ভাগ করা যায়:

- ডেটা পর্যালোচনার জন্য ব্যবহৃত CAATs;
- প্রোগ্রাম নিয়ন্ত্রণ পর্যালোচনার জন্য ব্যবহৃত CAATs।

৫.৪। তথ্য পদ্ধতি নিয়ন্ত্রণের উদ্দেশ্য:

নিয়ন্ত্রণগুলি সনাক্তকরণের সুবিধার্থে নিরীক্ষককে একটি উত্তম নিয়ন্ত্রণ পরিবেশের উদ্দেশ্য সম্পর্কে অবহিত হতে হবে। এটি করার ক্ষেত্রে তথ্য ও যোগযোগ প্রযুক্তি নিরীক্ষককে সাধারণ নিয়ন্ত্রণের লক্ষ্যগুলি গ্রহণ করতে হবে এবং তাদের নির্দিষ্ট তথ্য সিস্টেম নিরীক্ষা পদ্ধতিতে রূপান্তর করতে হবে। তথ্য পদ্ধতি নিয়ন্ত্রণের উদ্দেশ্যগুলি হলো:-

- তথ্য সুরক্ষা
- অনুমোদিত লেনদেন
- সঠিক সময়ে ইনপুট সম্পূর্ণতা
- প্রতিবেদনের সাদৃশ্য
- প্রতিবেদনের প্রত্যাখ্যান
- পর্যাপ্ত ব্যাক আপ
- সফ্টওয়্যার পরিবর্তন নিয়ন্ত্রণ

৫.৫। তথ্য পদ্ধতির নিয়ন্ত্রনের কাঠামো মূল্যায়ণ:

চিহ্নিত নিয়ন্ত্রণ পদ্ধতি দ্বারা নিয়ন্ত্রণের লক্ষ্যগুলি অর্জন করা হবে কিনা নিরীক্ষককে অবশ্যই তা বিবেচনা করতে হবে। নিয়ন্ত্রণগুলি যুক্তিসঙ্গত পরিস্থিতিতে ত্রুটিগুলি রোধ বা সনাক্ত করবে কিনা তার উপর গুরুত্ব আরোপ করতে হবে। তাহলেই নিরীক্ষকগন সার্বিক পরীক্ষা পরিচালনা করতে সম্মতি প্রদান করবে। তথ্য পদ্ধতি নিরীক্ষককে অবশ্যই নিম্ন লিখিত বিষয়গুলি সম্পর্কে প্রতিবেদন প্রদান করতে হবে।

- সিস্টেমটি নিয়ন্ত্রণের উদ্দেশ্যগুলি পূরণ করতে সক্ষম কিনা, যদি সক্ষম না হয় তাহলে তার কারন;

➢ কোনও চিহ্নিত দুর্বলতার কারনে ত্রুটির উৎপত্তি হয়েছে কিনা;

➢ নির্দিষ্ট উদ্দেশ্য অনুযায়ী নিয়ন্ত্রন পরিচালিত হচ্ছে কিনা;

➢ কোন নির্দিষ্ট ত্রুটি আবিষ্কার করা হয়েছে কিনা এবং আরও অজানা ত্রুটি থাকার সম্ভবনা রয়েছে কিনা।

প্রতিবেদনে যেকোন ত্রুটি মোকাবেলা এবং ভবিষ্যতে উৎপন্ন হতে পারে এমন ত্রুটি এড়িয়ে যাবার জন্য গঠনমূলক এবং কার্যকর প্রস্তাবসমূহ উল্লেখ থাকতে হবে।

৫.৬ বিভিন্ন ধরনের নিয়ন্ত্রণ:

৫.৬ .১ অপারেশনাল নিয়ন্ত্রণ:

➢ **নিরীক্ষার উদ্দেশ্য:** প্রতিনিয়ত চলমান সিস্টেমসমূহে পর্যাপ্ত পরিমান সামঞ্জস্য ও শৃঙ্খলা রয়েছে কিনা তা নিশ্চিত করা

➢ **লক্ষ্য:** ডেটা প্রস্তুতি সম্পর্কিত নিয়ন্ত্রণ এবং প্রক্রিয়াজাতকরণের সময় ডেটা নিয়ন্ত্রণ

➢ **নিয়ন্ত্রণের বিষয়সমূহ :**

ক) প্রাপ্ত এবং রূপান্তরিত ডাটার উপর নিয়ন্ত্রণ;
খ) প্রক্রিয়াকরণের সময় ডেটা নিয়ন্ত্রণ;
গ) আউটপুট বিতরণের উপর নিয়ন্ত্রণ;
ঘ) অপারেটিং সিস্টেম নিয়ন্ত্রণ;
ঙ) ডাটা পুন:প্রাপ্তির উপর নিয়ন্ত্রণ।

৫.৬.২ ফাইল এবং সফটওয়্যার নিয়ন্ত্রণ:

➢ **নিরীক্ষার উদ্দেশ্য:** ডেটা ফাইল এবং সফটওয়্যারকে সব ধরণের ক্ষতি, অননুমোদিত প্রকাশ হতে সুরক্ষা প্রদান করা এবং হারিয়ে যাওয়া তথ্যের পুন:প্রাপ্তি নিশ্চিত করা।

➢ **লক্ষ্য:** সমস্ত ভৌত/বাস্তব ফাইলে প্রবেশ এবং তাদের নিরাপত্তা সংশ্লিষ্ট নিয়ন্ত্রণ।

➢ **নিয়ন্ত্রণের বিষয়সমূহ :**

ক) ভৌত/বাস্তব ফাইলের সুরক্ষা নিয়ন্ত্রণ;
খ) সফটওয়্যারে প্রবেশ নিয়ন্ত্রণ;
গ) ফাইল শনাক্তকরণ, সিস্টেম সফ্টওয়্যার, প্রবেশ মোড এবং ফাইল এনক্রিপশন;
ঘ) প্রোগ্রামের পরিবর্তনের উপর নিয়ন্ত্রণ;
ঙ) ব্যাকআপ।

৫.৬.৩ নেটওয়ার্ক নিয়ন্ত্রণ:

➢ **নিরীক্ষার উদ্দেশ্য:** সমস্ত টার্মিনাল এবং নেটওয়ার্ক কার্যক্রমের যথাযথ অনুমোদন এবং ভুল ও অদক্ষ প্রক্রিয়াকরণ হ্রাস নিশ্চিত করা।

➢ **লক্ষ্য:** কম্পিউটারে সংযুক্ত সমস্ত টার্মিনাল দ্বারা সম্পাদিত প্রক্রিয়াসমূহে প্রবেশ পরিচালনা করা।

➢ **নিয়ন্ত্রণের বিষয়সমূহ :**

ক) পরিচালনাসংক্রান্ত বিষয়সমূহে প্রবেশ নিয়ন্ত্রণ;
খ) প্রবেশের ভৌত সীমাবদ্ধতা;
গ) প্রবেশের সফটওয়্যার সংক্রান্ত সীমাবদ্ধতা;
ঘ) প্রান্তিক কার্যক্রম রেকর্ডিং।

৫.৬.৪ পরিবেশগত নিয়ন্ত্রণ:

➢ **নিরীক্ষার উদ্দেশ্য:** কর্মী, কম্পিউটার সরঞ্জাম ও পরিবেশ, সফটওয়্যার, ডেটা, ইচ্ছাকৃত বা দুর্ঘটনাজনিত ক্ষতির বিরুদ্ধে দলিলায়ন এবং কোনও বড় বিপর্যয়ের ঘটনায় সেবার ধারাবাহিকতা নিশ্চিত করার জন্য পর্যাপ্ত সুরক্ষা নিশ্চিত করা।

➢ **লক্ষ্য:** প্রক্রিয়াজাতকরনের মূল বাধাসমূহ এবং বড় বিপর্যয় হতে পুনরুদ্ধারের পদ্ধতি এবং নিয়ন্ত্রণ।

➢ **নিয়ন্ত্রণের বিষয়সমূহ :**

ক) হুমকি হতে সুরক্ষা;
খ) অপারেশনের ধারাবাহিকতা।

অধ্যায়-৬

প্রমাণ সংগ্রহ, মূল্যায়ন এবং নিরাপদ সংরক্ষণ

নিরীক্ষার আওতাধীন প্রতিষ্ঠান, কর্মসূচি, কর্মকান্ড অথবা কার্যক্রম সম্পর্কে নিরীক্ষণের সিদ্ধান্ত ও মতামতের সমর্থনে উপযুক্ত, প্রাসঙ্গিক ও যুক্তিসংগত প্রমাণ থাকা উচিত। অধিকন্তু, অন্যান্য বিষয়ের মধ্যে আদর্শমান নির্দেশক হল- উপাত্ত সংগ্রহ ও নমুনা বাছাই কৌশল সতর্কভাবে নির্বাচন করা এবং নিরীক্ষা প্রমাণ সংগ্রহে পরিদর্শন, পর্যবেক্ষন, অনুসন্ধান ও নিশ্চিতকরণ এর মত কৌশল ও প্রক্রিয়া সম্পর্কে নিরীক্ষকগণের স্বচ্ছ ধারণা থাকা বাঞ্ছনীয়।

৬.১ নিরীক্ষা প্রমাণকের প্রকারভেদ :

তথ্য ও যোগাযোগ প্রযুক্তি (ICT) নিরীক্ষা কাজের পরিকল্পনাকালে নিরীক্ষককে সংগৃহীতব্য নিরীক্ষা প্রমাণকের ধরন নিরীক্ষার উদ্দেশ্য পূরণে নিরীক্ষা প্রমাণক হিসেবে এর ব্যবহার ও এর নির্ভরযোগ্যতার বিভিন্ন পর্যায়কে বিবেচনায় নিতে হবে। উদাহরণস্বরূপ, নিরীক্ষিতব্য প্রতিষ্ঠানের নিজস্ব নিরীক্ষা প্রমাণের তুলনায় কখনো কখনো স্বাধীন তৃতীয় পক্ষ (Third party) থেকে প্রাপ্ত দৃঢ় সমর্থন সূচক নিরীক্ষা প্রমাণ বেশী নির্ভরযোগ্য হতে পারে। ব্যক্তি বিশেষের সাক্ষ্য অপেক্ষা প্রত্যক্ষ দালিলিক প্রমাণ বেশী নির্ভরযোগ্য।

নিরীক্ষকগণ যে ধরনের দালিলিক প্রমাণক ব্যবহারের বিষয় বিবেচনা করতে পারে তার মধ্যে অন্যতম হলঃ

- অনুসৃত প্রক্রিয়া ও ভৌত বস্তুসমূহের অস্তিত্ব (Observed process and existence of physical items)
- দালিলিক নিরীক্ষা প্রমাণ, ইলেক্ট্রনিক রেকর্ডসহ (Documentary audit evidence including electronic records)
- বিশ্লেষণ , CAATs ব্যবহার করে (Analysis using CAATs)

পর্যবেক্ষণের মাধ্যমে ভৌত (physical) প্রমাণ পাওয়া যায় । বিশেষতঃ কোনো নিরীক্ষা ফলাফলের জন্য গুরুত্বপূর্ণ হলে তার সমর্থনে ভৌত প্রমাণক থাকা বাঞ্ছনীয়। ভৌত প্রমাণকের অন্যতম সমর্থনযোগ্যতা হল- কর্তৃপক্ষের কাছে এ ধরনের প্রমাণকের গ্রহণযোগ্যতা।

চাক্ষুষ যাচাই বাছাই হল নিরীক্ষক কর্তৃক পরিমেয় সম্পদ পরিদর্শন করা অথবা হিসাব করা। নিরীক্ষক কম্পিউটার টার্মিনাল এবং প্রিন্টার ইত্যাদির উপস্থিতি ভৌত পরিদর্শন করতে পারেন। পানি ও ধোয়া সনাক্তকারী যন্ত্র, অগ্নি নির্বাপক যন্ত্র ইত্যাদির উপস্থিতি প্রত্যক্ষভাবে যাচাই বাছাইয়ের জন্য কম্পিউটার কেন্দ্র পরিদর্শন করা অপরিহার্য । যন্ত্রের অবস্থান পরিস্কারভাবে চিহ্নিত ও দৃশ্যমান করা অপরিহার্য । প্রতিষ্ঠানে অননুমোদিত প্রবেশ রোধকল্পে ভৌত পরিবেশ নিয়ন্ত্রণ ব্যবস্থা থাকা দরকার। তথ্য ও যোগাযোগ প্রযুক্তিতে সিস্টেমের ভৌত পরিবেশকে যথেষ্ট গুরুত্ব দেয়া হয়। তাই এ পরিবেশ গ্রহণযোগ্য নীতিমালার সাথে সামঞ্জস্যপূর্ণ হওয়ার বিষয়টিও নিরীক্ষায় নিশ্চিত করতে হয় ।

নিরীক্ষা প্রমাণ সংগ্রহের জন্য নিম্নের পদ্ধতিসমূহ ব্যবহার করা হয়:

৬.১.১ সাক্ষাৎকার:

প্রমাণ সংগ্রহের সময় নিরীক্ষকগণ গুণগত ও পরিমাণগত উভয় তথ্য প্রাপ্তির জন্য সাক্ষাৎকার গ্রহণ করতে পারেন। নিরীক্ষকের ব্যবহৃত সাক্ষাৎকারের মধ্যে উল্লেখযোগ্য হলঃ

- সিস্টেমে নিহিত কার্যাবলী ও নিয়ন্ত্রণ সম্পর্কে স্বচ্ছ ধারণা পেতে সিস্টেম এনালিস্ট এবং প্রোগ্রামারদের সাক্ষাৎকার নেয়া যেতে পারে;
- এপ্লিকেশন সিস্টেম কর্তৃক চিহ্নিত ভুল বা অসম্পূর্ণ উপাত্ত কিভাবে সংশোধন করা হয় তা জানতে করণিক/ডাটা এন্ট্রি কর্মীদের সাক্ষাৎকার নেয়া যেতে পারে;
- সিস্টেমের ব্যবহারকারীদের কর্মজীবনের গুণগতমানকে সিস্টেম কিভাবে প্রভাবিত করছে সে বিষয়ে তাদের ধারণা জানতে এপ্লিকেশন ব্যবহারকারীদের সাক্ষাৎকার নেয়া যেতে পারে;
- কোনো এপ্লিকেশন সিস্টেম পরিচালনায় মাত্রাতিরিক্ত সংস্থান (রিসোর্স) ব্যবহৃত হচ্ছে কিনা তা জানতে পরিচালনার কাজে নিয়োজিত কর্মীদের সাক্ষাৎকার নেয়া যেতে পারে, ইত্যাদি।

সফল সাক্ষাৎকার পরিচালনার ক্ষেত্রে সতর্কতামূলক প্রস্তুতির জন্য প্রয়োজনীয় বিষয়াদিঃ

- প্রয়োজনীয় তথ্য অন্যত্র সহজলভ্য না হলে বিকল্প উৎস হতেও প্রয়োজনীয় তথ্য পাওয়া যেতে পারে;
- প্রতিষ্ঠানের যে সকল ব্যক্তি সাক্ষাৎকারের সময় সবচেয়ে ভাল তথ্য দিতে পারবে তাদের চিহ্নিতকরণ। অর্গানাইজেশন চার্ট প্রায়শই সঠিক উত্তরদাতাদের তথ্যের প্রথম উৎস হয়ে থাকে;
- সাক্ষাৎকারের উদ্দেশ্য সঠিকভাবে চিহ্নিতকরণ এবং সাক্ষাৎকারে যেসকল তথ্য চাওয়া হবে তার একটি তালিকা প্রণয়ন;

- সাক্ষাৎকারের শুরুতে এবং শেষে সাধারণ তথ্যের জন্য এবং সাক্ষাৎকারের মাঝামাঝি পর্যায়ে সুনির্দিষ্ট তথ্যের জন্য অনুরোধ করতে হবে। সাক্ষাৎকারের শুরুতে বিতর্কিত কিংবা স্পর্শকাতর তথ্যের জন্য অনুরোধ করা উচিত নয়;
- উত্তরদাতাদের সাথে সাক্ষাৎকারের সময় এবং স্থান নির্ধারণের জন্য যোগাযোগ করা যেতে পারে।

সাক্ষাৎকার শেষ হওয়ার পর নিরীক্ষকগণের উচিত যত দ্রুত সম্ভব প্রতিবেদন প্রস্তুত করা। সাক্ষাৎকার প্রতিবেদন প্রস্তুতের সময় নিরীক্ষকগণের দু'টি প্রধান উদ্দেশ্য হলো:-

- প্রথমত, মতামতসমূহ হতে প্রকৃত ঘটনা আলাদা করার চেষ্টা করা;
- দ্বিতীয়ত, সাক্ষাৎকারের মাধ্যমে প্রাপ্ত তথ্যসমূহ একত্রিত করা এবং সেগুলো তাদের সামগ্রিক নিরীক্ষার উদ্দেশ্য পরিপালনের ক্ষেত্রে কতটুকু অর্থবহ তা নির্ধারণ করা।

৬.১.২ প্রশ্নপত্র:

সাধারনত পদ্ধতির অন্তর্গত নিয়ন্ত্রণগুলো মূল্যায়নের জন্য প্রশ্নপত্র ব্যবহার করা হয়। নিরীক্ষকগণও প্রমাণক সংগ্রহের সময় পদ্ধতির দুর্বলতার ক্ষেত্রসমূহ নির্ধারণ করার জন্য প্রশ্নপত্র ব্যবহার করতে পারেন। উদাহরণস্বরূপ, নিরীক্ষকগণ পদ্ধতির কার্যকারিতার একটি নির্দেশক হিসেবে পদ্ধতি সম্পর্কে ব্যবহারকারীদের সামগ্রিক অনুভূতি মূল্যায়নের জন্য প্রশ্নপত্র ব্যবহার করতে পারেন। একইভাবে একটি তথ্য পদ্ধতির মধ্যে বিরাজমান সম্ভাব্য অকার্যকারিতাসমূহের ক্ষেত্র চিহ্নিত করতে প্রশ্নপত্র ব্যবহার করা যেতে পারে। প্রশ্নসমূহের বানান যথাযথ এবং স্পষ্ট হতে হবে, পরিভাষাসমূহ সংজ্ঞায়িত হতে হবে এবং প্রশ্নসমূহ পূরণের নির্দেশাবলী স্পষ্ট হতে হবে। প্রশ্নাবলী তৈরিতে নিম্নোক্ত সাধারণ নির্দেশাবলী বিবেচনায় রাখতে হবেঃ

- প্রশ্ন যেন সুনির্দিষ্ট হয় তা নিশ্চিত করা;
- প্রশ্নকারীর বোধগম্য যথাযথ ভাষা ব্যবহার করতে হবে। উদাহরণস্বরূপ, সিস্টেম এডমিনিস্ট্রেটর অথবা ডাটাবেজ এডমিনিস্ট্রেটরকে বোঝানোর জন্য প্রশ্ন সুনির্দিষ্ট হওয়া প্রয়োজন এবং প্রশ্নসমূহে তথ্য প্রযুক্তি পরিভাষা সংক্রান্ত শব্দসমূহ ব্যবহৃত হতে পারে কিন্তু যথাযথভাবে প্রশ্নসমূহ বোঝানোর জন্য এসকল শব্দসমূহের ব্যবহার অনিবার্য হতে পারে;
- একেবারে অত্যাবশ্যকীয় না হলে নিম্নোক্ত বিষয়গুলো পরিহার করা :-
    - পরিচালনা সংক্রান্ত প্রশ্নাবলী;
    - আচরণ সংক্রান্ত প্রশ্নাবলী;
    - অনুমান নির্ভর প্রশ্নাবলী;
    - ব্রিবতকর প্রশ্নাবলী।

৬.১.৩ ফ্লোচার্ট:

নিয়ন্ত্রণ ফ্লোচার্টসমূহ পদ্ধতির মধ্যে বিদ্যমান নিয়ন্ত্রণসমূহ এবং সেগুলোর অবস্থান প্রদর্শন করে থাকে। এর তিনটি প্রধান নিরীক্ষা উদ্দেশ্য আছেঃ

- **বোধগম্যতা:** একটি কন্ট্রোল ফ্লোচার্ট নিরীক্ষকগণ কর্তৃক অবোধগম্য পদ্ধতি বা পদ্ধতির অন্তর্গত নিয়ন্ত্রণ ক্ষেত্রসমূহকে দৃষ্টিগোচর বা বোধগম্য করে;
- **মূল্যায়ন:** অভিজ্ঞ নিরীক্ষকগণ পদ্ধতির অন্তর্গত নিয়ন্ত্রণসমূহের শক্তিমত্তা/প্রবলতা অথবা দুর্বলতা প্রকাশের ধরন চিহ্নিত করার জন্য কন্ট্রোল ফ্লোচার্ট ব্যবহার করে থাকে;
- **যোগাযোগ:** নিরীক্ষকগণ একটি পদ্ধতি এবং এর সংশ্লিষ্ট নিয়ন্ত্রণসমূহ অন্য পদ্ধতি এবং নিয়ন্ত্রণসমূহের সাথে কিভাবে যোগসূত্র স্থাপন করে তা বোঝার জন্য কন্ট্রোল ফ্লোচার্ট ব্যবহার করে থাকে;

কন্ট্রোল ফ্লোচার্ট তৈরিতে চারটি ধাপ জড়িতঃ

- একটি পদ্ধতির নির্দিষ্ট বৈশিষ্ট্যসমূহ দৃষ্টিগোচর করা এবং ভালভাবে বোঝার জন্য প্রাথমিক ফ্লোচার্ট কৌশল নির্বাচন করা যেতে পারে;
- কাজের যথাযথ স্তর পূর্ণাঙ্গভাবে নির্বাচন করা যাতে নিরীক্ষকগণ বিষয়বস্তুতেই আবিষ্ট/মগ্ন হয়ে অন্তত গুরুত্বপূর্ণ নিয়ন্ত্রণসমূহের শক্তিমত্তা অথবা দুর্বলতা এড়িয়ে না যান;
- প্রাথমিক ফ্লোচার্ট এমনভাবে তৈরি করতে হবে যাতে পদ্ধতির বৈশিষ্ট্যসমূহ সহজবোধ্য হয়;
- প্রাথমিক ফ্লোচার্টের ভিত্তিতে কন্ট্রোল ফ্লোচার্ট এমনভাবে তৈরি করতে হবে যাতে নিয়ন্ত্রণসমূহের শক্তিমত্তা এবং দুর্বলতা প্রকাশ পায়।

৬.১.৪ বিশ্লেষণাত্মক প্রক্রিয়া:

বিভিন্ন তুলনা এবং সম্পর্ক ব্যবহারপূর্বক বিশ্লেষণাত্মক প্রক্রিয়া একটি হিসাবের জের যুক্তিসংগতভাবে প্রদর্শিত হচ্ছে কিনা তা নির্ধারণ করে। একটি উদাহরণ হল-পূর্ববর্তী বছরের সাথে চলতি বছরের গ্রস মার্জিনে শতকরা হারের তুলনা। কোন হিসাবগুলো অধিকতর যাচাই এর প্রয়োজন নেই, কোন প্রমাণক হ্রাস করা যেতে পারে এবং কোন বিষয়সমূহের উপর পুঙ্খানুপুঙ্খ তদন্তের প্রয়োজন তা বিশ্লেষণাত্মক প্রক্রিয়ায় নির্ধারন করা উচিত। CAAT এর সাহায্যে বিশ্লেষণাত্বক পর্যালোচনার জন্য পরিসংখ্যান তৈরি করা যেতে পারে। বিশেষত, CAAT যে সকল বিশ্লেষণ তৈরি করতে পারে তা অন্যভাবে পাওয়া সহজসাধ্য নয়।

৬.২ প্রমাণক সংগ্রহের সরঞ্জামসমূহ :

সিস্টেম সার্টিফিকেশনের প্রয়োজনীয়তা বৃদ্ধির সাথে সাথে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণ ব্যবহার করতে পারেন এমন উপকরণও সহজ লভ্য হয়েছে।

৬.২.১ সার্বজনীন নিরীক্ষা সফটওয়্যার :

এটি একটি অফ-দ্য-সেলফ সফটওয়্যার যা কম্পিউটার তথ্য ভান্ডারে প্রবেশ এবং উপাত্ত ব্যবহারের সুযোগ তৈরী করে দেয়। IDEA একটি বহুল ব্যবহৃত সার্বজনীন নিরীক্ষা সফটওয়্যারের উদাহরণ । বিশেষতঃ বিভিন্ন ধরনের হার্ডওয়্যার ও সফটওয়্যার প্লাটফর্ম উপযোগী করে সার্বজনীন নিরীক্ষা সফটওয়্যার উন্নয়ন করা হয়েছে। এগুলো বিভিন্ন ধরনের কাজ করে, যেমন-ফাইল দেখা, ফাইল পুনর্গঠন, তথ্য নির্বাচন ও আহরণ, নানা ধরনের উপাত্ত বিশ্লেষণ এবং প্রতিবেদন কার্যাবলী। এগুলো ব্যবহার করে (ক) তথ্যের অস্তিত্ব পরীক্ষণ, সঠিকতা, সম্পূর্ণতা, ধারাবাহিকতা এবং যথাকালীনতা যাচাই; (খ) এপ্লিকেশন সিস্টেমের অন্তর্গত প্রক্রিয়াসমূহের গুণগত মান যাচাই; (গ) প্রবণতা বিশ্লেষণ (Trend Analysis) এর মতন মূল নিরীক্ষা সূচকের বিশ্লেষণাত্বক পুনঃমূল্যায়ন নিরীক্ষণ করা হয়। তবে সার্বজনীন নিরীক্ষা সফটওয়্যার ব্যবহারের কিছু সীমাবদ্ধতা রয়েছে, যেমন-প্রসেসিং লজিক যাচাইয়ের সীমিত সামর্থ এবং ভুলের প্রবণতা নির্ধারণের সীমিত দক্ষতা ।

৬.২.২ শিল্প ভিত্তিক নিরীক্ষা সফটওয়্যার:

একটি নির্দিষ্ট সংস্থার প্রয়োজনীয় সাধারণ নিরীক্ষা কার্যাবলী সম্পাদনের জন্য শিল্প ভিত্তিক সফটওয়্যার ডিজাইন করা হয় যার দ্বারা উচ্চ পর্যায়ের নির্দেশনা প্রদান করা যায়। আরও নির্দিষ্ট করে বললে বলা যায় এটা একটি শিল্প ভিত্তিক যুক্তি প্রদান করে। উদাহরণস্বরপ আর্থিক বিশ্লেষণ বা অনুপাত যা আর্থিক প্রতিষ্ঠানকে সক্রিয় করে।

৬.২.৩ ইউটিলিটি সফটওয়্যার:

এই সফটওয়্যার পুন: পুন: ব্যবহৃত কার্যাদি যেমন কপি, বাছাই/সাজান, ডিস্ক অনুসন্ধান, ডিস্ক ফরমেট ইত্যাদি সম্পাদন করে। এগুলো প্রায়শই প্রধান সিস্টেম সফটওয়্যারের সাথে সরবরাহকৃত গুচ্ছ এপ্লিকেশন হিসেবে পাওয়া যায় । ইউটিলিটি সফট্ওয়্যার বিনামূল্যে বা শোয়ারওয়্যার হিসাবে অথবা কিনতে পাওয়া যায় এবং নিরীক্ষকগণ কর্তৃক এককভাবে অথবা নতুন নিরীক্ষা সফটওয়্যার উন্নয়নের জন্য এগুলো ব্যবহার করা যেতে পারে । তবে বলাবাহুল্য, ইউটিলিটি সফটওয়্যার ব্যবহারের ক্ষেত্রে এগুলো ব্যবহারের যথাযথ অনুমোদন ও লাইসেন্স গ্রহণ করা হয়েছে কিনা সে বিষয়ে সতর্কতা অবলম্বন করতে হবে ।

৬.২.৪ এক্সপার্ট সিস্টেম :

এক্সপার্ট সিস্টেম হচ্ছে এমন প্রোগ্রাম যার মধ্যে একটি বিশেষ ডোমেইন সম্পর্কে আহরিত দক্ষতার জ্ঞান অন্তর্ভুক্ত করা হয় এবং নির্দিষ্ট সমস্যা মোকাবেলায় এই জ্ঞান ব্যবহৃত হয়। এটি একটি জ্ঞান ভিত্তিক সফটওয়্যার যার দ্বারা নিরীক্ষিতব্য তথ্যের মূল্যায়ন করার জন্য অপরিহার্য নিরীক্ষার আওতা এবং প্যারামিটারসমূহের প্রকৃত অবস্থা অন্তর্ভূক্ত থাকে। উদাহরণস্বরূপ, ডাটাবেইজে অন্তর্ভূক্ত বিভিন্ন আদর্শমানসমূহ যা নিরীক্ষিত তথ্য তুলনা করার জন্য ব্যবহৃত হয়।

৬.২.৫ বিশেষায়িত নিরীক্ষা সফটওয়্যার:

একটি নির্দিষ্ট ধরনের নিরীক্ষা সম্পাদনের জন্য এই সফটওয়্যার উন্নয়ন করা হয়। সবচেয়ে ভালভাবে উন্নয়নকৃত একটি পদ্ধতিতে নিরীক্ষা মডিউলসমূহ সংযুক্ত থাকে যেখানে আবশ্যিকভাবে প্রাত্যহিক ক্রিয়াকলাপের সূচিসমূহ অন্তর্ভূক্ত থাকে যা নিয়মিত সতর্কতা এবং তথ্য প্রদানের মাধ্যমে পদ্ধতিতে ব্যবহৃত নিয়ন্ত্রণগুলোর অব্যাহত নির্ভরতা নিশ্চিত করে। নিরীক্ষা মডিউলের পর্যাপ্ততা, মডিউল হতে প্রাপ্ত তথ্যের পাশাপাশি নিরীক্ষা ফলাফলের উপর কর্তপক্ষের ফলোআপও নিরীক্ষা নিরাপত্তার জন্য অপরিহার্য। সহজ কথায় যখন নিরীক্ষা মডিউল কার্যকর না থাকে অথবা নিস্ক্রিয় করা থাকে অথবা বিভিন্ন সময়ে পর্যায়ক্রমে পর্যালোচনা করা না হয় তখন পদ্ধতি লঙ্ঘনের উচ্চ ঝুঁকি থাকে।

৬.২.৬ সংঘটনশীল নিরীক্ষা (Concurrent Auditing) উপকরণ:

ম্যানুয়াল নিরীক্ষা ব্যবস্থায় নিরীক্ষকগণ সচরাচর কোনো কাজ সংঘটিত হওয়ামাত্র সংঘটনশীল বা তাৎক্ষণিক নিরীক্ষা (Concurrent Auditing) পরিচালনা করেন না। তবে কম্পিউটারাইজেশনের ক্রমবৃদ্ধির ফলে যখন কোনো এপ্লিকেশন পদ্ধতিতে উপাত্ত প্রক্রিয়াকরণ করা হয় তখন নিরীক্ষা প্রমাণ সংগ্রহের জন্য সংঘটনশীল নিরীক্ষা কৌশলের উপর নির্ভরতা

অবশ্যিকভাবে বৃদ্ধি পায়। নিরীক্ষা প্রমাণকসমূহ সংগ্রহ, প্রক্রিয়াকরণ এবং মূদ্রণের লক্ষ্যে বিশেষ নিরীক্ষা মডিউল আকারে এপ্লিকেশন সিস্টেমে সংঘটনশীল বা তাৎক্ষণিক নিরীক্ষা উপকরণ সংযুক্ত থাকতে পারে। অধিকাংশ সিস্টেম সফটওয়্যারে নিরীক্ষা মডিউল সংযুক্ত থাকে যা ব্যবস্থাপনা কর্তৃপক্ষকে কার্যকরভাবে তদারকিতে সহায়তা করে। বিভিন্ন ধরনের সংঘটনশীল নিরীক্ষা কৌশলের অধিকাংশই তিনটি শ্রেণীর মধ্যে পড়ে:-

(ক) উৎপাদন প্রক্রিয়াকরণের জন্য ব্যবহৃত এপ্লিকেশন সিস্টেম মূল্যায়নের জন্য পরীক্ষামূলক উপাত্তসহ যে নিরীক্ষা কৌশল ব্যবহৃত হয়;

(খ) নিরীক্ষা পর্যালোচনার জন্য উৎপাদন প্রক্রিয়াকরণে সংশ্লিষ্ট লেনদেনসমূহে যে নিরীক্ষা কৌশল ব্যবহৃত হয়;

(গ) উৎপাদন প্রক্রিয়াকরণের সময় এপ্লিকেশন সিস্টেমের পরিবর্তনশীল অবস্থা চিহ্নিত অথবা চিত্রিত করার জন্য যে নিরীক্ষা কৌশল ব্যবহৃত হয়। এসব কৌশলের কয়েকটি হলঃ

- সমন্বিত পরীক্ষণ সুবিধা (Integrated Test Facility , ITF);
- সিস্টেম নিয়ন্ত্রিত নিরীক্ষা পর্যালোচনা ফাইল এবং নিহিত নিরীক্ষা মডিউলসমূহ (SCARF/EAM);
- স্ন্যাপশটস;
- নিরীক্ষা হুকস;
- অব্যাহত ও সবিরাম সহসংঘটন (Continuous and Intermittent Simulation ,CIS)।

নিরীক্ষকগণ সাধারণত দুই ধরনের পরীক্ষা পদ্ধতি ব্যবহার করেন :-

- প্রতিপালন পরীক্ষা (Compliance tests)
- বাস্তব/স্বতন্ত্র পরীক্ষা (Substantive test)।

৬.২.৭ প্রতিপালন পরীক্ষা (Compliance tests) :

প্রতিষ্ঠানের বিধি-বিধান মেনে লেন-দেনের কাজ সম্পাদন করা হয় কিনা তা প্রতিপালন পরীক্ষার (Compliance tests) মাধ্যমে যাচাই করা হয় এবং এ পরীক্ষা অভ্যন্তরীণ নিয়ন্ত্রণের উপস্থিতি/অনুপস্থিতি সম্পর্কে নিরীক্ষককে প্রমাণ সরবরাহ করে। একটি সুনির্দিষ্ট প্রক্রিয়ার অস্তিত্ব ও কার্যকারিতা যাচাই করতে এ পরীক্ষা ব্যবহার করা যেতে পারে, দালিলিক চিহ্ন অথবা স্বয়ংক্রিয় প্রমাণকসমূহ এর অন্তর্ভুক্ত হতে পারে। আইসিটি পরিবেশ সংশ্লিষ্ট প্রতিপালন পরীক্ষার (Compliance tests) কিছু উদাহরণ হলঃ

- সময় সময় পাসওয়ার্ডসমূহ পরিবর্তন করা হয় কিনা তা নিশ্চিতকরণ/নির্ধারণ;
- সিস্টেম লগ পর্যালোচনা করা হয় কিনা তা নিশ্চিতকরণ;
- অনুমোদিতভাবে প্রোগ্রাম পরিবর্তন করা হয় কিনা তা নিশ্চিতকরণ;
- পরামর্শ মত নিয়ন্ত্রণ ব্যবস্থা কাজ করছে কিনা তা নিশ্চিতকরণ;
- দুর্যোগ পরবর্তী উদ্ধার পরিকল্পনা পরীক্ষা করা হয়েছে কিনা তা নিশ্চিতকরণ।

৬.২.৮ বাস্তব/স্বতন্ত্র পরীক্ষা (Substantive test):

বাস্তব/স্বতন্ত্র পরীক্ষা (Substantive test) লেন-দেন এবং স্থিতির বৈধতা ও স্বত্ত্ব বিষয়ে নিরীক্ষককে প্রমাণ সরবরাহ করে। উদাহরণস্বরূপ-আর্থিক বিবরণের স্থিতির উপর সরাসরি প্রভাব ফেলে এমন অর্থ সংক্রান্ত ভুল যাচাই করার জন্য নিরীক্ষকগণ বাস্তব পরীক্ষা করেন। আইসিটি পরিবেশ সংশ্লিষ্ট বাস্তব পরীক্ষার আরও কিছু উদাহরণ হলঃ

- পদ্ধতি প্রাপ্যতা বিশ্লেষণ পরিচালনা;
- পদ্ধতি সংরক্ষণ মাধ্যম বিশ্লেষণকরণ;
- পদ্ধতি বিভ্রাট বিশ্লেষণ পরিচালনা;
- খাতায় লিখিত দ্রব্যাদির প্রকৃত সংখ্যার সাথে কম্পিউটারে রক্ষিত সংখ্যার মুখোমুখি (vis-a-vis) তুলনাকরণ;
- হিসাব স্থিতি পুনর্মিলকরণ।

কোন পর্যায় পর্যন্ত বাস্তব পরীক্ষা (Substantive test) করা যাবে প্রতিপালন পরীক্ষা (Compliance test) তা নির্ধারণ করে। প্রতিপালন পরীক্ষায় উদ্ভুত শক্তিশালী নিয়ন্ত্রণসমূহ বাস্তব পরীক্ষাকে (Substantive test) সীমিত করতে পারে এবং বিপরীতভাবে এটি ঘটতে পারে ।

৬.৩ নমুনা বাছাই:

একটি নিরীক্ষা মতামত প্রদানের জন্য যথেষ্ট হয় এমন ন্যূনতম নিরীক্ষা প্রমাণ প্রাপ্তির উপর নিরীক্ষা নৈপুণ্য নির্ভর করে। নিরীক্ষা কার্যে নমুনা বাছাই এর ব্যবহার নিরীক্ষককে অগণিত সুবিধা প্রদান করে। এসব-সুবিধার মধ্যে রয়েছেঃ

- এটি এমন একটি কাঠামো প্রদান করে যার মধ্যে পর্যাপ্ত নিরীক্ষা প্রমাণ পাওয়া যায়;
- কিভাবে নিরীক্ষার উদ্দেশ্য অর্জিত হবে তা নির্ধারণে নিরীক্ষা চিন্তায় স্পষ্টতা বেগবান করে;
- অতি-নিরীক্ষার (over-auditing) ঝুঁকি কমায়;
- কার্যপত্রের মূল্যায়নের সুযোগ আরো ত্বরান্বিত করে;
- নিরপেক্ষ বিবেচিত হওয়ায় নিরীক্ষক কর্তৃক প্রদত্ত নিরীক্ষা ফলাফলের গ্রহণযোগ্যতা বৃদ্ধি করে।

নিরীক্ষা নমুনা বাছাই হল একটি পপুলেশন থেকে ঐ পপুলেশনের কিছু বৈশিষ্ট্যের প্রমাণ সংগ্রহ ও যাচাই করে ঐ জনগোষ্ঠী সম্পর্কে সিদ্ধান্তে পৌছাতে বাছাইকৃত নমুনার পরীক্ষা।

পুরো পপুলেশনের বিষয়ে সিদ্ধান্ত নেয়ার ক্ষেত্রে নির্বাচিত নমুনা প্রতিনিধিত্বমূলক হওয়া গুরুত্বপূর্ণ। উদাহরণস্বরপ শুধু অতি গুরুত্বপূর্ণ উপাদানের মত একটি নির্দিষ্ট বৈশিষ্ট্যের কিছু উপাদানের উপর পরীক্ষান্তে ফলাফল নির্ধারণ করলে পুরো জনগোষ্ঠীর বিষয়ে তা অসম্পূর্ণ ফলাফল দেবে।

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষকগণ সাধারণত দু'ধরনের নমুনা বাছাই প্রক্রিয়া ব্যবহার করেন; এগুলো হলোঃ

- গুণবাচক নমুনা বাছাই (Attribute sampling) ও
- পরিবর্তনশীল নমুনা বাছাই (Variable sampling)।

প্রতিপালন পরীক্ষার ক্ষেত্রে সাধারণত গুণবাচক নমুনা বাছাই করা হয় এবং এ গুণের উপস্থিতি বা অনুপস্থিতি নিয়ে কাজ করা হয় এবং ঘটনা সংঘটিত হওয়ার হারের মাধ্যমে এ ক্ষেত্রে মতামত বা সিদ্ধান্ত গ্রহণ করা হয়। বাস্তব পরীক্ষার (Substantive testing) ক্ষেত্রে সাধারণত চলক বা পরিবর্তনশীল নমুনা বাছাই পদ্ধতি ব্যবহার করা হয় ও জনগোষ্ঠীর পরিবর্তিত বৈশিষ্ট্যসমূহ নিয়ে কাজ করে এবং প্রচলিত সাধারণ মান (Norm) থেকে বিচ্যুতি বিষয়ে মতামত প্রদান করে।

বিভিন্ন নিরীক্ষা পরিস্থিতিতে পরিসংখ্যানগত নমুনা বাছাই পদ্ধতিও ব্যবহার করা যায়। বিভিন্নভাবে পরিসংখ্যানগত নমুনা বাছাই করা যেতে পারে। সচরাচর ব্যবহৃত পদ্ধতি হল যথেচ্ছভাবে নমুনা বাছাই (Random Selection) যেখানে জনগোষ্ঠীর প্রতিটি উপাদানের নির্বাচিত হওয়ার সমান সুযোগ রয়েছে। অভ্যন্তরীণ নিয়ন্ত্রণ পরীক্ষার জন্য এটি ব্যবহার করা হয়। উদাহরণস্বরূপ, নিরীক্ষক সিদ্ধান্ত নিতে পারেন যে একটি নিয়ন্ত্রণ ব্যবস্থা অকার্যকর যদি উক্ত নিয়ন্ত্রণ ব্যবস্থায় ভুলের পরিমান কোন একটি নির্দিষ্ট সীমর উপরে থাকে। কম্পিউটারের মাধ্যমে যথেচ্ছভাবে সংখ্যা ব্যবহার করে নমুনা বাছাই করা যেতে পারে। নমুনা নির্বাচনের জন্য IDEA এর মত নিরীক্ষা সফটওয়্যার ব্যবহার করা যেতে পারে।

নমুনা বাছাই করা হয়ে গেলে নমুনার উপর নির্ধারিত নিরীক্ষামূলক পরীক্ষা চালানো যেতে পারে।

৬.৪ সমাপনী বৈঠক:

নিরীক্ষা তদন্ত শেষে সংশোধনমূলক পদক্ষেপ নেয়ার জন্য আনুষ্ঠানিক বৈঠকের মাধ্যমে নিরীক্ষা ফলাফল এবং পরামর্শসমূহ উর্ধ্বতন ব্যবস্থাপনা কর্তৃপক্ষের কাছে উপস্থাপন করা যেতে পারে। এটি ভাল বোঝাপড়া নিশ্চিত করবে ও নিরীক্ষা সুপারিশের গ্রহণযোগ্যতা বৃদ্ধি করবে। এটি উত্থাপিত বিষয়ে নিরীক্ষিত কর্তৃপক্ষের মতামত প্রদানেরও সুযোগ সৃষ্টি করবে। নিরীক্ষায় প্রাপ্ত সমস্যসমূহের বিষয়ে একমত হলে এ ধরনের বৈঠকের পর রিপোর্ট প্রণয়ন নিরীক্ষার কার্যকারিতা অনেক বৃদ্ধি করে। সমাপনী বৈঠক বাস্তবভিত্তিক ও বাস্তবায়নযোগ্য সুপারিশ চূড়ান্তকরণে সহায়তা করে।

অধ্যায়-৭

আইসিবিতে তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা

৭.১। নিরীক্ষার প্রকারভেদ:

আইসিবি নিম্নলিখিত তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা কার্যক্রম পরিচালনা করে থাকেঃ

নিয়মিত নিরীক্ষাঃ দৈনিক কার্যক্রম নিরীক্ষা করা। পূর্ববর্তী তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা থেকে বর্তমান তারিখ পর্যন্ত তথ্য ও যোগাযোগ প্রযুক্তি সংশ্লিষ্ট ঝুঁকি ভিত্তিক নিরীক্ষা ও পর্যবেক্ষণ পরিচালনা করা।

আইটেম নিরীক্ষাঃ শাখা/প্রধান কার্যালয়ের বিভিন্ন ডিপার্টমেন্টে একটি নির্দিষ্ট আইটেম পুঙ্খানুপুঙ্খভাবে নিরীক্ষা ও এর গুরুত্ব বিবেচনা করা ।

সিস্টেম নিরীক্ষাঃ আইসিবিতে ব্যবহৃত বিভিন্ন হার্ডওয়্যার সামগ্রী ও পরিচালিত বিভিন্ন সফটওয়্যারের এর পরিচালন ত্রুটি এবং নিরাপত্তা বিষয় নিরীক্ষা করা।

বিশেষ নিরীক্ষাঃ পূর্ববর্তী তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষায় উত্থাপিত উচ্চ ঝুঁকি সম্পন্ন আপত্তির পুনরাবৃত্তি ঘটেছে কিনা তা নিরীক্ষা করা। এছাড়া, শাখার অভ্যন্তরীণ নিয়ন্ত্রণ ও সুপারিশ পরিপালনের অবস্থাও পর্যবেক্ষণ করা।

আকস্মিক নিরীক্ষাঃ শাখার তথ্য প্রযুক্তি সংক্রান্ত সামগ্রিক কার্যক্রম পরিদর্শন ও পূর্ববর্তী নিরীক্ষায় উত্থাপিত আপত্তিসমূহ পরিপালনে পরামর্শ/নির্দেশনা প্রদান করতে আইটি এবং অডিট ডিপার্টমেন্টের প্রধান/নির্বাহী কর্তৃক পরিচালিত সংক্ষিপ্ত নিরীক্ষা কার্যক্রম।

তদারকি: শাখার গুরুত্ব বিবেচনা করে নিরীক্ষা কার্যক্রম চলাকালে আইটি এবং ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান কর্তৃক নিরীক্ষা দলের কার্যক্রম তদারকি।

৭.২.১ নিয়মিত নিরীক্ষা প্রক্রিয়াঃ

ধাপ-১: নিয়মিত অভ্যন্তরীণ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা সম্পূর্ণ করতে আইসিবি প্রধান কার্যালয় কর্তৃক একজন কর্মকর্তা/এসপিও/নির্বাহীকে দলনেতা করে কমপক্ষে দুইজন নিরীক্ষকের সমন্বয়ে একটি নিরীক্ষা দল গঠন এবং এই উদ্দেশ্যে নিরীক্ষা দলকে অফিস নির্দেশ প্রদান করা।

ধাপ-২: অফিস নির্দেশ পাওয়ার পর দলনেতা তার দল, প্রয়োজনীয় ডকুমেন্টস ও উপকরণসহ নিরীক্ষাধিন স্থানে গমন করবেন। নিরীক্ষা দল চেকলিস্ট অনুসারে নিরীক্ষা/যাচাই করবেন। চেকলিস্টের পাশাপাশি নিরীক্ষকের নিজস্ব মতামতও থাকতে পারে।

ধাপ-৩: চেকলিস্টের পয়েন্টসমূহ যাচাই করার পর একটি নিরীক্ষা প্রতিবেদন প্রস্তুত করতে হবে যাতে নিরীক্ষা আপত্তি, ঝুঁকি এবং তার প্রভাব ও প্রয়োজনীয় করনীয়সমূহ উল্লেখ থাকবে । প্রতিবেদন প্রস্তুতের পর নিরীক্ষা দলের সদস্য ও দলনেতা স্বাক্ষর করবেন এবংডিপার্টমেন্টের প্রধানের কাছে স্বাক্ষরের জন্য উপস্থাপন করবেন। স্বাক্ষর করার পর এক কপি সংশ্লিষ্ট ডিপার্টমেন্ট কে এবং এক কপি নিয়ন্ত্রণকারী কার্যালয়কে প্রদান করতে হবে।

ধাপ-৪: অফিসে ফিরে এসে নিরীক্ষা দল সংক্ষিপ্তভাবে প্রতিবেদনটি ডিপার্টমেন্টের প্রধানের নিকট উপস্থাপন করবেন। ডিপার্টমেন্ট প্রধান উক্ত প্রতিবেদনে উত্থাপিত আপত্তি ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনে প্রেরণ করবেন। প্রয়োজনে ডিভিশনের প্রধান প্রতিবেদনটি উর্ধ্বতন কর্তৃপক্ষ বরাবরেও পাঠাতে পারেন।

৭.২.২ আইটেম নিরীক্ষা প্রক্রিয়াঃ

ধাপ-১: আইসিবির প্রধান নির্বাহী কর্মকর্তা একজন এসপিও/নির্বাহীকে দলনেতা করে কমপক্ষে দুইজন নিরীক্ষকের সমন্বয়ে একটি নিরীক্ষা দল গঠন করবেন । এই উদ্দেশ্যে নিরীক্ষা দলকে অফিস নির্দেশ ও শাখা/ ডিপার্টমেন্ট প্রধানকে পত্র প্রদান করবেন।

ধাপ-২: অফিস নির্দেশ পাওয়ার পর দলনেতা তার দল, প্রয়োজনীয় ডকুমেন্টস ও উপকরণসহ নিরীক্ষাধিন স্থানে যাবেন। নিরীক্ষা দল চেকলিস্ট অনুসারে যাচাই করবেন। চেকলিস্টের পাশাপাশি নিরীক্ষকগণ নিজস্ব মতামতের ভিত্তিতে নিরীক্ষা করতে পারবেন।

ধাপ-৩: চেকলিস্টের বিষয়সমূহ যাচাই বাছাই এর পর নিরীক্ষা দল একটি নিরীক্ষা প্রতিবেদন প্রস্তুত করবেন। প্রতিবেদনের এক কপি সংশ্লিষ্ট ডিপার্টমেন্ট/কার্যালয়/শাখাকে এবং এক কপি ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান বরাবর উপস্থাপন করবেন।

ধাপ-৪: ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান নিরীক্ষা দলের প্রতিবেদন পাওয়ার পর সংশ্লিষ্ট ডিপার্টমেন্ট/শাখাকে পত্র প্রদান করবেন এবং নির্দিষ্ট সময়ের মধ্যে উত্থাপিত আপত্তিসমূহ পরিপালন করার অনুরোধ করবেন। এছাড়া, ডিভিশনের প্রধান প্রয়োজনে প্রতিবেদনটি উর্ধ্বতন কর্তৃপক্ষ ও বিভিন্ন ডিপার্টমেন্টে (যে সমস্ত ডিপার্টমেন্ট প্রতিবেদনে উত্থাপিত আপত্তিসমূহ সমাধানের সাথে যুক্ত) প্রয়োজনীয় পদক্ষেপ গ্রহণের জন্য পাঠাতে পারবেন।

৭.২.৩: সিস্টেম নিরীক্ষা প্রক্রিয়া:

ধাপ-১ নির্বাচিত কোনো হার্ডওয়্যার/সফটওয়্যারের জন্য দলনেতা হিসেবে এসপিও/নির্বাহী কর্মকর্তা ও কমপক্ষে দুইজন নিরীক্ষকের সমন্বয়ে ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান একটি নিরীক্ষা দল গঠন করেন। এ উদ্দেশ্যে নিরীক্ষা দলকে অফিস নির্দেশ ও সংশ্লিষ্ট ডিপার্টমেন্টেকে চিঠি প্রদান করবেন ।

ধাপ-২ অফিস নির্দেশ পাওয়ার পর দলনেতা ও তার দল প্রয়োজনীয় উপকরণ ও ডকুমেন্টসহ সংশ্লিষ্ট স্থানে গমন করবেন। নিরীক্ষা দল প্রয়োগযোগ্য বিষয়সমূহ যাচাই বাছাই করবে। তাছাড়া নিরীক্ষা দলের নিজস্ব পর্যবেক্ষণও থাকতে পারে।

ধাপ-৩: চেকলিস্টের বিষয়সমূহ যাচাই বাছাই এর পর নিরীক্ষা দল নিরীক্ষা প্রতিবেদন প্রস্তুত করবে। প্রতিবেদনের এককপি সংশ্লিষ্ট ডিপার্টমেন্ট এবং এক কপি ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের এর প্রধানের কাছে উপস্থাপন করবে।

ধাপ-৪: ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান সংশ্লিষ্ট বিভাগ ও নিয়ন্ত্রণকারী কর্তৃপক্ষের নিকট নির্দিষ্ট সময়ের মধ্যে উত্থাপিত আপত্তিসমূহ পরিপালন করার অনুরোধ প্রদান করবেন। এছাড়াও প্রতিবেদনটি প্রয়োজনে উর্ধতন কর্তৃপক্ষের নিকট প্রয়োজনীয় পদক্ষেপের গ্রহণের জন্য প্রেরণ করা যেতে পারে।

৭.২.৪: বিশেষ নিরীক্ষা প্রক্রিয়া:

ধাপ-১: নির্বচিত শাখা বা ডিপার্টমেন্টে বিশেষ নিরীক্ষা পরিচালনার জন্য ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের এর প্রধানকে দলনেতা করে একটি নিরীক্ষা দল গঠন করতে হবে। এ উদ্দেশ্যে উর্ধ্বতন কর্তৃপক্ষ নিরীক্ষা দলকে অফিস নির্দেশ ও সংশ্লিষ্ট শাখা/ডিপার্টমেন্টকে পত্র প্রদান করবেন।

ধাপ-২: অফিস নির্দেশ পাওয়ার পর দলীয় প্রধান নিরীক্ষা দল ও প্রয়োজনীয় ডকুমেন্টস, উপকরণসহ সংশ্লিষ্ট স্থানে গমন করবেন। নিরীক্ষা দল পূর্ববর্তী নিয়মিত নিরীক্ষার উচ্চ ঝুঁকিপূর্ণ আপত্তিসমূহ পর্যালোচনা করবে। নিরীক্ষা দল সংশ্লিষ্ট শাখায় অভ্যন্তরীণ নিয়ন্ত্রণ ও পরিপালন এর অবস্থা নিরীক্ষা করবে। তাছাড়া, নিরীক্ষা দলের নিজস্ব পর্যালোচনা থাকতে পারে।

ধাপ-৩: নিরীক্ষা সম্পন্ন করার পর নিরীক্ষা দল আইসিবির উর্ধ্বতন কর্তৃপক্ষকে প্রতিবেদন প্রদান করবে। পরিপালনের জন্য এক কপি সংশ্লিষ্ট শাখা বা ডিপার্টমেন্টে প্রেরণ করবে ।

৭.২.৫: আকস্মিক নিরীক্ষা প্রক্রিয়া:

ধাপ-১: নির্বাচিত শাখা/ডিপার্টমেন্ট আকস্মিক নিরীক্ষার জন্য ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধানের নেতৃত্বে নিরীক্ষা দল গঠন করা হবে। এ জন্য উর্ধ্বতন কর্তৃপক্ষ নিরীক্ষা দলকে অফিস নির্দেশ ও সংশ্লিষ্ট শাখা/ডিপার্টমেন্টকে পত্র প্রদান করবেন।

ধাপ-২: অফিস আদেশ পাওয়ার পর দলীয় প্রধান তার প্রয়োজনীয় ডকুমেন্টস/উপকরণ/সরঞ্জামাদিসহ সংশ্লিষ্ট শাখা/ডিপার্টমেন্টে গমন করবেন । দলটি সংক্ষিপ্ত ভাবে শাখা/ডিপার্টমেন্টে তথ্য ও যোগাযোগ প্রযুক্তি কার্যক্রম পরিদর্শন করবেন এবং পূর্ববর্তী নিরীক্ষায় উত্থাপিত আপত্তিসমূহের পরিপালনের জন্য প্রয়োজনীয় পরামর্শ/নির্দেশনা প্রদান করবেন। তাছাড়াও নিরীক্ষা দলের নিজস্ব পর্যবেক্ষণও থাকতে পারে ।

ধাপ-৩: নিরীক্ষা পর দলটি একটি নিরীক্ষা প্রতিবেদন প্রস্তুত করে এর এক কপি উর্ধ্বতন কর্তৃপক্ষের নিকট উপস্থাপন করবেন এবং এক কপি ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনে ও এক কপি সংশ্লিষ্ট শাখা/কার্যালয়ে প্রেরণ করবেন।

৭.২.৬: তদারকি:

ধাপ-১: নির্বাচিত শাখা/ডিপার্টমেন্ট (যেখানে নিয়মিত নিরীক্ষা দল নিরীক্ষা কার্যক্রম পরিচালনা করছেন) পর্যবেক্ষণের জন্য ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান/নির্বাহীর নেতৃত্বে একটি দল গঠন করা হবে। এই উদ্দেশ্যে উর্ধ্বতন কর্তৃপক্ষ নিরীক্ষা দলকে অফিস নির্দেশ প্রদান করবেন।

ধাপ-২: অফিস নির্দেশ পাওয়ার পর দলনেতা তার দল নিয়ে প্রয়োজনীয় ডকুমেন্টস/উপকরণ/সরঞ্জামাদিসহ সংশ্লিষ্ট শাখা/ডিপার্টমেন্টে যাবেন। দলটি সংক্ষিপ্তভাবে নিয়মিত নিরীক্ষা দলের কার্যক্রম পরিদর্শন করবেন। দল নেতার মন্তব্য শাখার ভিজিটরস্ বুকে লিপিবদ্ধ করতে হবে। নিরীক্ষা ও পরিদর্শন দলের নিজস্ব পর্যবেক্ষণও থাকতে পারে।

ধাপ-৩: পরিদর্শন সম্পন্ন করার পর দলটি ভিজিটরস বুকের পাতার কপি সংগ্রহ করবেন এবং ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের এর প্রধান অথবা উধর্বতন কর্তৃপক্ষের কাছে উপস্থাপন করবেন।

৭.২.৭: জালিয়াতি ও অপরাধ পরিদর্শন ও পর্যবেক্ষণ:

ধাপ-১: কোনো শাখা/ডিপার্টমেন্টের জালিয়াতি কার্যক্রম অনুসন্ধানের জন্য কর্তৃপক্ষ ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান কোনো নির্বাহী/এসপিওকে দলনেতা করে একটি নিরীক্ষা দল গঠন করবেন। এ উদ্দেশ্যে নিরীক্ষা দলকে অফিস নির্দেশ ও সংশ্লিষ্ট শাখা/ডিপার্টমেন্টকে পত্র প্রদান করবেন।

ধাপ-২: অফিস নির্দেশ পাওয়ার পর দলনেতা বিশদভাবে অনুসন্ধানের জন্য প্রয়োজনীয় ডকুমেন্ট/উপকরণ/সরঞ্জামাদিসহ তার দলকে নিয়ে শাখা/কার্যালয়/ডিপার্টমেন্টে যাবেন।

ধাপ-৩: পর্যবেক্ষণের পর দলটি একটি অনুসন্ধানী প্রতিবেদন প্রস্তুত করে ইন্টারনাল কন্ট্রোল এন্ড কমপ্লাইন্স ডিভিশনের প্রধান এর মাধ্যমে উর্ধ্বতন কর্তৃপক্ষের নিকট তা উপস্থাপন করবে।

অধ্যায়- ৮
প্রতিবেদন প্রণয়ন

৮.১ তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা প্রতিবেদন:

প্রস্তুতকারকের পরিচয়:

নিরীক্ষা প্রক্রিয়ার প্রকৃতি, সময়, পরিধি দলিলায়নে নিরীক্ষককে নিম্নোক্ত বিষয়সমূহ রেকর্ড করতে হবে:

- কে নিরীক্ষা সম্পাদন করেছে ও এ ধরনের কাজের তারিখ এবং
- কে নিরীক্ষা দলিলায়ন (documentation) পর্যালোচনা করেছেন এবং এ ধরনের নিরীক্ষার তারিখ।

নিরীক্ষা প্রমাণক:

ইলেক্ট্রনিক উৎস থেকে প্রাপ্ত প্রমাণকও নিরীক্ষা প্রতিবেদন বিবেচনায় প্রমাণ হিসেবে গ্রহণযোগ্য । যতদূর সম্ভব প্রমাণকের মধ্যে তারিখ ও সময় এর উল্লেখ নিশ্চিত করতে হবে। উদাহরণস্বরূপ, SQL Query করার সময় প্রমাণকে Query ও অন্তর্ভূক্ত থাকবে। Query-তে সিস্টেমের তারিখ এবং সময়ও অন্তর্ভুক্ত থাকবে ।

কোনো পদ্ধতি থেকে অন্য পদ্ধতিতে উপাত্ত স্থানান্তর করার সময় সম্ভব হলে ফরওয়ার্ডিং লেটার অথবা অনুমোদনের কপি সংগ্রহ করতে হবে । এটি সম্ভব না হলে সংশ্লিষ্ট অফিস কোনো ফাইল থেকে কবে উপাত্ত স্থানান্তর করেছে, উপাত্ত ঘটনা চলাকালীন না কি অন্য কোনো পরিবেশ থেকে গৃহীত হয়েছে ইত্যাদির মত গুরুত্বপূর্ণ তথ্য লিখে অভ্যন্তরীণ প্রমানক তৈরি করতে হবে। নিরীক্ষা প্রতিবেদনের জন্য প্রস্তুতকৃত ও ব্যবহৃত ইলেক্ট্রনিক প্রমাণক ও এ ধরনের দলিলের সাথে সম্পর্কিত হতে হবে ।

ব্যবস্থাপনা কর্তৃপক্ষের জবাব :

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার ক্ষেত্রে নিরীক্ষা পর্যবেক্ষণের অনুমোদন/জবাব গ্রহণ খুবই গুরুত্বপূর্ণ । আনুষ্ঠানিক জবাব নেয়া কঠিন হলে সংশ্লিষ্ট অফিসের সর্বোচ্চ ব্যবস্থাপনা কর্তৃপক্ষের সাথে বৈঠকের চেষ্টা করা এবং প্রাপ্ত ফলাফল লিখে তা সংরক্ষণ করতে হবে। এ প্রচেষ্টা ব্যর্থ হলেও চেষ্টা করার বিষয়ে পর্যাপ্ত প্রমাণ রেকর্ড করা এবং এ চেষ্টা করার বিষয়টি প্রতিবেদনে উল্লেখ করতে হবে।

নিরীক্ষা প্রতিবেদন তৈরি :

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার ক্ষেত্রে নিরীক্ষা পর্যবেক্ষণের মূল ভিত্তি হল পদ্ধতি । নিরীক্ষার ক্ষেত্রে সাধারণ প্রতিবেদন কাঠামো অনুসরণ করতে হবে। প্রতিবেদন প্রণয়নের ক্ষেত্রে প্রাপ্ত উপাদানের দীর্ঘ পর্যালোচনা এবং অপ্রয়োজনীয় বিষয় উল্লেখ করা যাবে না। নিরীক্ষিত একটি মাত্র বিষয়কে গুরুত্ব দিয়ে খসড়া অনুচ্ছেদ উপস্থাপন করতে হবে।

প্রতিবেদনের আবশ্যিক বৈশিষ্ট্যাবলী:

- **নৈর্ব্যক্তিকতা ও বস্তুনিষ্ঠতা :** নিরীক্ষিত বিষয়সমূহ সম্পর্কে প্রদত্ত মন্তব্য, মতামত, সুপারিশ ইত্যাদি নিরপেক্ষ ও পক্ষপাতমুক্ত এবং ব্যক্তিগত স্বার্থের উর্ধ্বে থেকে প্রতিবেদন প্রদান।
- **স্পষ্টতা:** প্রতিবেদনে প্রদত্ত মতামত সরল ভাষায় ও স্পষ্টভাবে উল্লেখকরণ।
- **যথার্থতা:** প্রতিবেদনে উল্লেখিত তথ্যসমূহ যথাসম্ভব সতর্কতার সাথে নির্ভুলভাবে উপস্থাপন করা।
- **সংক্ষিপ্ততা:** তথ্যবহুল সংক্ষিপ্ত প্রতিবেদন।
- **সময়ানুবর্তিতা:** প্রতিবেদন নির্ধারিত সময়ে প্রস্তুত করে জমা প্রদান।

৮.২ প্রতিবেদনের উপাদান :

প্রতিবেদন প্রণয়নে সাধারণত নিম্নোক্ত শিরোনামগুলো ব্যবহার করা যেতে পারেঃ

ভূমিকা:

পরিচালিত তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার সংক্ষিপ্ত ভূমিকায় প্রতিবেদনে গুরুত্বপূর্ণ পয়েন্টসমূহ থাকতে হবে। প্রতিবেদনে অবশ্যই সংক্ষেপে পদ্ধতির বিস্তারিত অবস্থা তুলে ধরতে হবে যাতে এর সফটওয়্যারের অবস্থা ও পদ্ধতি চালাতে প্রয়োজন এমন হার্ডওয়্যার উৎসের উল্লেখ থাকবে। উপাত্তের পরিমাণ, প্রক্রিয়াকরণে জটিলতা এবং অন্যান্য প্রাসঙ্গিক বিস্তারিত বিষয়ও এতে তুলে ধরতে হবে যাতে পাঠক নিরীক্ষা ফলাফল মূল্যায়নে পদ্ধতি সম্পর্কে একটি পরিষ্কার ধারণা পায়। উপাত্ত প্রবাহ জটিল হলে প্রতিবেদনে ফ্লোচার্ট সংযোজন করতে হবে।

উদ্দেশ্য, আওতা ও পদ্ধতি :

নিরীক্ষার উদ্দেশ্য হল, নিরীক্ষার লক্ষ্য অর্জনের আওতা ও পদ্ধতি সম্পর্কে জ্ঞাত হওয়া, নিরীক্ষা কাজের যথার্থতা বিচার করা এবং কি রিপোর্ট করা হয়েছে তার গুরুত্বপূর্ণ সীমাবদ্ধতা সম্পর্কেও ধারণা রাখা। প্রতিবেদন প্রণয়নের সময় নিরীক্ষার প্রেক্ষিতে নিরীক্ষার উদ্দেশ্যগুলি স্পষ্ট ভাবে তুলে ধরতে হবে।

নিরীক্ষার পরিধি উপস্থাপনে নিরীক্ষককে নিরীক্ষা কর্মের গভীরতা ও ব্যাপ্তি তুলে ধরতে হবে। নিরীক্ষক ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যার এবং ঘাটনা কাল, প্রমাণকের ধরন ও উৎস প্রতিবেদনে তুলে ধরবেন। উপাত্তের সীমাবদ্ধতা বা সুযোগের স্বল্পতার কারণে নিরীক্ষা কার্যক্রমে নিরীক্ষক যে উল্লেখযোগ্য বাধার সম্মুখীন হয়েছেন তাও প্রতিবেদনে থাকবে।

পদ্ধতি সম্পর্কে প্রতিবেদন তৈরির ক্ষেত্রে প্রমাণ সংগ্রহ ও বিশ্লেষণে ব্যবহৃত কৌশল সম্পর্কে নিরীক্ষককে স্পষ্টভাবে ব্যাখ্যা করতে হবে। নিরীক্ষা কার্যক্রম পরিচালনায় কোনো গুরুত্বপূর্ণ অনুমান গ্রহণ করে থাকলে তা উল্লেখ করা; কোনো তুলনামূলক কৌশল প্রয়োগ করলে তা বর্ণনা করা; বাছাইকৃত নমুনায় ব্যবহৃত মানদন্ড ও নিরীক্ষকের প্রাপ্ত ফলাফলকে কখন তাৎপর্যপূর্ণভাবে সমর্থন করেছে তা তুলে ধরা এবং নমুনা বাছাই এবং কেন তা বাছাই করা হয়েছে এ ব্যাখ্যায় তা উল্লেখ করতে হবে ।

নিরীক্ষায় প্রাপ্ত ফলাফল:

প্রতিটি নিরীক্ষা উদ্দেশ্যের বিপরীতে প্রাপ্ত ফলাফল নিরীক্ষক তার প্রতিবেদন উপস্থাপন করবেন। ফলাফল উপস্থাপনের ক্ষেত্রে প্রতিবেদনের বিষয় সম্পর্কে পর্যাপ্ত ধারণা দিতে এবং সঠিক, বিশ্বাসযোগ্য ও নিরপেক্ষভাবে তা উপস্থাপন করতে নিরীক্ষককে পর্যাপ্ত, উপযুক্ত ও প্রাসঙ্গিক তথ্য সংযোজন করতে হবে।

অর্থের মানদন্ডে মূল্যায়ন:

তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষার আর্থিক মূল্যের প্রশ্ন একটি জটিল বিষয় । উপাত্তের বিশ্লেষণমূলক পর্যালোচনা ও ফলাফলের বিষয়ে প্রতিবেদন প্রস্তুতের ক্ষেত্রে যেকোনো পর্যালোচনায় আর্থিক দিকটি উঠে আসে । একইভাবে ক্রয় কার্যক্রমের মত বিষয়ে মন্তব্য করা হলে আর্থিক মূল্য নির্ধারণ একটি প্রধান বিবেচ্য বিষয় হয়ে দাঁড়ায়। সুতরাং, পর্যালোচনার আকারে উপস্থাপিত প্রচলিত তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা প্রতিবেদনে এই মূল্যসহ এবং আর্থিক মূল্য ছাড়া পর্যবেক্ষণ উঠে আসতে হবে। তথ্য ও যোগাযোগ প্রযুক্তি নিরীক্ষা নিয়ন্ত্রণের অভাবের সাথে সংশ্লিষ্ট সম্ভাব্য ঝুঁকির উপর করা হয় বলে সে মূল্য নির্ধারণ করা যায় না। নিরীক্ষা কাযর্ক্রম পরিচালনা করার সময় অবশ্যই নিরীক্ষায় আনুমানিক ক্ষতির সম্ভব্যতা (Exposure) হিসাব করার চেষ্টা থাকতে হবে। এটি ঝুঁকির সম্মুখীন কোনো বিষয়ের সঠিক চিত্র উপস্থাপন করে এবং পর্যবেক্ষণকে বিশ্বাসযোগ্যতা প্রদান করে। নিরীক্ষায় এ ধরনের ক্ষতির সম্ভাব্যতা নির্ণয় করা না গেলে সেটি কেন করা যায় না প্রতিবেদনে তাও স্পষ্টভাবে বর্ণনা থাকবে। উদাহরণস্বরূপ, অগ্নি নির্বাপন ব্যবস্থার মত বাহ্যিক নিরাপত্তার অভাবের উপর মন্তব্য করা হলে ঝুঁকিপূর্ণ সম্পদের মোট মূল্যও নিরীক্ষায় উল্লেখ্য ।

অর্থমূল্যের গুরুত্বকে প্রয়োগের ধরন ও বৃহত্তর পরিসরে প্রতিষ্ঠানের ভূমিকার প্রেক্ষিতে দেখা হয়। উদাহরণস্বরূপ, প্রতিরক্ষা বিষয়ক কোনো প্রতিষ্ঠানে প্রবেশ নিয়ন্ত্রণে ঘাটতির সে মুহূর্তে কোনো আর্থিক কার্যকারিতা না থাকলেও গুরুতর প্রতিক্রিয়া হতে পারে। অন্যদিকে প্রতারণার ঘটনা, তছরুপ, আত্নসাৎ ইত্যাদি না ঘটলে এ ব্যবস্থায় আর্থিক মূল্য গুরুত্বপূর্ণ বলে বিবেচিত হবে ।

৮.৩ উপসংহার

নিরীক্ষার উদ্দেশের ভিত্তিতে রিপোর্টে সিদ্ধান্ত উপস্থাপন করতে হবে। নিরীক্ষকের প্রদত্ত সিদ্ধান্তসমূহ নিরীক্ষায় প্রাপ্ত ফলাফলের সমর্থনে প্রদত্ত প্রমাণকের বিশ্বাসযোগ্যতা এবং যুক্তির উপর নির্ভর করে ।

বাস্তব পরীক্ষায় সমর্থিত না হলে নিয়ন্ত্রণ ও ঝুঁকি অনুপস্থিতির বিষয়ে সুস্পষ্ট সিদ্ধান্তে উপনীত হওয়া যাবে না। উদাহরণস্বরূপ কোনো প্রতিষ্ঠানের তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা না থাকার বিষয়টি নিরীক্ষায় উঠে এলেও 'তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা না থাকলে একটি প্রতিষ্ঠানে তথ্য ও যোগাযোগ প্রযুক্তি বিশৃঙ্খলভাবে সংযোজিত হতে পারে ও এর ফলে হার্ডওয্যার ক্রয় ও সফটওয়্যার ডেভেলপমেন্টে অসংগতি দেখা দিতে পারে। এক্ষেত্রে বিশৃঙ্খলভাবে তথ্য ও যোগাযোগ প্রযুক্তি সংযোজিত হয়েছে কিনা এবং তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালার অভাবেই এমনটি হয়েছে কি না এবং যদি হয়ে থাকে তাহলে কিভাবে এমনটি হয়েছে নিরীক্ষায় সেটিও দেখতে হবে । প্রতিবেদনটি বিভিন্ন পর্যবেক্ষণের মধ্যে যুক্তিসংগতভাবে সংযোগ স্থাপন করার উপযোগী হতে হবে । উদাহরণস্বরূপ, CAATs ব্যবহার করে দেখা গেছে যে, দুর্বল নিরাপত্তা নিয়ন্ত্রণের ফলে অননুমোদিত লেনদেনের ঘটনা ঘটে। এসব আলাদা আলাদাভাবে উল্লেখ না করে এর মাধ্যমে আরও পরিস্কারভাবে তথ্য ও যোগাযোগ প্রযুক্তি পরিবেশের সামগ্রিক ঘাটতি তুলে ধরতে হবে।

৮.৪ সুপারিশ:

আইন ও বিধি-বিধান পরিপালনে বিচ্যুতির গুরুত্বপূর্ণ উদারহণ পাওয়া গেলে বা নিয়ন্ত্রণে উল্লেখযোগ্য দুর্বলতা দেখা গেলে পরিপালনে যথাযথ ভূমিকা রাখতে এবং ব্যবস্থাপনা নিয়ন্ত্রণ উন্নয়নে তৎপর হওয়ার সুপারিশ করতে হবে। বর্তমান নিরীক্ষার উদ্দেশ্যকে প্রভাবিত করতে পারে পূর্ববর্তী নিরীক্ষার এমন অসংশোধিত গুরুত্বপূর্ণ বিষয় ও সুপারিশের অবস্থা নিরীক্ষককে তার প্রতিবেদনে তুলে ধরতে হবে ।গঠনমূলক সুপারিশ উন্নয়নকে উৎসাহিত করতে পারে ।

গঠনমূলক সুপারিশের বৈশিষ্ট্যগুলি হলো:

- চিহ্নিত সমস্যার কারণ দূরীকরণের উপায় নির্দেশ করা;
- পদক্ষেপ নেয়া উপযোগী ও সুনির্দিষ্ট সুপারিশ প্রদান;
- দায়িত্বরত কর্তৃপক্ষের উদ্দেশ্যে সুপারিশ করা,
- বাস্তবায়নযোগ্য ও বাস্তব ভিত্তিক এবং ব্যয়সাশ্রয়ী সুপারিশ প্রদান।

কোনো গুরুত্বপূর্ণ পরিপালন-বিচ্যুতির বিষয়ে প্রতিবেদন প্রস্তুত করতে হলে নিরীক্ষককে সংগতিপূর্ণভাবে প্রাপ্ত ফলাফল উপস্থাপন করতে হবে। পাঠককে পরিপালন-বিচ্যুতির প্রবলতা ও প্রতিফল বিচারের ভিত্তি দেয়ার জন্য, পরিপালন-বিচ্যুতির ঘটনাকে সামগ্রিক অবস্থা অথবা যাচাইকৃত ঘটনার সংখ্যার সাথে সম্পর্কিত এবং আর্থিক মানে পরিমাপ করতে হবে।

শাখার জন্য কার্যদর্শন তালিকা (Check list for Branch)

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
১. আইসিটি সম্পদ/ইনভেন্টরি ব্যবস্থাপনা (ICT Asset/Inventory Management)				
১.১	আইসিটি সম্পদসমূহ স্পষ্টভাবে চিহ্নিত ও লেবেলযুক্ত করা হয়েছে কিনা? লেবেল সম্পদের প্রতিষ্ঠিত শ্রেণীবিন্যাস (যথা: নাম, ক্রমিক নম্বর, ডিপার্টমেন্ট/ডিভিশন/শাখার নাম এবং ক্রয়ের বৎসর) প্রতিফলিত করে কিনা?	L		
১.২	গুরুত্বপূর্ন বিস্তারিত বিষয় (যথা: মালিক,তত্ত্বাবধায়ক (custodian) কর্মকর্তা, ক্রয়ের তারিখ,স্থান, লাইসেন্স নম্বর, কনফিগারেশন ইত্যাদি) উল্লেখপূর্বক আইসিটি অ্যাসেট ইনভেন্টরি সংরক্ষণ করা হয় কি না?	M		
১.৩	আইসিটি অ্যাসেট ইনভেন্টরি সময়ে সময়ে পর্যালোচনা ও হালনাগাদ করা হয় কি না?	M		
১.৪	অননুমোদিত প্রবেশ, অপব্যবহার বা জালিয়াতিমূলক পরিবর্তন, সংযোজন, বিয়োজন, প্রতিস্থাপন, তথ্য গোপন অথবা প্রকাশ করা থেকে ইনফরমেশন সিস্টেম সুরক্ষিত কি না?	H		
১.৫	আইসিবিতে ব্যবহৃত সফটওয়্যারসমূহ সফটওয়্যার লাইসেন্সের শর্তাবলী পরিপালন করে কি না?	H		
১.৬	অননুমোদিত ও পাইরেটেড সফটওয়্যার ব্যবহার সম্পূর্নভাবে/কঠোরভাবে নিষিদ্ধ কি না?	H		
১.৭	শাখার অ্যাসেট কম্পিউটার রেজিস্টারে হার্ডওয়্যার/সফটওয়্যারের ক্রয়মূল্য ও বুক ভেলু লেখা হয় কি না?	M		
১.৮	বছর শেষে ক্রয়কৃত হার্ডওয়্যার/সফটওয়্যারের অবচয় কর্তন করা হয় কি না?	H		
১.৯	ক্রয়কৃত হার্ডওয়্যার/সফটওয়্যারের ক্রয় বা অধিগ্রহনের তারিখ, ভেন্ডর পরিচিতি, সংযোজন/বিতরণের তারিখ, ওয়ারেন্টি পিরিয়ড ইত্যাদিসহ আইসিটি অ্যাসেটের জন্য ডেড স্টক রেজিস্টার (বর্জন তালিকা) যথাযথভাবে সংরক্ষণ করা হয় কি না?	M		
১.১০	বিধি মোতাবেক ক্রয় কমিটি গঠন করা হয়েছে কি না?	M		
১.১১	কম্পিউটার স্টেশনারি খাতে ব্যয় বাজেটের মধ্যে থাকে কি না ?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
২. ডেস্কটপ/ল্যাপটপ/ওয়ার্ক স্টেশন ডিভাইস নিয়ন্ত্রণ (Desktop/Laptop/Workstation Devices Controls)				
২.১	উপাত্ত ও হার্ডওয়্যারের ক্ষতি প্রতিরোধ করতে ইউপিএস এর সাথে ডেস্কটপ কম্পিউটার সংযুক্ত করা হয়েছে কি না?	M		
২.২	ডেস্কটপ বা ল্যাপটপ ত্যাগ করার পূর্বে ব্যবহারকারিগণ "লক ওয়ার্কস্টেশন" ফিচার কার্যকর করেন কি না?	H		
২.৩	৫ মিনিট সময় নির্ধারণ করে প্রতিটা কম্পিউটারে পাসওয়ার্ড প্রোটেকটেড স্ক্রিন সেভার সেট করা আছে কি না?	H		
২.৪	ল্যাপটপে সংরক্ষিত গোপনীয় ও স্পর্শকাতর তথ্য এনক্রিপ্ট করা থাকে কি না?	H		
২.৫	প্রত্যেক কর্মদিবস শেষে ডেস্কটপ কম্পিউটার, ল্যাপটপ, মনিটর, ইউপিএস, প্রিন্টার ইত্যাদি সঠিকভাবে বন্ধ করা হয় কি না ?	M		
২.৬	ব্যবহৃত না হলে ল্যাপটপ, কম্পিউটার মিডিয়া এবং স্পর্শকাতর তথ্য রয়েছে এমন সব রিমোভ্যাবল স্টোরেজ (যথা: সিডি রমস, জিপ ডিস্কস, প্যাডস, ফ্লাশ ড্রাইভস, এক্সটারনাল হার্ড ড্রাইভস) নিরাপদ স্থানে বা ডাটা সেভ লকারে সংরক্ষণ করা হয় কি?	H		
২.৭	ডেস্কটপ/ল্যাপটপ কম্পিউটারের ইউএসবি পোর্ট এ প্রবেশাধিকার নিয়ন্ত্রিত কি না?	M		
২.৮	পূর্বানুমতি ছাড়া কোনো ব্যবহারকারী কোনো ডেস্কটপ বা ল্যাপটপে সফটওয়্যার এবং/অথবা ব্যবহারযোগ্য ফাইল ইন্সটল বা ডাউনলোড করে কি না?	H		
২.৯	সেলফ রেপ্লিকেট, ক্ষতি অথবা অন্যভাবে কোনো কম্পিউটারের কার্যক্রম বাধাগ্রস্থ করতে ডেস্কটপ ও ল্যাপটপ ব্যবহারকারী কোনো কম্পিউটার কোড (যথাঃ ভাইরাস, ওয়ার্ম, ট্রোজান ইত্যাদি) লেখা, সংকলন, নকল, জেনেবুঝে প্রচার, প্রয়োগ বা সংযোজনের প্রচেষ্টা চালায় কি না?	H		
২.১০	সনাক্তকৃত ভাইরাস সম্পর্কে যথাযথ কর্তৃপক্ষকে তাৎক্ষণিকভাবে অবহিত করা হয় কি না?	H		
২.১১	দক্ষ ব্যক্তির সহায়তা ছাড়া ভাইরাস ক্লিন/ডিলিট করা হয় কি না?	H		
২.১২	ডেস্কটপ ও ল্যাপটপসমূহ চালু অথবা পুণঃচালু করতে ব্যবহারকারীর পরিচিতি (ID) ও পাসওয়ার্ড প্রয়োজন হয় কি না?	H		
২.১৩	সকল ডেস্কটপ ও লেপটপ কম্পিউটারে মানসম্মত ভাইরাস চিহ্নিতকরণ সংক্রান্ত সফটওয়্যার ইন্সটল করা আছে কি না?	H		
২.১৪	ফাইল পড়া এবং ভাইরাস সনাক্তকরণে নিয়মিতভাবে সিস্টেম স্ক্যান করার জন্য মানসম্মত ভাইরাস চিহ্নিতকরণ সফটওয়্যার কনফিগার করা আছে কি না?	H		
২.১৫	সকল গুরুত্বপূর্ণ কম্পিউটার নিরাপত্তা সংশ্লিষ্ট বিষয় (যথা: পাসওয়ার্ড অনুমান, অননুমোদিতভাবে প্রবেশের চেষ্টা বা এপ্লিকেশন বা সিস্টেম সফটওয়্যারের পরিবর্তন) লগ করার জন্য ডেস্কটপ ও ল্যাপটপ কম্পিউটার কনফিগার করা আছে কি না?	H		
২.১৬	সকল কম্পিউটার মেঝে থেকে উপরে ও জানালা থেকে দূরে স্থাপন করা হয়েছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৩. সার্ভার/নেটওয়ার্ক রুম/র‍্যাক নিয়ন্ত্রণ (Server/Network Room/Rack Controls)				
৩.১	দায়িত্বশীল কোনো ব্যক্তির অধীনে সার্ভার/নেটওয়ার্ক কক্ষ/তাক কাচ ঘেরা স্থানে তালাবদ্ধ আছে কি না?	H		
৩.২	নির্ধারিত কাজের উল্লেখ পূর্বক ব্যবহারকারীর সার্ভার ব্যবহারের সুনির্দিষ্ট অনুমোদন আছে কি না?	H		
৩.৩	যথাযথ ফরমেট অনুসারে সার্ভার কক্ষের জন্য ভিজিটরস লগ বই সংরক্ষণ করা হয় কি?	M		
৩.৪	১ মিনিট সময় নির্ধারণ করে সার্ভারে পাসওয়ার্ড প্রোটেকটেড স্ক্রিন সেভার সেট করা আছে কি না?	M		
৩.৫	সিস্টেম এডমিনিস্ট্রেটরের কর্মকান্ড লগ করা হয় কি না?	H		
৩.৬	সার্ভার/নেটওয়ার্ক কক্ষ/তাক শীতাতপ নিয়ন্ত্রিত কি না?	H		
৩.৭	সার্ভার/নেটওয়ার্ক কক্ষ/তাক এ সংস্থাপিত শীতাতপ নিয়ন্ত্রণ যন্ত্র থেকে পানি চোয়ানো বা পানি নিষ্কাশন (Drainage) ব্যবস্থা আছে কি না?	H		
৩.৮	ফাইল শেয়ার করার প্রক্রিয়ার (যথাঃ শুধু পড়ার সুযোগ দিয়ে ফাইল শেয়ার করা) নিরাপত্তা নিশ্চিত করা হয়েছে কি না?	H		
৩.৯	প্রয়োজন না হলে ফাইল ও প্রিন্টার শেয়ার করার ব্যবস্থা অকার্যকর অথবা সম্ভব হলে এর ব্যবহার নিম্নতম পর্যায়ে রাখা হয় কি না?	H		
৩.১০	সার্ভর কক্ষে প্রবেশাধিকার নিয়ন্ত্রিত কি না?	H		
৩.১১	সার্ভারে প্রবেশের অনুমোদন তালিকা সংরক্ষণ ও নিয়মিতভাবে পর্যবেক্ষণ করা হয় কি না?	M		
৩.১২	কোনো বিপর্যয় ঘটলে যথাসম্ভব কম সময়ে সার্ভার ও নেটওয়ার্ক সরঞ্জামাদি পুনঃস্থাপনের ব্যবস্থা আছে কি না?	H		
৩.১৩	কোনো কারণে বিদ্যুৎ বিভ্রাট ঘটলে কার্যক্রম অব্যাহত রাখার জন্য জেনারেটর এর সংযোগ করা আছে কি না?	H		
৩.১৪	প্রয়োজনীয় তার টানার জন্য বিদ্যুতের তার ও ডাটা কেবলের হুক অনুযায়ী পরিচ্ছন্ন ও নিরাপদ দুরত্ব বজায় রেখে দেয়ালে চ্যানেল স্থাপন করা হয়েছে কি না?	H		
৩.১৫	জরুরি পরিস্থিতি মোকাবেলায় যোগাযোগের জন্য সকল ঠিকানা ও ফোন নম্বর (যথা: ফায়ার সার্ভিস, পুলিশ স্টেশন, সেবা প্রদানকারী, ভেন্ডর এবং সকল আইসিটি/ দায়িত্বপ্রাপ্ত ব্যক্তি) আছে কি না এবং তা দেয়ালে দৃশ্যমান অবস্থায় রয়েছে কিনা?	M		
৩.১৬	অন্য কোনো কারণে প্রয়োজন না হলে সার্ভার কক্ষ ত্যাগ করার পূর্বে বিদ্যুৎ সংযোগ বন্ধ করা হয় কি না?	H		
৩.১৭	সার্ভার কক্ষের বাইরে দৃশ্যমান স্থানে অগ্নি নির্বাপক যন্ত্র স্থাপন করা আছে কি না?	H		
৩.১৮	প্রতি বছর অগ্নি নির্বাপক যন্ত্র রিফিল ও মেয়াদ পরীক্ষা করা হয় কি না?	H		
৩.১৯	দূরবর্তী স্থান থেকে সার্ভারে সংযোগ স্থাপনের সুযোগ আছে কি না? দূর থেকে সংযোগ স্থাপনের জন্য 'টিম ভিউয়ার" এর মত কোনো সফটওয়্যার ইন্সটল করা আছে কি না?	H		
৩.২০	কোনো অপ্রয়োজনীয় প্রোগ্রাম সার্ভারে ইন্সটল করা আছে কি না?	H		
৩.২১	সার্ভারে চালু থাকা অপ্রয়োজনীয় সেবাদান ব্যবস্থা অকার্যকর করা হয়েছে কি না?	H		
৩.২২	সার্ভার এবং প্রয়োজনীয় নেটওয়্যার্ক সরঞ্জামাদিতে অন-লাইন ইউপিএস সংযোগ দেয়া আছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৪. নেটওয়ার্ক নিরাপত্তাব্যবস্থা (Networks Security Management)				
৪.১	ইউটিপি, ফাইবার, বিদ্যুৎসহ সব ধরনের (ভবিষ্যৎ সংশোধন বা প্রতিরোধমূলক সংস্কার কাজের জন্য) ক্যাবল চিহ্নযুক্ত (labeled) করা হয়েছে কি না?	M		
৪.২	নেটওয়ার্ক সরঞ্জামাদির জন্য বস্তুগত নিরাপত্তা নিশ্চিত করা হয়েছে কি না?	H		
৪.৩	WAN সংযোগের জন্য Redundant যোগাযোগ লিংক বিদ্যমান আছে কি না?	H		
৪.৪	অফিস নেটওয়ার্কে ব্যক্তিগত ল্যাপটপ বা অফিসের কোনো ব্যক্তিগত ওয়্যারলেস মডেম সংযোগ দেয়া হয় কি না?	H		
৪.৫	নেটওয়ার্ক সরঞ্জামাদির ডিফল্ট পাসওয়ার্ড পরিবর্তন করা হয় কি না?	H		
৪.৬	একসেস সুইচে (প্রযোজ্য ক্ষেত্রে) সকল অব্যবহৃত পোর্ট বাই ডিফল্ট বন্ধ হয়ে/করা যায় কি না ?	H		
৪.৭	যথাযথ সত্যায়ন (Authentication) সহ সকল যোগাযোগ সরঞ্জামাদি স্বতন্ত্রভাবে চিহ্নিত করা যায় কি না?	M		
৪.৮	বৈদ্যুতিক তার ও নেটওয়ার্ক তার টানার জন্য আলাদা চ্যানেল ব্যবহার করা হয়েছে কি না?	M		
৫. মেলিসিয়াস কোড/ভাইরাস নিরাপত্তা ব্যবস্থা (Malicious Code/Virus Protection)				
৫.১	মেলিসিয়াস কোড থেকে সুরক্ষার জন্য সার্ভার ও ওয়ার্কস্টেশনে অনুমোদিত (লাইসেন্সকৃত) এন্টি-ভাইরাস প্যাকেজ ইন্সটল করা হয়েছে কি না?	H		
৫.২	সম্ভাব্য মেলিসিয়াস কোড চিহ্নিত করার জন্য সিস্টেমসমূহে চলমান গুরুত্বপূর্ণ ব্যবসায়িক কার্যক্রম নিয়মিত স্ক্যান করা হয় কি না?	H		
৫.৩	অনিশ্চিত বা অজ্ঞাত নেটওয়ার্ক থেকে ইলেক্ট্রনিক মিডিয়ার মাধ্যমে প্রাপ্ত ফাইল ব্যবহারের পূর্বে মেলিসিয়াস কোড যাচাই করে দেখা হয় কি না?	H		
৫.৪	ইলেক্ট্রনিক মেইলের সংযুক্তি (Attachments) ব্যবহারের পূর্বে মেলিসিয়াস কোড যাচাই করে দেখা হয় কি না?	H		
৫.৫	স্বয়ংক্রিয় ও সময়ানুগত প্রক্রিয়া ব্যবহার করে সর্বশেষ ভাইরাস সনাক্তকরণ ফাইল দ্বারা এন্টিভাইরাস প্যাকেজ হাল নাগাদ রাখা হয় কি না?	H		
৫.৬	নেটওয়ার্কের সকল কম্পিউটার সার্ভার থেকে স্বয়ংক্রিয়ভাবে হালনাগাদ (Updated) এন্টিভাইরাস সফটওয়্যার পায় কি না?	M		
৫.৭	ডিস্ক, টেপ, সিডি বা ভাইরাসবাহী অন্যান্য মাধ্যমে ভাইরাস থেকে স্বয়ংক্রিয় সুরক্ষা ব্যবস্থা (Mode) সক্রিয় আছে কি না?	H		
৫.৮	ভুয়া ভাইরাসের (Hoax Viruses) সমস্যা সম্পর্কে কর্মকর্তা-কর্মচারিগণ সচেতন আছে কি না যাতে তারা এ ক্ষেত্রে ভাইরাস বিষয়ক সতর্ক সংকেত (Virus Alarms) না পাঠায় ?	H		
৫.৯	কম্পিউটার ভাইরাস ও তার প্রতিরোধ কৌশল সম্পর্কে অবহিত করতে প্রান্তিক ব্যবহারকারীদের জন্য কোনো সচেতনতামূলক কর্মসূচি আয়োজন করা হয় কি না?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৬. ইন্টারনেটে প্রবেশ ব্যবস্থাপনা(Internet Access Management)				
৬.১	অনুমোদিত ইন্টারনেট ব্যবহার-ব্যবস্থাপনা-নীতি অনুযায়ী কর্মকর্তা-কর্মচারিদের ইন্টারনেট ব্যবহারের সুযোগ দেয়া হয় কি না?	M		
৬.৩	তথ্যের নিরাপত্তার বিষয়টি নিশ্চিত না হলে আইসিবি ভবন বা একক কম্পিউটার ও ল্যাপটপসহ সিস্টেম থেকে ইন্টারনেটে সরাসরি স্থানীয় সংযোগ দেয়া নিষিদ্ধ কি না?	H		
৬.৪	আইসিবির সিস্টেম বা শাখা কার্যালয় থেকে কর্মকর্তা-কর্মচারিদের ইন্টারনেটে নিজস্ব সংযোগ স্থাপন নিষিদ্ধ কি না?	H		
৬.৫	সুনির্দিষ্টভাবে অনুমোদিত না হলে ব্রডব্যান্ড, আইএসডিএন বা পিএসটিএন সেবা ব্যবহার করে ইন্টারনেট বা কোনো তৃতীয় পক্ষ (Third-party) অথবা গণ নেটওয়ার্কে (Public Network) সংযোগ স্থাপনের জন্য আইসিবির সিস্টেমের সাথে স্থানীয়ভাবে যুক্ত মডেম ব্যবহার করা নিষিদ্ধ কি না?	H		
৬.৬	আইসিবি কর্তৃক পরিচালিত নয় এমন কোনো বাণিজ্যিক ব্যবসায়িক কর্মকান্ড (আইসিবির কর্মী অথবা অন্য কারও ব্যক্তিগত ব্যবসা) সম্পাদনে আইসিবি প্রদত্ত ইন্টারনেট ব্যবহার করা হয় কি না?	H		
৬.৭	আইসিবি প্রদত্ত ইন্টারনেট সংযোগ সচেতনভাবে এমন কোনো কাজে ব্যবহার করা হয় কি না যা কোনো ফৌজদারী বা দেওয়ানী আইনের লংঘন?	H		
৭. ই-মেইল ব্যবস্থাপনা(Email Management)				
৭.১	আইসিবির নীতিমালা অনুযায়ী ইমেইল সিস্টেম ব্যবহার করা হয় কি না?	M		
৭.২	দাপ্তরিকভাবে অনুরোধের (Official Request) মাধ্যমে ইমেইল সিস্টেমে প্রবেশাধিকার দেয়া হয় কি না?	M		
৭.৩	ইমেইল ব্যবহার করে বহিঃস্থ কোনো পক্ষের সাথে এনক্রিপশন ছাড়া গোপনীয় তথ্য আদান-প্রদান করা হয় কি না?	H		
৭.৪	ইমেইল প্রেরণের পূর্বে অথবা বহিঃস্থ পক্ষের ইমেইলের জবাব প্রদানের ক্ষেত্রে কর্মকর্তা-কর্মচারিগণ ইমেইলের বিষয়বস্তুর গোপনীয়তা ও স্পর্শকাতরতার বিষয়টি বিবেচনায় রাখেন কি না?	H		
৭.৫	ইমেইলের মাধ্যমে প্রেরিত তথ্য মানহানিকর, অবমাননাকর, কোনো ধরনের জাতিগত বিদ্বেষ বা যৌন নির্যাতনমূলক, আইসিবির সুনামের জন্য হানিকর অথবা এতে এমন কোনো উপাদান থাকে যা কর্মকর্তা-কর্মচারি, গ্রাহক, প্রতিযোগী বা অন্যের জন্য ক্ষতিকর?	H		
৭.৬	কর্মকর্তা-কর্মচারিগণ (ব্যবস্থাপনা কর্তৃপক্ষের ইচ্ছা ও যথাযথ অনুমতি ছাড়া) ব্যক্তিগত কাজে আইসিবির ইমেইল ব্যবহার করেন কি না?	M		
৭.৭	ব্যবস্থাপনা কর্তৃপক্ষের অনুমতি না নিয়ে কোনো ধরনের সামাজিক যোগাযোগ, ব্লগ, গ্রুপ, ফোরাম ইত্যাদিতে কর্পোরেট ইমেইল ঠিকানা ব্যবহার হয় কি না?	M		
৭.৮	আইসিবি কর্তৃক প্রেরিত ইমেইলের বিষয়বস্তুকে গোপনীয় ঘোষনা করে যথাযথ ব্যক্তি কর্তৃক তা খোলার কথা বলা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৮. ব্যবহারকারীর প্রবেশাধিকার ব্যবস্থাপনা (User Access Management)				
৮.১	কাঙ্খিত সময়ে ও ব্যবহারের প্রয়োজনের উপর ভিত্তি করে আইসিটি সিস্টেম ও নেটওয়ার্কে ব্যবহারকারীর প্রবেশাধিকার অনুমোদন করা হয় কি না?	M		
৮.২	নেটওয়ার্কে প্রবেশাধিকার সংরক্ষণের জন্য আইসিবির (স্থায়ী) কর্মী নয় (চুক্তিভিত্তিক, বাইরে থেকে সংগৃহিত বা ভেন্ডর কর্মী) এমন ব্যক্তিদের নিবিড়ভাবে পর্যবেক্ষণ করা হয় কি না?	H		
৮.৩	প্রত্যেক ব্যবহারকারীর একটি স্বতন্ত্র পরিচিতি ও বৈধ পাসওয়ার্ড আছে কি না?	H		
৮.৪	ব্যবহারের সুযোগসমূহ (Access Privileges) উল্লেখসহ নানা রকম পরিচিতি রক্ষণাবেক্ষণ ফরম (User ID Maintenance Form) যথাযথ কর্তৃপক্ষ কর্তৃক নিয়মানুগভাবে অনুমোদন করা হয় কি না?	H		
৮.৫	উপর্যুপরি তিন বার অসফল লগইন প্রচেষ্টার (Unsuccessful Login Attempts) পর ইউজার একসেস বন্ধ হয়ে যায় কি না?	M		
৮.৬	কাজের ধরন পরিবর্তনের সাথে সাথে ব্যবহারকারীর ব্যবহারের সুযোগসমূহ (User access Privileges) হালনাগাদ করা হয় কি না?	H		
৮.৭	অডিট ও পর্যবেক্ষণের উদ্দেশ্যে ব্যবহারকারীর প্রবেশাধিকার (User Access) স্বতন্ত্রভাবে চিহ্নিত ও লগ করা হয় কি না?	H		
৮.৮	ব্যবহারকারী সংযোজন/বিয়োজন/স্থগিতকরণ/হালনাগাদকরণের জন্য ব্যবহারকারী পরিচিতি রক্ষণাবেক্ষণ ফরম (User ID Maintenance Form) ব্যবহার করা হয় কি না?	M		
৮.৯	ব্যবহারকারীর পরিচিতি রক্ষণাবেক্ষণ ফরম (User ID Maintenance Form) এ সকল প্রয়োজনীয় তথ্য (শুরু/শেষের তারিখ/সময়, সুযোগ ইত্যাদি) থাকে কি না?	L		
৮.১০	ব্যবহার পরিচিতি রক্ষণাবেক্ষণ ফরম (User ID Maintenance Form) বাস্তবায়নের পূর্বে যথাযথ কর্তৃপক্ষ কর্তৃক অনুমোদিত হয় কি না এবং অডিট ও পর্যালোচনার উদ্দেশ্যে তা সংরক্ষণ করা হয় কি না?	M		
৮.১১	ব্যবহারকারীরা তাদের লগইন তথ্য (User ID, Password) গোপন রাখে কি না এবং অন্যের সাথে শেয়ার করা এড়িয়ে চলে কি না?	H		
৮.১২	ইউজার আইডি রেজিস্টার যথাযথ ফরমেটে সংরক্ষণ ও হালনাগাদ করা হয় কি না?	M		
৮.১৩	শাখা প্রধান/ব্যবস্থাপক আইসিবির এপ্লিকেশন সফটওয়্যারের সকল ব্যবহারকারীর প্রবেশাধিকার (User access right) আনুষ্ঠানিকভাবে পর্যালোচনা এবং প্রদত্ত অধিকার (Rights) অনুযায়ী অফিস নির্দেশ জারি করেন কি না?	M		
৮.১৪	কোনো কর্মকর্তা বদলী/পদত্যাগ/পিআরএল এ গমন করলে তাদের অব্যাহতি প্রদানের পূর্বে শাখা নির্বাহী/ব্যবস্থাপক তাদের ব্যবহারকারী পরিচিতি (User ID) অকার্যকর করেন কি না?	H		
৯. পাসওয়ার্ড ব্যবস্থাপনা (Password Management)				
৯.১	প্রথম লগঅন করলে ব্যবহারকারীদের বাধ্যতামূলকভাবে পাসওয়ার্ড পরিবর্তন করা হয় কি না?	M		
৯.২	ন্যূনতম ১০ অক্ষরের মধ্যে পাসওয়ার্ড দেয়ার বিষয়টি মেনে চলা হয় কি না?	M		
৯.৩	বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্নের মধ্যে অন্তত তিনটি শ্রেণীর সমন্বয়ে পাসওয়ার্ড দেয়ার বিষয়টি সিস্টেম নিশ্চিত করে কি না?	H		
৯.৪	সর্বোচ্চ ৯০ দিন পর পাসওয়ার্ড পরিবর্তন করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৯.৫	একই পাসওয়ার্ড অন্তত তিন বার ব্যবহার করা যাবে এমনভাবে সিস্টেমে পাসওয়ার্ড ইতিহাস সংরক্ষণের ব্যবস্থা কার্যকর করা আছে কি না?	H		
৯.৬	অপারেটিং সিস্টেম, ডাটাবেইজ এবং বিজনেস এপ্লিকেশন সফটওয়্যারে ব্যবহৃত এডমিনিস্ট্রেটিভ পাসওয়ার্ড সমূহ এনভেলপে ভরে সিলগালা করে নিরাপদ স্থানে সংরক্ষণ করা হয় কি না?	H		
৯.৭	ব্যবহারকারীগণ কোনো এপ্লিকেশনে "Remember Password"বৈশিষ্ট্যের ব্যবহার এড়িয়ে চলে কি না?	H		
৯.৮	এনক্রিপশন ছাড়া কোনো টেক্স ফাইলে পাসওয়ার্ড সংরক্ষণ করা হয় কি না?	H		
৯.৯	সাধারন ব্যবহারকারী পাসওয়ার্ড কাগজে লিখে রাখা হয় কি না?	H		
৯.১০	লগইন তথ্য জনসাধারণের ব্যবহৃত চ্যানেলের মাধ্যমে ইমেইল প্রেরণ করা হয় কি না?	H		
১০. ইনপুট নিয়ন্ত্রণ (Input Control)				
১০.১	প্রতিটি সিস্টেম ব্যবহারকারীকে সেশন টাইম আউট সময় নির্ধারণ করা আছে কি না?	M		
১০.২	এপ্লিকেশন সফটওয়্যার ব্যবহারকারীদের ইনপুটের সময়সূচি অর্ন্তভূক্ত করা হয় কি	H		
১০.৩	উপাত্ত সংযোজন, বিয়োজন, পরিবর্তনের জন্য ব্যবহারকারী পরিচিতি (User ID) ও ডেট-টাইম স্ট্যাম্প সহ অডিট ট্রায়াল সংরক্ষণ করা হয় কি না?	M		
১০.৪	একই ট্রানজেকশনের ক্ষেত্রে একই ব্যক্তিকে মেকার ও চেকার করা হয় কি না?	H		
১০.৫	স্পর্শকাতর উপাত্ত এবং এপ্লিকেশনের ক্ষেত্রে প্রবেশাধিকার সংরক্ষিত কিনা?	H		
১১. অগ্রাধিকার প্রবেশ ব্যবস্থাপনা(Privileged Access Management)				
১১.১	অগ্রাধিকারপ্রাপ্ত ব্যবহারকারীদের জন্য নিম্নলিখিত নিয়ন্ত্রণ ও নিরাপত্তা ব্যবস্থা গ্রহণ করা হয়েছে কি না? ক. যথাযথ শক্তিশালী বাছাইকরন কৌশল প্রয়োগ; খ.দূরবর্তী স্থান (Remote Access) থেকে প্রবেশের ক্ষেত্রে শক্তিশালী নিয়ন্ত্রণ আরোপ ; গ. সুবিধাপ্রাপ্ত ব্যবহারকারীর সংখ্যা সীমিতকরণ । ঘ. প্রয়োজনের (need-to-have) ভিত্তিতে প্রবেশাধিকার অনুমোদন; ঙ.সময়ের ভিত্তিতে সুবিধাপ্রাপ্ত ব্যবহারকারীদের কার্যক্রম পর্যালোচনা; চ.Privileged হিসাবসমূহের শেয়ারিং নিষিদ্ধকরণ।	H		
১২. ব্যবসা চালু রাখার পরিকল্পনা (Business Continuity Plan)				
১২.১	আইটি কর্মকর্তা অথবা দায়িত্ব প্রাপ্ত ব্যক্তি দ্বারা সার্ভার, নেটওয়ার্কিং সরঞ্জামাদি, ল্যান এবং অন্যান্য হার্ডওয়্যার রক্ষণাবেক্ষণ করা হয় কি না?	H		
১২.২	জরুরি অবস্থায় কনফিগারকৃত ব্যাকআপ সার্ভার ও অন্যান্য রিসোর্স প্রস্তুত রাখার বিষয়টি নিশ্চিত করা হয়েছে কি না?	M		
১২.৩	শাখাসমূহে দৈনিক/মাসিক/ত্রৈমাসিক/ষান্মাসিক/বার্ষিক ডাটা ব্যাকআপসংরক্ষণ করা হয় কি না?	M		
১২.৪	বিদ্যুৎ ব্যবস্থা ও তার সাথে সম্পৃক্ত সরঞ্জামাদি (Online UPS, standalone UPS, Generator, AVRইত্যাদি) পর্যাপ্ত আছে কি নেই?	M		
১২.৫	প্রয়োজনীয় দাপ্তরিক তথ্য-উপাত্ত নিরাপদ রাখা হয়েছে কি না?	M		
১২.৬	প্রয়োজনীয় তথ্যের ব্যাকআপ রাখা হয়েছে কি না ?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
১২.৭	পর্যাপ্ত বিদ্যুৎ সরবরাহ, তাপমাত্রা নিয়ন্ত্রণ ব্যবস্থা এবং তার সাথে সংশ্লিষ্ট সরঞ্জামাদির ব্যবস্থা নিশ্চিত করা হয়েছে কি হয় নাই?	M		
১২.৮	অগ্নি নির্বাপক ব্যবস্থা নিশ্চিত করে সময়ে সময়ে পরীক্ষা করা হয় কি না?	H		
১২.৯	শুধু হার্ডড্রাইভ থেকে কম্পিউটার বুট করতে বায়োস কনফিগার করা হয়েছে কি না?	M		
১২.১০	কম্পিউটার বায়োস পাসওয়ার্ড সুরক্ষিত কি সুরক্ষিত নয়?	M		
১২.১১	উপাত্ত প্রাপ্তির বিষয়টি নিয়ন্ত্রিত কি নিয়ন্ত্রিত নয়?	H		
১২.১২	টেবিলের উপর বসানো স্পর্শকাতর উপাত্তধারী কম্পিউটার নিরাপদে অথবা তালা বন্ধ কক্ষে রাখা আছে কি না?	H		
১২.১৩	অতিথি হিসাব (Guest Account) নিষ্ক্রিয় করা হয়েছে কিনা?	M		
১৩. ডাটা ব্যাকআপ ও পুনরুদ্ধার ব্যবস্থাপনা (Data Backup and Restore Management)				
১৩.১	শাখার লিগেসি এপ্লিকেশন সফটওয়্যারের ব্যাকআপ সার্ভার প্রস্তুত কি প্রস্তুত নয়?	H		
১৩.২	শাখাসমূহে দৈনিক/মাসিক/ত্রৈমাসিক/ষান্মাসিক/বার্ষিক ডাটা ব্যাকআপসংরক্ষণ করা হয় কি না?	M		
১৩.৩	প্রধান কার্যালয়ের নির্দেশনা মোতাবেক সফলভাবে সমাপনান্তে (Day End Process) এ শাখা কর্তৃক সিডি/ডিভিডিতে (লিগেসি এপ্লিকেশন সফটওয়্যারের) সেকেন্ডারি ব্যাকআপ নিয়ে এর একটি কপি শাখায় অথবা অন্য কোথাও সংরক্ষণ করে কি না?	M		
১৩.৪	প্রধান কার্যালয়ের নির্দেশ মোতাবেক ত্রৈমাসিক/ষান্মাসিক এবং বার্ষিক ব্যাকআপের (এপ্লিকেশন সফটওয়্যারসহ) সিডি/ডিভিডি নিকটতম শাখা অথবা অন্য কোনো স্থানে সংরক্ষণ করে কি না?	M		
১৩.৫	ব্যাকআপের তথ্য ধারণকারী সকল মাধ্যম তথ্যের বিষয়বস্তু, ব্যাকআপ সাইকেল, ব্যাকআপের ক্রম চিহ্ন (Backup Serial Identifier), ব্যাকআপের তারিখ এবং তথ্যের শ্রেণি বিন্যাস সহ লেবেল যুক্ত (Labeled) করা হয় কি না?	M		
১৩.৬	তদারককারী কর্তৃক ব্যাকআপ ইনভেন্টরি ও লগ শিট সংরক্ষণ, যাচাই-বাছাই ও স্বাক্ষরিত হয় কি না?	M		
১৩.৭	ব্যাকআপ মিডিয়ায় স্পর্শকাতর বা গোপনীয় তথ্যের ব্যাকআপ অফিসের বাইরে (offsite) সংরক্ষণের জন্য প্রেরণের পূর্বে এনক্রিপ্ট করা হয় কি না?	H		
১৩.৮	দুর্যোগপূর্ণ সময়ে কর্মকান্ড অব্যাহত রাখতে অন্তত এককপি ব্যাকআপ on-site এ সংরক্ষণ করা হয় কি না?	M		
১৩.৯	অন-সাইট ও অফ-সাইট উভয় ব্যাকআপ স্টোরেজ থেকে তথ্য পুণঃস্থাপনের প্রক্রিয়া নথিবদ্ধ করা হয় কি না?	H		
১৩.১০	ব্যাক আপ মিডিয়ার (উপাত্ত) পুনরুদ্ধারের সক্ষমতা সময়ে সময়ে পরীক্ষা ও গ্রহণযোগ্যভাবে যাচাই করা হয় কি না?	H		
১৩.১১	অন-সাইট ব্যাকআপ মিডিয়া লগ রেজিস্টারে নিম্নে বর্ণিত তথ্য থাকে কি না? ক.ব্যাকআপ নেওয়ার তারিখ। খ. মিডিয়ার বিষয়বস্তু (যেমনঃ ট্রানজেকশন ব্যাকআপ, এপ্লিকেশন ব্যাকআপ এবং সম্পূর্ন সিস্টেমের ব্যাকআপ)। গ. অফ-সাইট অবস্থানে মিডিয়া পরিবহনের তারিখ। ঘ. ব্যাকআপের ধরন (যেমনঃ সম্পূর্ণ ব্যাকআপ বা ডাটাবেইজ অথবা ফাইল কপি)। ঙ. অন-সাইট লোকেশন এর দায়িত্বপ্রাপ্ত ব্যক্তির নাম ও স্বাক্ষর। চ.অন্য যেকোন স্তরের তথ্য।	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
১৩.১২	অফ-সাইট ব্যাকআপ মিডিয়া লগ রেজিস্টারে নিয়ে বর্ণিত তথ্যাদি থাকে কি না? ক. অফ-সাইট লোকেশনে মিডিয়া গ্রহণের তারিখ; খ.মিডিয়ার বিষয়বস্তু (যেমনঃ ট্রানজেকশন বাকআপ, এপ্লিকেশন ব্যাকআপ এবং সম্পূর্ন সিস্টেমের ব্যাকআপ); গ. ব্যাকআপের ধরন (যেমনঃ সম্পূর্ণ ব্যাকআপ বা ডাটাবেইজ অথবা ফাইল কপি); ঘ. বহনকারীর নাম; ঙ. প্রকৃত স্থানের নাম; চ. অন-সাইট লোকেশনে গ্রহণের দায়িত্বপ্রাপ্ত ব্যক্তির নাম ও স্বাক্ষর; ছ.অন্য যেকোন স্তরের তথ্য।	M		
১৩.১৩	ব্যাকআপের নিম্নবর্ণিত রিটেনশন পিরিয়ড পলিসি অনুসরণ করা হয় কি না? ক. প্রতি কার্যদিবসই প্রাত্যহিক ব্যাকআপ এবং ০৬ দিন (অফলাইনে) ব্যাকআপ রাখা। খ. সাপ্তাহিক পরিক্রমায় ব্যাকআপ নেয়া। গ. প্রতি মাসের শেষ দিনে মাসিক ভিত্তিতে সার্ভারের ডাটা ব্যাকআপ নেয়া। ঘ. সারা বছর ত্রৈমাসিক ভিত্তিতে ব্যাকআপ নেয়া। ঙ. সারা বছর ষান্মাসিক ভিত্তিতে ব্যাকআপ নেয়া। চ. বছরান্তে বার্ষিক ব্যাকআপ নেয়া।	M		
১৩.১৪	পরিবহনকৃত ব্যাকআপ গ্রহণ এবং প্রেরণের রেজিস্টার সংরক্ষণ করা হয় কি হয় না?	M		
১৩.১৫	একটি ব্যাপক কর্মসূচি অনুযায়ী প্রয়োজনীয় ব্যবসায়িক তথ্য, উপাত্ত ও সফটওয়্যারে দৈনিক/সাপ্তাহিক/মাসিক/ত্রৈমাসিক এবং বাৎসরিক ব্যাকআপ নেয়া হয় কি না?	M		
১৩.১৬	ব্যাকআপ সফলভাবে নেয়ার বিষয়টি নিশ্চিত করতে ব্যাকআপ নেয়া উপাত্ত যাচাই বাছাই করা হয় কি না?	H		
১৩.১৭	প্রাথমিক ব্যাকআপ সার্ভারের হার্ড ডিস্ক ড্রাইভে এবং ব্যাকআপ মিডিয়ায় সংরক্ষণ করা হয় কি না?	M		
১৪.	**সিসিটিভি সারভেইলেন্স (CCTV surveillance)**			
১৪.১	শাখার ভল্ট রুম, ক্যাশ কাউন্টার, সার্ভার রুম/ আইটি রুম, ভেতরের স্থানসমূহ, বাইরের প্রবেশ পথসহ আশপাশের এলাকা জুড়ে পর্যাপ্ত সিসিটিভি/ আইপি ক্যামেরা/ স্পাই ক্যামেরা স্থাপন করা আছে কি না?	M		
১৪.২	আইসিবি'র কেন্দ্রীয় ইনফরমেশন সিস্টেমের সাথে সিসিটিভি/ আইপি ক্যামেরা/ স্পাই ক্যামেরা সংযুক্ত করা আছে কি না?	M		
১৪.৩	শাখায় কোনো স্বয়ংক্রিয় এলার্ম ব্যবস্থা রয়েছে কি না?	M		
১৪.৪	সিসিটিভি ক্যামেরায় ধারনকৃত ছবি অন্তত এক বৎসর/ অনুমোদিত সময় পর্যন্ত সংরক্ষণ করা হয় কি না?	H		
১৪.৫	সিসিটিভি/ আইপি ক্যামেরা/ স্পাই ক্যামেরাসমূহ সার্বক্ষনিক চালু রাখা এবং সপ্তাহে প্রতিদিন চব্বিশ ঘন্টা ভিডিও নজরদারী করা হয় কি না?	H		
১৪.৬	সিসিটিভি কার্যক্রম পরিচালনার জন্য সিসিটিভি এ্যাক্সেস নিয়ন্ত্রন ব্যবস্থা আছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
১৪.৭	শুধু দায়িত্বপ্রাপ্ত কর্মকর্তারই সিসিটিভি নজরদারী সিস্টেমে প্রবেশাধিকার থাকে কি না? অন্য কর্মকর্তার উপরও সিসিটিভি নজরদারী ব্যবস্থায় প্রবেশাধিকার দেয়া হয় কি না?	H		
১৪.৮	অনুপস্থিত বা ছুটিকালীন সময়ে যথাযথ কর্তৃপক্ষের অনুমতি সাপেক্ষে সংশ্লিষ্ট কর্মকর্তা অন্য জনের কাছে সিসিটিভি এ্যাক্সেস নিয়ন্ত্রণ হস্তান্তর করেন কি না?	H		
১৪.৯	সিসিটিভি অপারেশনের দায়িত্বপ্রাপ্ত কর্মকর্তার প্রয়োজনীয় প্রশিক্ষণ আছে কি না?	M		
১৪.১০	প্রতিদিন ২৪ ঘন্টাই সচল কোনো এলার্ম ভল্টে রয়েছে কি না (যেটি কর্পোরেশনের কেন্দ্রীয় ইনফরমেশন সিস্টেমের সাথে যুক্ত)	H		
১৪.১১	শাখার ভল্টে সপ্তাহের ৭ দিনে ২৪ ঘন্টা ব্যাপী কোনো নিরাপত্তা সংকেত (এ্যালার্ম) ব্যবস্থা প্রধান কার্যালয়ের তথ্য প্রযুক্তির সঙ্গে সংযুক্ত কি না?	H		
১৪.১২	ভল্টে স্বয়ংক্রিয় অগ্নি নির্বাপক যন্ত্র আছে কি না?	H		
১৪.১৩	প্রধান কার্যালয়, নিকটবর্তী থানা, র‍্যাব অফিস ও অন্যান্য অন্তত: ১০ টি গুরুত্বপূর্ন সংস্থার জরুরি টেলিফোন নম্বরসহ শাখায় স্বয়ংক্রিয় এ্যালার্ম সিস্টেম আছে কি না?	M		
১৫. এপ্লিকেশন সফটওয়্যার (Application Software)				
১৫.১	হিসাব বন্ধ হওয়ার সাথে সাথে এপ্লিকেশন সফটওয়্যারে "ক্লোজড" মার্ক করা হয় কি না?	H		
১৫.২	হিসাবের সর্বশেষ লেনদেন এর কপি ম্যানুয়াল হিসাব খোলার ফরমে 'একাউন্ট ক্লোজ' কথা লিখে যৌথ স্বাক্ষরে সংরক্ষণ করা হয় কি না?	M		
১৫.৩	গ্রাহকের নিকট থেকে লেনদেন বন্ধ করার আবেদন পাওয়ার সাথে সাথে এপ্লিকেশন সফটওয়্যারে "স্টপ পেমেন্টে" মার্কিং করা হয় কি না?	H		
১৫.৪	প্রযোজ্য ক্ষেত্রে সফটওয়্যারে "লিয়েন মার্ক" করে রাখা হয় কি না?	H		
১৫.৫	লিমিট অনুসারে এপ্লিকেশন সফটওয়্যারের বিভিন্ন ঋণ ও অগ্রীম হিসাবে লিমিট সেট করা হয় কি না?	H		
১৫.৬	সর্বশেষ বিজ্ঞপ্তি অনুসারে শাখার এপ্লিকেশন সফটওয়্যারে সুদহার/ আবগারী শুল্ক/ আনুষঙ্গিক চার্জ/ সেবা চার্জ স্টেট ও হালনাগাদ করা হয় কি না?	H		
১৫.৭	এপ্লিকেশন সফটওয়্যারে কোনো হিসাবে সুদ/ আবগারী শুল্ক/ আনুষাঙ্গিক চার্জ/ সেবা চার্জ একসেপশন সেট করা আছে কি না?	H		
১৫.৮	এপ্লিকেশন সফটওয়্যারে সঠিকভাবে 'হলিডে মার্কিং' করা আছে কি না?	H		
১৬. সিআইবি (CIB)				
১৬.১	শাখা সময়মত সিআইবি ডাটা প্রধান কার্যালয়ে প্রেরণ এবং এর এক সেট হার্ড কপি সংরক্ষণ করে কি না?	M		

প্রধান কার্যালয়ের ডিপার্টমেন্টের জন্য কার্যদর্শন তালিকা।
(Check List for Head Office Departments)

ক. আইসিটি সেবা দান ব্যবস্থাপনা (ICT Service Delivery Management)

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
১. পরিবর্তন ব্যবস্থাপনা (Change Management)				
১.১	কোন পরিবর্তনের ক্ষেত্রে Change Request Form এর মাধ্যমে আবেদন করা হয় কি না?	H		
১.২	Change Request Form যথাযথ কর্তৃপক্ষ কর্তৃক অনুমোদিত হয় কিনা?			
১.৩	প্রয়োজনীয় ডকুমেন্ট প্রস্তুত করা হয় কি না?	M		
১.৪	উৎপাদনের ক্ষেত্রে প্রয়োগকৃত বিজনেস এপ্লিকেশনের সমস্ত পরিবর্তন বিস্তারিত বিবরণসহ একটি আনুষ্ঠানিক দলিলায়ন প্রক্রিয়ার মধ্য দিয়ে পরিচালিত হয় কি?	H		
১.৫	অনাকাঙ্খিত কোনো ঘটনার উদ্ভব ঘটলে তা উত্তীর্নের জন্য রোলব্যাক পরিকল্পনা আছে কি না?	H		
১.৬	এপ্লিকেশনের কোনো পরিবর্তন কিংবা আপগ্রেডিং করা হলে প্রয়োগের পূর্বে ইউজার এক্সেপটেন্স টেস্ট করা হয় কি না?	H		
১.৭	এপ্লিকেশন সংযোজনের পর ইউজার ভেরিফিকেশন টেস্ট (UVT) করা হয় কি না?	H		
২. দুর্ঘটনা ব্যবস্থাপনা (Incident Management)				
২.১	কোনো দুর্ঘটনার পর ক্ষতির মাত্রা সহনীয় পর্যায়ে রেখে জরুরি ভিত্তিতে পুনরায় আইসিটি সার্ভিস চালু করার জন্য কোনো দুর্ঘটনা ব্যবস্থাপনা কাঠামো আছে কি না ?	H		
২.২	দুর্ঘটনা ব্যবস্থাপনা প্রক্রিয়ায় জড়িত কর্মকর্তা-কর্মচারির দায়িত্ব ও কর্তব্য (ঘটনা রেকর্ড বিশ্লেষণ প্রতিকার ও তদারকি করাসহ) নির্ধারিত আছে কি না?	H		
২.৩	দুর্ঘটনার তীব্রতার মাত্রা নিরূপন ও মূল্যায়নের কাজ কোনো কারিগরি সহায়তা ডেস্কের উপর ন্যস্ত করা হয়েছে কি না?	M		
২.৪	উচ্চ মাত্রার দুর্ঘটনা নির্ধারনে কারিগরি সহায়তা ডেস্কে দায়িত্বরতদের সঠিক প্রশিক্ষণ দেয়া হয়েছে কি না?	H		
২.৫	দুর্ঘটনার তীব্র মাত্রার সাথে সমানুপাতিকভাবে কোনো প্রচেষ্টা জোরদারকরণ ও সমাধান প্রক্রিয়া প্রতিষ্ঠিত আছে কি না?	M		
২.৬	নিরাপত্তা সংশ্লিষ্ট ঘটনায় পূর্ব নির্ধারিত প্রচেষ্টা জোরদারকরণ এবং তৎপরতার/সাড়া দেয়ার পরিকল্পনা সময়ে সময়ে পরীক্ষা করা হয় কি না?	H		
২.৭	কোনো গুরুতর দুর্ঘটনা মোকাবেলার জন্য কর্পোরেশনের কারিগরি ও অপারেশন পরিচালনায় দক্ষ কর্মীদের দ্বারা ICT Emergency Response Team গঠন করা হয়েছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
২.৮	কোনো গুরুতর দুর্ঘটনার সংবাদ গ্রাহকদের অবহিত করা হয় কি না?	M		
২.৯	একই ধরনের দুর্ঘটনার পুনরাবৃত্তি রোধে প্রতিরোধমূলক ব্যবস্থা নেয়া হয়েছে কি না?	H		
২.১০	যেসব গুরুতর দুর্ঘটনায় আইসিটি সেবা মারাত্মকভাবে ব্যাহত হয় তার মূল কারণ ও প্রভাব বিশ্লেষণ করা হয়েছে কি না?	H		
২.১১	প্রতিবেদনে নিম্নোক্ত বিষয়সমূহ অর্ন্তভূক্ত করা হয় কি না? **ক. মূল কারণ বিশ্লেষণ** i. কখন তা সংঘটিত হয় ? ii. কোথায় তা সংঘটিত হয়? iii.কেন এবং কিভাবে দুর্ঘটনা সংঘটিত হয়? iv.বিগত ২ বৎসরের মধ্যে অনুরূপ দুর্ঘটনা আরও কতবার সংঘটিত হয়েছে? v. কি ধরনের শিক্ষা উক্ত দুর্ঘটনা থেকে গ্রহণ করা হয়েছে? **খ. প্রতিফলন ও তার বিশ্লেষন** i. সংঘটিত দুর্ঘটনার ফলে সিস্টেমসমূহের তথ্য, উৎস এবং গ্রাহক কেমন ক্ষতির সম্মুখীন হতে পারে? ii. রাজস্ব হারানো, ক্ষতি, মূল্য, বিনিয়োগ, ক্ষতিগ্রস্থ গ্রাহকের সংখ্যা, প্রয়োগ, সুনাম ও আত্মবিশ্বাসের উপর প্রভাবসহ দূর্ঘটনার মাত্রা কিরূপ হতে পারে? iii. দূর্ঘটনার কারণে বিধিগত বাধ্যবাধকতা ও শর্তের লঙ্ঘন হয়েছে কি না? **গ) সংশোধন ও প্রতিরোধমূলক ব্যবস্থা** i. দূর্ঘটনার প্রভাব মোকাবেলায় তাৎক্ষনিকভাবে সংশোধনমূলক ব্যবস্থা গ্রহণ করতে হবে এবং গ্রাহকদের বিষয়কে প্রাধান্য দিতে হবে। ii. দুর্ঘটনার মূল কারণ উদঘাটন করতে হবে iii. ভবিষ্যতে একই ধরনের বা তৎসম্পর্কিত দুর্ঘটনা প্রতিরোধে ব্যবস্থা গ্রহণ করতে হবে।	H		
৩. সমস্যা ব্যবস্থাপনা (Problem Management)				
৩.১	ইনফরমেশন সিস্টেম সম্পর্কিত সমস্যা লগ আকারে সংরক্ষণ করার কোনো ব্যবস্থা আছে কি না?	H		
৩.২	এমন কোনো ব্যবস্থা প্রস্তুত রয়েছে কি না যাতে সমস্যা সংঘটিত হওয়ার সাথে সাথে সংশ্লিষ্ট ব্যক্তি খুব তাড়াতাড়ি ও কার্যকরভাবে সমাধান কল্পে সাড়া দিতে পারে?	H		
৩.৩	সমস্যা সমাধান প্রক্রিয়া চলাকালে সমস্যা চিহ্নিত করা ও কর্মপদক্ষেপ গ্রহণ করার বিষয় দলিলায়ন করা হয়েছে কি না?	H		
৩.৪	একই ধরনের সমস্যা চিহ্নিতকরণ ও পুনরাবৃত্তি রোধে পূর্বে সংঘটিত সমস্যার প্রবণতা বিশ্লেষণ করা হয়েছে কি না?	H		
৪. সক্ষমতা ব্যবস্থাপনা (Capacity Management)				
৪.১	আইসিটি সিস্টেম এবং অবকাঠামো ব্যবসা কার্যক্রমকে সহায়তা করতে সক্ষম এটা নিশ্চিত করতে কর্ম সম্পাদনের অবস্থা (performance), সক্ষমতা ও ব্যবহারের মত নির্দেশকসমূহ তদারকি ও পর্যালোচনা করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৪. ২	কার্যকরভাবে পরিচালনাগত ও ব্যবসায়িক চাহিদা মেটাতে বাড়তি সম্পদের পরিকল্পনা করা ও তা নির্ধারণে কোনো তদারকি ব্যবস্থা এবং উপযুক্ত সীমা নির্ধারন করা হয়েছে কি না ?	H		
খ. অবকাঠামোর নিরাপত্তা ব্যবস্থাপনার কার্যদর্শন তালিকা (Check List for Infrastructure Security Management)				
১. সম্পদ ব্যবস্থাপনা (Asset Management)				
১.১	নতুন আইসিটি সম্পদ ক্রয় করার পূর্বে তার দক্ষতা ও সক্ষমতা মূল্যায়ন করা হয়েছে কি না?	H		
১.২	সমস্ত আইসিটি সম্পদ ক্রয় ও সংস্থাপন করার পূর্বে আইসিবি'র ক্রয় নীতি অনুসরণ করা হয় কি না?	H		
১.৩	প্রতিটি আইসিটি সম্পদের উন্নয়ন, রক্ষনাবেক্ষন, ব্যবহার, নিরাপত্তা ও সঠিকতা নিশ্চিত করার দায়িত্ব কোনো তত্ত্বাবধায়কের (ব্যক্তি /প্রতিষ্ঠান) উপর অর্পণ করা হয়েছে কি না?	M		
১.৪	সকল আইসিটি সম্পদ স্পষ্টভাবে চিহ্নিত করে লেবেলযুক্ত করা হয়েছে কি না? লেবেলযুক্ত করণে সম্পদের শ্রেণিবিন্যাসের প্রতিষ্ঠিত রীতির প্রতিফলন ঘটে কি না?	M		
১.৫	উল্লেখযোগ্য বিস্তারিত তথ্য (যথা: সিরিয়াল নং, সরবরাহকারীর তথ্য, ওয়ারেন্টিকাল, মালিক, তত্ত্বাবধায়ক, ক্রয়ের তারিখ, স্থান, লাইসেন্স নম্বর, কনফিগারেশন ইত্যাদি) উল্লেখ করে আইসিটি ইনভেন্টরি সম্পন্ন করা হয় কি না?	M		
১.৬	আইসিটি সম্পদের ইনভেন্টরি সময় সময় পর্যালোচনা এবং হালনাগাদ করা হয় কি না?	M		
১.৭	অননুমোদিত প্রবেশ, অপব্যবহার, প্রতারণামূলক পরিবর্তন, সংযোজন, বিয়োজন, গোপন অথবা গোপনীয় তথ্য প্রকাশ করা থেকে ইনফরমেশন সিস্টেম সম্পদ সুরক্ষিত কি না?	H		
১.৮	তথ্য সিস্টেম সম্পদ সুরক্ষায় বর্জন নীতি (Disposal Policy) আছে কি না?	H		
১.৯	পোর্টেবল ডিভাইসের ব্যবহার বিশেষ করে কর্পোরেশনের বাইরে ব্যবহার করার কোনো গাইডলাইন আছে কি না?	H		
১.১০	কর্মী/ বহি:স্থ পক্ষের (employees/external parties) চাকুরিচ্যুতি, চুক্তি বাতিলের ক্ষেত্রে তাদের কাছে থেকে প্রতিষ্ঠানের সম্পদ ফিরিয়ে আনার কোনো নীতিমালা আছে কি না?	M		
১.১১	কর্পোরেশনে ব্যবহৃত সফটওয়্যারসমূহ লাইসেন্সের শর্ত প্রতিপালন করা হয় কি না?	M		
১.১২	Production Environment এর জন্য ক্রয়কৃত সফটওয়্যার ব্যবহারে ভেন্ডরের সাথে কোনো চুক্তি আছে কি না?	M		
১.১৩	যে কোনো কম্পিউটারে ব্যবহৃত হবে এমন সফটওয়্যারের কোনো অনুমোদিত তালিকা আছে কি না?	M		
১.১৪	অননুমোদিত অথবা পাইরেটেড সফটওয়্যার ব্যবহার কঠোরভাবে নিষিদ্ধ কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
২. ডেস্কটপ/ ল্যাপটপ সামগ্রী নিয়ন্ত্রণ (Desktop/ Laptop Devices Controls)				
২.১	ডেস্কটপ কম্পিউটারের তথ্য উপাত্ত এবং কোনো যন্ত্রাংশ নষ্ট হয়ে যাওয়া থেকে রক্ষা পাওয়ার জন্য ইউপিএস সংস্থাপন করা হয়েছে কি না?	M		
২.২	ব্যবহারকারীগণের ডেস্কটপ অথবা ল্যাপটপে ডাটা এনক্রিপ্ট করে সংরক্ষণ করা হয় কি না?	M		
২.৩	গোপনীয় বা স্পর্শকাতর তথ্যসমূহ ল্যাপটপে /ডেস্কটপে এনক্রিপ্ট করে সংরক্ষন করা হয় কি না?	H		
২.৪	প্রতি কর্মদিবস শেষে ডেস্কটপ কম্পিউটার মনিটর ইত্যাদি নিয়মিত বন্ধ করে রাখা হয় কি না?	M		
২.৫	যে সমস্ত মাধ্যমে স্পর্শকাতর তথ্য ধারণ করা হয় যেমন : সিডিরোম, জীপ ডিস্ক, পিডিএ, ফ্ল্যাশ ড্রাইভ, বাহিরের হার্ডড্রাইভ সমূহ ইত্যাদি; সে সমস্ত মাধ্যমগুলো যথেষ্ট নিরাপত্তা বলয়ের মধ্যে রাখা অথবা ব্যবহার না করার সময়ে কেবিনেটের মধ্যে বন্ধ করে রাখা হয় কি না?	M		
২.৬	ডেস্কটপ / ল্যাপটপ কম্পিউটারে ইউএসবি পোর্ট ব্যবহার নিয়ন্ত্রণ করা হয় কি না?	H		
২.৭	অন্যান্য গুরুত্বপূর্ন ও গোপনীয় তথ্য যেখানে সংরক্ষণ করা হয় যেমন: প্রয়োজনীয় কাগজ, নথি, টেপ ইত্যাদি অবশ্যই নিরাপত্তা বেষ্টিত এলাকায় অথবা যখন ব্যবহার করা হয় না তখন কেবিনেটে তালা বন্ধ করে রাখা হয় কি না?	H		
২.৮	পূর্ব অনুমতি ব্যতিরেকে ডেস্কটপ অথবা ল্যাপটপ কম্পিউটারে কোনো ধরনের এপ্লিকেশন সফটওয়্যার অথবা কার্যকরী ফাইল ইনস্টল বা ডাউনলোড করা হয় কি না?	H		
২.৯	ডেস্কটপ বা ল্যাপটপ কম্পিউটার ব্যবহারকারীগণ রাইট, কম্পাইল ও কপি পরিচালনা করার পূর্বে অবশ্যই সম্যক জ্ঞাত হতে হবে নতুবা কম্পিটার কোডের নকশা নষ্ট হতে পারে, এমন কি ওয়ার্ম, ট্রোজান ইত্যাদি ভাইরাস দ্বারা আক্রান্ত হয়ে কম্পিউটারের কার্যক্ষমতা হ্রাস পেতে পারে। এতদ বিষয়ে ব্যবস্থা গ্রহণ করা হয় কি না?	H		
২.১০	ভাইরাস দ্বারা আক্রান্ত হয়েছে নিশ্চিত হলে অতিসত্তর সংশ্লিষ্ট কর্তৃপক্ষকে অবহিত কর হয়া কি না?	H		
২.১১	অভিজ্ঞ ব্যক্তির সহায়তা ছাড়া ভাইরাস অপসারণ অথবা অনুসন্ধান করা হয় কি না?	H		
২.১২	ডেস্কটপ এবং ল্যাপটপ কম্পিউটার চালু এবং বন্ধের ক্ষেত্রে অনুমোদিত আইডি এবং পাসওয়ার্ড ব্যবহার করা হয়েছে কি না ?	M		
২.১৩	ব্যবহৃত ডেস্কটপ অথবা ল্যাপটপ কম্পিউটারে উন্নত মানের ভাইরাস ডিটেকশন সফটওয়্যার ইন্সটল করা হয়েছে কি না?	H		
২.১৪	ডেস্কটপ এবং ল্যাপটপ কম্পিউটারসমূহে আদর্শমানের ভাইরাস ডিটেকশন সফটওয়্যার কনফিগার নিয়মিতভাবে ব্যবহার করে বিভিন্ন ধরনের ডকুমেন্ট স্ক্যান করে ভাইরাসমুক্ত করা হয় কি না?	H		
২.১৫	ডেস্কটপ এবং ল্যাপটপ কম্পিউটারসমূহের কনফিগারেশন এমন ভাবে প্রস্তুত করা হয়েছে কি না যাতে নিরাপত্তা বিষয়ক যে কোনো সংকেত ধরতে পারে? (যেমন : পাসওয়ার্ড গেজিং, অননুমোদিতভাবে প্রবেশ চেষ্টা, এপ্লিকেশন অথবা সিস্টেমস সফটওয়্যার মডিফিকেশন)	H		
২.১৬	ব্যবহারিক কম্পিউটারসমূহ জানালা থেকে দূরে এবং মেঝে থেকে কিছু উপরে রাখা হয়েছে কি না?	M		
২.১৭	পাসওয়ার্ড প্রোটেকশন স্ক্রিন অন্তত: ০৫ মিনিট পর কার্যকর হবে এমন সময় নির্ধারণ করে সেটআপ করা আছে কি না?	L		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৩. বিওয়াইওডি (ব্রিং ইওর ওউন ডিভাইস) নিয়ন্ত্রন (BYOD (Bring Your Own Device) Controls)				
৩.১	বিওয়াইওডি এর সাথে সম্পৃক্ত নিরাপত্তা ঝুঁকি মোকাবেলায় পর্যাপ্ত ব্যবস্থা গ্রহণ নিশ্চিত করতে বিওয়াইওডি ব্যবহারের জন্য ব্যাপক ঝুঁকি মূল্যায়ন করা হয়েছে কি ?	M		
৩.২	প্রতিটি নির্দিষ্ট ডিভাইস এর জন্য তৈরি ডিজিটাল সার্টিফিকেটের মত পডস (POD) এর জন্য কর্তৃপক্ষ অনুমোদিত ডিভাইস অথেন্টিকেশনের যথাযথ ব্যবস্থা নেয়া হয়েছে কি না?	M		
৩.৩	পডস (PODs) এর মাধ্যমে নেটওয়ার্ক (যেমন : SSL বা VPN) এর মাধ্যমে প্রেরিত উপাত্ত এনক্রিপ্ট করা থাকে কি না ?	H		
৩.৪	কোনো কর্মকর্তা-কর্মচারির ডিভাইস হারিয়ে গেলে কিংবা কর্মকর্তা কর্মচারি চাকুরি ছেড়ে দিলে অথবা আইসিটি ডিপার্টমেন্ট কোনো উপাত্ত বা নীতিমালার লঙ্ঘন, ভাইরাস বা কর্পোরেশনের উপাত্ত ও প্রযুক্তি অবকাঠামোর জন্য হুমকি চিহ্নিত করলে উক্ত কর্মকর্তা কর্মচারির ডিভাইস দূর থেকে নিষ্ক্রিয় করে দেয়া হয় কি না?	H		
৪. সার্ভার নিরাপত্তা নিয়ন্ত্রণ (Server Security Controls)				
৪.১	ব্যবহারকারীরা সার্ভারে কী ধরনের কার্য সম্পাদন করবে তা নির্দিষ্ট করে দিয়ে তাদের সার্ভারে প্রবেশের সুনির্দিষ্ট অনুমোদন আছে কি না?	H		
৪.২	দূরবর্তী স্থান থেকে সার্ভার ব্যবহারকারীদের সার্ভারে প্রবেশ নিয়ন্ত্রনের জন্য অতিরিক্ত অনুমোদন দেয়ার ব্যবস্থা (mechanism) আছে কি না?	H		
৪.৩	একটি নির্দিষ্ট সময় পর্যন্ত কার্যক্রম না চললে নিষ্ক্রিয় সেশন বন্ধ হয়ে যায় কি না?	M		
৪.৪	সিস্টেমস এডমিনিস্ট্রেটরের কার্যক্রম লগ করা হয় কি না?	H		
৪.৫	নতুন কোনো সার্ভিস প্রয়োগ করার পূর্বে কনফিগারেশন সেটিংস নতুন প্যাচ ও সার্ভিস প্যাকস পরীক্ষার জন্য টেস্ট সার্ভার সংরক্ষণ করা হয় কি না?	H		
৪.৬	ফাইল শেয়ারিং পদ্ধতির নিরাপত্তা নিশ্চিত করা হয় কি না? (নিরাপত্তা ব্যবস্থা মজবুত করার লক্ষ্যে যে সমস্ত ফাইল এবং প্রিন্টিং শেয়ার করার প্রয়োজন নেই সেগুলো যথাসম্ভব কম সংখ্যক রাখা কিংবা নিষ্ক্রিয় করে রাখা উচিত)	M		
৪.৭	প্রডাকশন সার্ভারে কোনো অপ্রয়োজনীয় সার্ভিস চালু আছে কি না?	H		
৪.৮	ভার্চুয়ালাইজেশনের ক্ষেত্রে নিম্নোক্ত নিরাপত্তামূলক পদক্ষেপ অনুসরণ করা হয় কি না? ক. প্রত্যেক ভার্চুয়াল মেশিন এর মাধ্যমে সম্পদের (যেমন; প্রসেসর, মেমোরী, ডিস্ক স্পেস, ভার্চুয়াল নেটওয়ার্ক ইন্টারফেস) ব্যবহারের সীমা নির্ধারণ করা; খ. নতুন/ অপ্রয়োজনীয় নিরাপত্তা প্যাচ এবং প্রয়োজনে অন্যান্য প্যাচ এর মাধ্যমে হোস্ট ও গেস্ট অপারেটিং সিস্টেম (OS) হালনাগাদ করা ও ভার্চুয়ালাইজেশন সফটওয়্যারে প্রয়োজনীয় প্যাচ সংযোজন করা। গ. নিয়মিতভাবে ভার্চুয়াল সার্ভারের ব্যাকআপ গ্রহণ ঘ. হোস্ট ও গেস্টের ক্ষেত্রে সমকালীন ব্যবহার। ঙ. প্রয়োজন না হলে হোস্ট ও গেস্ট অপারেটিং সিস্টেম এর মধ্যে কোনো ফাইল শেয়ার না করা	H		
৪.৯	সার্ভার রুমে প্রবেশের ক্ষেত্রে ভিজিটরদের জন্য লগবুক সংরক্ষণ করা হয় কি না?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৪.১০	সার্ভারে পাসওয়ার্ড প্রোটেক্টেড স্ক্রিন এমনভাবে কি সেটআপ করা আছে যাতে ১ মিনিটের মধ্যে স্বয়ংক্রিয়ভাবে স্ক্রিণ বন্ধ হয়ে যায়।	M		
৫. ডাটা সেন্টার নিয়ন্ত্রন (Data Center Controls)				
৫.১ ভৌত নিরাপত্তা (Physical Security)				
৫.১.১	ডাটা সেন্টারে প্রবেশাধিকার সংরক্ষিত কি না এবং যথাযথ প্রবেশ অনুমোদন নীতি (Access Authorization Policy) মানা হয় কি না?	H		
৫.১.২	শুধু প্রয়োজন হলেই কর্মীদের ডাটা সেন্টারে প্রবেশ করতে দেয়া হয় কি না এবং প্রয়োজন না হলে তাতে ভৌত প্রবেশাধিকার তাৎক্ষনিক প্রত্যাহার করা হয় কি না?	H		
৫.১.৩	ডাটা সেন্টারে ভেন্ডর, সেবা প্রদানকারী, সাপোর্ট স্টাফ এবং পরিচ্ছন্ন কর্মীদের কাজের সময় একজন অনুমোদিত কর্মকর্তা/কর্মচারি সার্বক্ষনিকভাবে তাদের সাথে থাকেন কি না?	H		
৫.১.৪	ডাটা সেন্টারে প্রবেশ অনুমোদনের তালিকা আছে কি না এবং সময় সময় তা পর্যালোচনা করা হয় কি না?	H		
৫.১.৫	ডাটা সেন্টারে সমস্ত স্পর্শকাতর স্থানে স্বশরীরে প্রবেশ নিবন্ধন করা হয় কি হয় না?	H		
৫.১.৬	ডাটা সেন্টারে নিরাপত্তা রক্ষী, কার্ড একসেস সিস্টেম, ম্যানট্র্যাপস এবং নজরদারী ব্যবস্থার (যেখানে ডাটা প্রয়োজন) মত ২৪ ঘন্টা ফিজিক্যাল, মানুষ দ্বারা এবং পদ্ধতিগত নিয়ন্ত্রণ আরোপ করা হয় কি না?	H		
৫.১.৭	জরুরি বর্হির্গমনের জন্য দরজা আছে কি না?	H		
৫.১.৮	অনুমোদন প্রদান ও নীতিমালা পরিপালন নিশ্চিত করতে ডাটা সেন্টারে কোনো দায়িত্বপ্রাপ্ত তত্বাবধায়ক/ব্যবস্থাপক আছে কি না?	H		
৫.১.৯	ব্যবস্থাপক বা ক্ষমতাপ্রাপ্ত ব্যক্তি কর্তৃক ডাটা সেন্টারের সমস্ত কম্পিউটার যন্ত্রপাতি এবং তৎসংগে প্রয়োজনীয় অন্যান্য যন্ত্রপাতির ইনভেন্টরি করা হয় কি না?	M		
৫.১.১০	বৎসরে কমপক্ষে এক বার ডাটা সেন্টার ভবনের নিরাপত্তা ব্যবস্থা পর্যালোচনা করা হয় কি না?	H		
৫.২	**পারিপার্শ্বিক নিরাপত্তা (Environmental Security)**			
৫.২.১	ক্ষতির ঝুঁকি (অগ্নিকান্ড, বন্যা, বিস্ফোরণ বা অন্যান্য যে কোনো দুর্যোগ) থেকে ডাটা সেন্টার সুরক্ষিত কি না?	H		
৫.২.২	বিদ্যুৎ সরবরাহ ব্যবস্থা ও নেটওয়ার্ক সংযোগসহ ডাটা সেন্টারের নকশা যথাযথভাবে নথিভুক্ত করা হয়েছে কি না?	H		
৫.২.৩	উন্নয়ন ও পরীক্ষার পরিবেশ প্রডাকশন সাইট থেকে আলাদা করা হয়েছে কি না?	H		
৫.২.৪	ডাটা সেন্টারে পৃথকভাবে নেটওয়ার্ক এবং বৈদ্যুতিক ক্যাবল ব্যবহার করা হয়েছে কি না?	M		
৫.২.৫	ডাটা সেন্টারের মেঝের নীচে ওয়াটারলিক ডিটেকশন ডিভাইস স্থাপন করা হয়েছে কি না?	H		
৫.২.৬	ডাটা সেন্টারের সাথে সম্পৃক্ত নয় এমন যন্ত্রপাতি ডাটা সেন্টারে আছে কি না? সব ধরনের অপ্রয়োজনীয় যন্ত্রপাতি রাখার জন্য আলাদা স্টোর রুম আছে কি না?	M		
৫.২.৭	ডাটা সেন্টারের চতুর্দিকে যথাযথভাবে পর্যবেক্ষণ করার জন্য সিসিটিভি ক্যামেরা	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
	উপযুক্ত স্থানে সংস্থাপন করা হয়েছে কি না?			
৫.২.৮	ডাটা সেন্টারের "নো ইটিং, ড্রিকিং অর স্কোমিং" সম্বলিত কোনো চিহ্ন দৃশ্যমান রাখা হয়েছে কি না?	L		
৫.২.৯	জরুরি প্রয়োজনে ব্যবহারের জন্য সার্বক্ষনিকভাবে কোন যানবাহনের সুবিধা আছে কি না?	H		
৫.২.১০	ডাটা সেন্টারে যোগাযোগের জন্য কোনো নির্দিষ্ট টেলিফোন যোগাযোগ ব্যবস্থা আছে কি না?	M		
৫.২.১১	জরুরি প্রয়োজনে বিভিন্ন ব্যক্তি বা প্রতিষ্ঠানের যেমন অগ্নি নির্বাপন, পুলিশ স্টেশন, সেবাপ্রদানকারী প্রতিষ্ঠান, ভেন্ডর ও আইসিটি বিষয়ক ব্যক্তির ঠিকানাসহ মোবাইল অথবা টেলিফোন নম্বর সংরক্ষন করা হয়েছে কি না?	H		
৫.২.১২	পরিবেশগত ঝুঁকি হ্রাসে বিদ্যুৎ সরবরাহ ব্যবস্থা এবং অন্যান্য সহযোগী ইউনিট প্রডাকশন সাইট থেকে আলাদা রেখে কোনো নিরাপদ এলাকায় স্থাপন করা হয়েছে কি না?	H		
৫.২.১৩	প্রধান উৎস বা জেনারেটর থেকে নির্ধারিত বিদ্যুৎ সরবরাহ ব্যবস্থা ডাটা সেন্টারে বিদ্যমান রয়েছে কি না?	H		
৫.২.১৪	ব্যাকআপ ইউনিটসহ ইউপিএস এর পর্যাপ্ত ব্যবস্থা বিদ্যমান আছে কি না?	H		
৫.২.১৫	ব্যাকআপ বিদ্যুৎ সরবরাহের ব্যবস্থা আছে কি না?	H		
৫.২.১৬	তাপমাত্রা এবং আদ্রতা পরিমাপক কোনো যন্ত্র সংস্থাপন করা আছে কি না?	M		
৫.২.১৭	ব্যাকআপ ইউনিট এর মানসম্মত শীতাতপ নিয়ন্ত্রণ ব্যবস্থা আছে কি না?	M		
৫.২.১৮	শীতাতপ নিয়ন্ত্রণ যন্ত্রের সাথে পনি চুঁয়ানোর সতর্কতা/সনাক্তকরণ ও পানি প্রবাহ ব্যবস্থা আছে কি না?	H		
৫.২.১৯	(প্রয়োজনের সময়) জরুরি আলোর ব্যবস্থা বিদ্যমান আছে কি না?	M		
৫.২.২০	আদ্রতা নিয়ন্ত্রণের জন্য কোনো ডিহিউমিডিফায়ার বিদ্যমান আছে কি না?	M		
৫.২.২১	সংশ্লিষ্ট কর্মকর্তা/কর্মচারি যথাযথ প্রশিক্ষণ ও শিক্ষা পাচ্ছে কিনা? এবং তাদের কাজের সাথে সম্পর্কিত আইসিটি নিরাপত্তা কর্মকান্ড বিষয়ে সচেতনতা বাড়ছে কি না?	M		
৫.২.২২	ইঁদুর/বিভিন্ন পোকামাকর থেকে কম্পিউটার যন্ত্রপাতি সুরক্ষার জন্য র‍্যাট/ রোডেন্ট রিপিলেন্ট ব্যবহার করা হয় কি না?	M		
৫.২.২৩	ডাটা সেন্টারের বিদ্যুৎ নিয়ন্ত্রণ কক্ষে গতিবিধি পর্যবেক্ষণ করার যন্ত্র স্থাপন করা আছে কি না?	H		
৫.৩ অগ্নি নিবারণ (Fire Prevention)				
৫.৩.১	ডাটা সেন্টারের দেয়াল, ছাদ ও দরজাসমূহ অগ্নি নিরোধক কি না?	H		
৫.৩.২	ডাটা সেন্টারে অগ্নিনির্বাপক যন্ত্র স্থাপন করা আছে কি না এবং তা সময় সময় পরীক্ষা করা হয় কি না?	H		
৫.৩.৩	আগুন/ধোঁয়া সনাক্তকারী যন্ত্র স্থাপন করা হয়েছে কি না এবং সময় সময় পরীক্ষা করা হয় কি না?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৫.৩.৪	রেইজড ফ্লোর এর নিচে আগুন এবং পানি সনাক্তকরণ যন্ত্র স্থাপন করা আছে কি না (ফ্লোর রেইজ করা থাকলে)	M		
৫.৩.৫	ডাটা সেন্টারে ব্যবহৃত বৈদ্যুতিক এবং ডাটা ক্যাবল মান সম্মত কি না এবং গুপ্ত রাখা হয়েছে কি না?	H		
৫.৩.৬	ডাটা সেন্টারে দাহ্য পদার্থ (যেমন : কাগজ, কাঠের আসবাবপত্র, প্লাস্টিক জাতীয় দ্রব্য) রাখা নিয়ন্ত্রিত কি না?	H		
৫.৪ সার্ভার/ নেটওয়ার্ক রুম/ র‍্যাক নিয়ন্ত্রণ (Server/Network Room/Rack Controls)				
৫.৪.১	সার্ভার/ নেটওয়ার্ক রুম/ র‍্যাক একজন দায়িত্বপ্রাপ্ত ব্যক্তির তত্ত্বাবধানে কাঁচ ঘেরা কক্ষে তালাবদ্ধ আছে কি না?	H		
৫.৪.২	সার্ভার রুমে শারীরিক প্রবেশ নিয়ন্ত্রিত কি না?	H		
৫.৪.৩	সার্ভার রুমে ভিজিটরস লগ সংরক্ষণ করা হয় কি না?	M		
৫.৪.৪	(সার্ভার রুমের জন্য) প্রবেশের জন্য অনুমোদিত তালিকা সংরক্ষণ ও নিয়মিত পর্যালোচনা করা হয় কি না?	M		
৫.৪.৫	কোনো বিপর্যয় ঘটলে সম্ভাব্য স্বল্পতম সময়ে সার্ভার ও নেটওয়ার্ক যন্ত্রপতি প্রতিস্থাপনের ব্যবস্থা আছে কি না?	H		
৫.৪.৬	সার্ভার / নেটওয়ার্ক রুম/ র‍্যাক শীতাতপ নিয়ন্ত্রিত কি না?	M		
৫.৪.৭	সার্ভার/নেটওয়ার্ক রুম/ র‍্যাক এ স্থাপিত শীতাতপ নিয়ন্ত্রণ যন্ত্রের সাথে পানি চুঁয়ানোর সতর্কতা ও পানি প্রবাহ ব্যবস্থা আছে কি না?	H		
৫.৪.৮	বিদ্যুৎ বিভ্রাট ঘটলে কার্যক্রম অব্যাহত রাখতে জেনারেটর স্থাপন করা হয়েছে কি না?	H		
৫.৪.৯	সার্ভার ও প্রয়োজনীয় যন্ত্রপাতিতে নিরবিচ্ছিন্ন বিদ্যুৎ সরবরাহ করতে এগুলোর সাথে ইউপিএস সংযুক্ত করা হয়েছে কি না?	M		
৫.৪.১০	পরিচ্ছন্ন ও নিরাপদভাবে প্রয়োজনীয় ক্যাবল স্থাপনের জন্য বিদ্যুৎ সরবরাহ ও ডাটা ক্যাবলের নকশা অনুযায়ী ভবনের দেয়ালে চ্যানেল প্রস্তুত করা হয়েছে কি না?	M		
৫.৪.১১	জরুরি পরিস্থিত মোকাবেলায় বিভিন্ন ব্যক্তি বা প্রতিষ্ঠানের (যেমন : অগ্নি নির্বাপন, পুলিশ স্টেশন, সেবাপ্রদানকারী প্রতিষ্ঠান, ভেন্ডর, আইসিটি বিষয়ক ব্যক্তি) ঠিকানা ও ফোন নম্বর আছে কি না?	H		
৫.৪.১২	প্রয়োজনে সার্ভার কক্ষ থেকে বের হওয়ার সময় বিদ্যুৎ বন্ধ করার জন্য চাবির ব্যবস্থা আছে কি না?	M		
৫.৪.১৩	সার্ভার রুমের দরজার বাইরে দৃশ্যমান স্থানে অগ্নি নির্বাপক যন্ত্র স্থাপন করা হয়েছে কি না?	H		
৫.৪.১৪	বৎসরান্তে অগ্নিনির্বাপক যন্ত্রের কার্যকারিতা পরীক্ষা করা হয় কি না?	M		
৫.৫ নেটওয়ার্ক নিরাপত্তা ব্যবস্থাপনা (Networks Security Management)				
৫.৫.১	প্রতিষ্ঠানের নীতি অনুসারে অপারেটিং সিস্টেম, ডাটাবেজ, নেটওয়ার্ক ইকুইপমেন্টস এবং পোর্টেবল ডিভাইসেস এর নিরাপত্তা নিশ্চিত করার জন্য কোন বেজলাইন স্ট্যান্ডার্ড প্রতিষ্ঠা করা হয়েছে কি না?	H		
৫.৫.২	নেটওয়ার্ক ডিজাইন এবং সিকিউরিটি কনফিগারেশন বিষয়ে কোনো দালিলিক নকশা আছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৫.৫.৩	পরবর্তী সময়ে সংশোধন ও পরিবর্তন করার সুবিধা রেখে সমস্ত ক্যাবল, ইউটিপি, ফাইবার বিদ্যুৎসহ সমস্ত ক্যাবল লেবেলযুক্ত করা হয়েছে কি না?	H		
৫.৫.৪	নেটওয়ার্ক সামগ্রির ফিজিক্যাল সিকিউরিটি নিশ্চিত করা হয়েছে কি না	H		
৫.৫.৫	নেটওয়ার্ক যেমন VLAN এ তথ্য সেবা, ব্যবহারকারী এবং তথ্য ব্যবস্থা পদ্ধতির গ্রুপ পৃথক করা আছে কি না?	H		
৫.৫.৬	একক বা গণ নেটওয়ার্কের এর মধ্য দিয়ে প্রেরিত স্পর্শকাতর উপাত্ত এনক্রিপ্ট এবং ডিক্রিপ্ট করার ব্যবস্থা আছে কি না?	M		
৫.৫.৭	নেটওয়ার্ক নিরাপত্তার জন্য ফায়ারওয়্যাল এবং ইনট্রুশন প্রিভেনশন সিস্টেম ও ইনট্রুশন ডিটেকশন সিস্টেম এর মত কোনো যন্ত্র স্থাপন করা হয়েছে কি না?	H		
৫.৫.৮	রিমোট এডমিনিস্ট্রেশন এর জন্য নেটওয়ার্ক ডিভাইসে নিরাপদ লগইন ফিচার (যথা:SSH) কার্যকর করা হয়েছে কি না?	M		
৫.৫.৯	নেটওয়ার্ক ডিভাইসে আনএনক্রিপ্টেড লগইন ব্যবস্থা (যথা : TELNET) অকার্যকর করা হয়েছে কি না?	H		
৫.৫.১০	নেটওয়ার্ক সিকিউরিটি ডিভাইস এর নিয়মাবলী নিয়মিতভাবে হালনাগাদ ও পর্যালোচনা করা হয় কি না?	H		
৫.৫.১১	একক কানেক্টিভিটির জন্য কোন বিকল্প সংযোগ বিদ্যমান আছে কি না?	H		
৫.৫.১২	নেটওয়ার্ক ডিভাইস সৃষ্ট লগ পর্যবেক্ষণ করার জন্য কোন সিসলগ সার্ভার প্রতিষ্ঠা করা আছে কি না?	M		
৫.৫.১৩	নেটওয়ার্ক ট্রাফিক নিয়ন্ত্রণে রাউটার ও রোল-বেজড এবং/অথবা সময়ানুগ প্রবেশ নিয়ন্ত্রণ তালিকা (ACLs) বাস্তবায়ন করা আছে কি না?	H		
৫.৫.১৪	সব নেটওয়ার্ক সরঞ্জাম ও সার্ভারে নজরদারীর জন্য অবকাঠামো ব্যবস্থাপনায় তাৎক্ষনিক হেলথ মনিটরিং ব্যবস্থা আছে কি না?	M		
৫.৫.১৫	অফিসের নেটওয়ার্কে ব্যক্তিগত ল্যাপটপ অথবা অফিসের ল্যাপটপ/ডেস্কটপ এ ব্যক্তিগত ওয়ারল্যাস মডেম সংযোগ দেয়া নিয়ন্ত্রিত কি না?	M		
৫.৫.১৬	নেটওয়ার্ক এর ডিফল্ট পাসওয়ার্ড পরিবর্তন করা হয় কি না?	M		
৫.৫.১৭	একসেস সুইচের সব অব্যবহৃত পোর্ট বন্ধ রাখা হয়েছে কি না?	M		
৫.৫.১৮	যথাযথ কর্তৃপক্ষের অনুমোদনক্রমে সমস্ত যোগাযোগের মাধ্যম নির্দিষ্ট করা হয়েছে কি না?	H		
৫.৫.১৯	সার্ভারের জন্য রোল-বেজড এডমিনিস্ট্রেশন নিশ্চিত করা হয়েছে কি না?	H		
৫.৬ মেলিসিয়াস কোড প্রোটেকশন (Malicious Code Protectio)				
৫.৬.১	মেলিসাস কোড প্রতিরোধ করার জন্য সার্ভার এবং ওয়ার্কস্টেশনগুলোতে যথাযথ অনুমোদিত এন্টিভাইরাস প্যাকেজ ব্যবহার করা হয় কি না?	H		
৫.৬.২	মেলিসিয়াস কোড অনুসন্ধানের জন্য নিয়মিতভাবে স্ক্যানকার্য সম্পাদন করে সফটওয়্যার এবং তথ্যসমূহ জটিল অবস্থা থেকে মুক্ত রাখা হয় কি না?	H		
৫.৬.৩	কোন অপরিচিত উৎস বা নেটওয়ার্ক থেকে প্রাপ্ত ফাইলসমূহ মেলিসাস কোড চেক করা ছাড়া ব্যবহার করা হয় কি না?	H		
৫.৬.৪	ইলেকট্রনিক মেইলসমূহ চেক না করে সংযুক্ত ফাইল ওপেন করা হয় কি না?	H		
৫.৬.৫	ইলেকট্রনিক মেইলে সংযুক্তির পূর্বে ক্ষতিকর কোড চেক করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৫.৬.৬	এন্টি ভাইরাস প্যাকেজ স্বয়ংক্রিয় এবং তাৎক্ষনিক/সময়ানুগ প্রক্রিয়া ব্যবহার করে সর্বশেষ ভাইরাস ডেফিনেশন ফাইল হাল নাগাদ করে রাখা হয় কি না?	H		
৫.৬.৭	নেটওয়ার্কের কম্পিউটারসমূহে (সার্ভার থেকে) এন্টি ভাইরাস সফটওয়্যার স্বয়ংক্রিয়ভাবে হাল নাগাদ করা হয় কি না?	M		
৫.৬.৮	ভাইরাস স্বয়ংক্রিয় সুরক্ষা মোড এ স্ক্রিন ডিস্ক, টেপ, সিডি অথবা ভাইরাসের জন্য অন্যান্য মিডিয়া সক্রিয় করে রাখা হয় কি না?	M		
৫.৬.৯	ভূয়া ভাইরাস সমস্যা সম্পর্কে কর্মকর্তাদের সচেতন করা হয় কি না যাতে এরা সতর্কতা জারি না করে?	H		
৫.৬.১০	ব্যবহারকারীদের জন্য কম্পিউটার ভাইরাস সচেতনতা এবং প্রতিরোধ সম্পর্কে কোন কর্মসূচির আয়োজন করা হয় কি না?	H		
৫.৭ ইন্টারনেটে প্রবেশাধিকার ব্যবস্থাপনা (Internet Access Management)				
৫.৭.১	ইন্টারনেটে প্রবেশের অনুমতি প্রাপ্ত কর্মকর্তা-কর্মচারিদের এতদসম্পর্কিত ব্যবস্থাপনা নীতিমালা সম্পর্কে অবহিত করা হয়েছে কি না?	M		
৫.৭.২	কর্পোরেশন প্রাঙ্গন/স্থাপনা এবং সিস্টেম থেকে ইন্টারনেট ব্যবহার নিরাপদ গেটওয়ের মাধ্যমে হয় কি না?	H		
৫.৭.৩	তথ্য নিরাপত্তা কর্তৃপক্ষের অনুমতি ব্যাতিরেকে কর্পোরেশন প্রাঙ্গন/স্থাপনা অথবা সিস্টেম এ স্থানীয়ভাবে সরাসরি (স্বতন্ত্র পিসি এবং ল্যাপটপসহ) ইন্টারনেটে সংযোগ নিষিদ্ধ করা হয়েছে কি না?	H		
৫.৭.৪	কর্মকর্তা-কর্মচারিদের কর্পোরেশনের সিস্টেম ব্যবহার করে ইন্টারনেট থেকে নিজেদের সংযোগ স্থাপনের বিষয়টি নিষিদ্ধ করা হয়েছে কি না?	H		
৫.৭.৫	বিশেষ অনুমোদন ছাড়া কর্পোরেশনের সিস্টেমের সাথে স্থানীয়ভাবে মডেম ব্যবহার করে ইন্টারনেট সংযোগ বা কোনো তৃতীয় পক্ষের বা ব্রডব্যান্ড, আই.এস.ডিএন. বা পিএসটিএন পরিসেবাগুলির মাধ্যমে পাবলিক নেটওয়ার্কের সঙ্গে সংযোগ স্থাপন নিষিদ্ধ করা হয়েছে কি না?	H		
৫.৭.৬	কর্পোরেশন প্রদত্ত ইন্টারনেট এক্সেস কোনো বাণিজ্যিক /ব্যবসায়িক লেনদেন করার জন্য (কর্মী বা অন্য ব্যক্তিদেরকে ব্যক্তিগত ব্যবসায়িক স্বার্থে) ব্যবহার করা হয় কি না?	H		
৫.৭.৭	কর্পোরেশন প্রদত্ত ইন্টারনেট সংযোগ ব্যবহার করে জ্ঞাতসারে কেউ কোনো ফৌজদারি বা দেওয়ানি আইন বিরোধি কর্মকান্ডের সাথে জড়িত কি না?	H		
৫.৭.৮	ইন্টারনেট বা থার্ড পার্টি ও গণ নেটওয়ার্ক এ সংযোগ নিতে হয় এমন সব এপ্লিকেশন ও সিস্টেম উন্নয়ন/উৎপাদন কাজে ব্যবহারের আগে (Before Production Use) আনুষ্ঠানিকভাবে ঝুঁকি বিশ্লেষণ ও প্রয়োজনীয় নিরাপত্তা ব্যবস্থা করা হয় কি না?	H		
৫.৮ ই-মেইল ব্যবস্থাপনা (Email Management)				
৫.৮.১	কর্পোরেশনের নীতিমালা অনুযায়ী ই-মেইল সিস্টেম ব্যবহার করা হয় কি না?	H		
৫.৮.২	অফিসিয়ালভাবে অনুরোধের মাধ্যমে ই-মেইল সিস্টেমের ব্যবহার করা হয় কি না?	M		
৫.৮.৩	ই-মেইল এ এনক্রিপশন ছাড়া স্বতন্ত্র গোপনীয় তথ্য বহিরাগত দলের সাথে যোগযোগ করতে ব্যবহার করা হয় কি না?	H		
৫.৮.৪	কর্মকর্তাগণ ই-মেইল ফরওয়ার্ডিং অথবা বহিরাগত দলের উত্তর দেওয়ার আগে গোপনীয়তাসহ ই-মেইলের বিষয়বস্তুর সংবেদনশীলতা বিবেচনা করেন কি না?	M		
৫.৮.৫	ই-মেইল দ্বারা এমন তথ্য প্রেরণ করা হয় কি না যা মানহানিকর, অবমাননাকর, বর্নবাদী বা যৌন নির্যাতন সম্পর্কিত কর্পোরেশনের খ্যাতি নষ্ট করে বা এমন কোনো সামগ্রী যা	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
	কর্পোরেশনের কর্মী, গ্রাহক, প্রতিদ্বন্দী বা অন্যদের জন্য ক্ষতিকর?			
৫.৮.৬	কর্মকর্তা-কর্মচারিগণ কর্পোরেশনের ই-মেইল সিস্টেম ব্যক্তিগত উদ্দেশ্যে ব্যবহার করে কি না? (ব্যবস্থাপনা কর্তৃপক্ষের অনুমোদন ছাড়া)	H		
৫.৮.৭	কর্তৃপক্ষের অনুমোদন ছাড়া কর্পোরেট ই-মেইল ঠিকানা কোনো সামাজিক নেটওয়ার্ক, ব্লগ গ্রপ, ফোরাম ইত্যাদিতে ব্যবহার করা হয় কি না?	H		
৫.৮.৮	কর্পোরেশন থেকে ই-মেইল সম্প্রচারে একটি দাবিত্যাগ আছে কি না যা ই-মেইলের বিষয়বস্তুর গোপনীয়তা সম্পর্কে উল্লেখপূর্বক প্রাপককে জিজ্ঞাসা করা যায়?	M		
৫.৮.৯	সংশ্লিষ্ট ডিপার্টমেন্ট নিয়মিত ই-মেইল সার্ভিস পর্যালোচনা ও পর্যবেক্ষণ করে কি না?	H		

৫.৯ আক্রম্যতা নিরুপণ এবং অনুপ্রবেশ পরীক্ষা (Vulnerability Assessment and Penetration Testing)				
৫.৯.১	আইসিটি পরিবেশ নিরাপত্তা আক্রম্যতা/বিপদসংকুলতা সনাক্ত করতে নিয়মিত আক্রম্যতা (Vulnerability assessments) নিরুপণ করা হয় কি না?	H		
৫.৯.২	ব্যাপকভাবে আক্রম্যতা নিরুপণ (Vulnerability assessments) করতে হলে সমন্বিতভাবে স্বয়ংক্রিয় সরঞ্জাম ও ম্যানুয়াল কৌশল প্রয়োগ করা হয় কি না?	H		
৫.৯.৩	ওয়েব ভিত্তিক সিস্টেমের আক্রম্যতা নিরুপণ(Vulnerability assessments) এ এসকিউএল ইনজেকশন, ক্রস-সাইট স্ক্রিপ্টিং ইত্যাদির মত সাধারণ ওয়েব ভিত্তিক দুর্বলতা অন্তর্ভুক্ত থাকে কি না?	M		
৫.৯.৪	আক্রম্যতা নিরুপণ (Vulnerability assessments) এ চিহ্নিত সমস্যা সমাধানে কোনো প্রক্রিয়া গ্রহণ করা হয়েছে কি না এবং ঐ দুর্বলতা সম্পূর্ণরূপে দূর করার বিষয়টি নিশ্চিত করতে কৃত সমাধানের সঠিকতা নিশ্চিত করা হয় কি না?	H		
৫.৯.৫	সিস্টেমের নিরাপত্তার অবস্থা গভীরভাবে পর্যালোচনার জন্য নির্দিষ্ট সময় পর পর অথবা প্রয়োজনের ভিত্তিতে প্রকৃত আক্রমণের স্বরূপ উদঘাটনে ছদ্মরূপ ধারণের প্রবেশ পরীক্ষা পরিচালনা করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
৫.১০ প্যাচ ব্যবস্থাপনা (Patch Management)				
৫.১০.১	নিরাপত্তা প্যাচ সনাক্তকরণ, শ্রেণিবদ্ধকরণ এবং এর অগ্রাধিকার নির্ধারণসহ প্যাচ ব্যবস্থাপনা পদ্ধতি প্রতিষ্ঠা এবং নিশ্চিত করা হয়েছে কি না?	H		
৫.১০.২	সময়ের ভিত্তিতে নিরাপত্তা প্যাচ বাস্তবায়নে প্রত্যেক শ্রেণির নিরাপত্তা প্যাচ এর জন্য বাস্তবায়নের সময়সীমা নির্ধারণ করা হয়েছে কি না?	H		
৫.১০.৩	উৎপাদন পরিবেশ স্থাপনের পূর্বে নিরাপত্তা প্যাচ কঠোরভাবে পরীক্ষা করা হয় কি না?	H		
৫.১১ নিরাপত্তা পর্যবেক্ষণ (Security Monitoring)				
৫.১১.১	অভ্যন্তরীণ ও বহিস্থঃ পক্ষ সম্পাদিত অননুমোদিত বা ক্ষতিকারক কার্যক্রম সনাক্তকরণে যথাযথ নিরাপত্তা পর্যবেক্ষণ ব্যবস্থা ও প্রক্রিয়া প্রতিষ্ঠা করা হয়েছে কি না?	H		
৫.১১.২	নেটওয়ার্ক অনাহত প্রবেশ/হামলা থেকে রক্ষা এবং অনাহূত প্রবেশ ঘটার সময় সতর্ক বার্তা দেয়ার জন্য আইপিএস/আইডিএস এর মত নেটওয়ার্ক নিরাপত্তা যন্ত্র ব্যবহার করে নেটওয়ার্ক নজরদারি এবং নিরাপত্তা পর্যবেক্ষণ পদ্ধতি বাস্তবায়ন করা হয়েছে কি না?	H		
৫.১১.৩	ডাটাবেজ, সিস্টেম বা ডাটা ফাইল ও প্রোগ্রাম এর মত গুরুত্বপূর্ণ আইসিটি রিসোর্সেস এ অননুমোদিত পরিবর্তন চিহ্নিতকরণে সহায়তা করতে নিরাপত্তা তদারকি টুলস সংযোজন করা হয়েছে কি না?	H		
৫.১১.৪	সিস্টেম, এপ্লিকেশন এবং নেটওয়ার্ক ডিভাইস এর ব্যতিক্রম সমূহের নিরাপত্তা লগ নিয়মিত পর্যালোচনা করা হয় কি না?	H		
৫.১১.৫	ভবিষ্যত তদন্ত কাজে সহায়তার জন্য এসব নিরাপত্তা লগ একটি নির্দিষ্ট সময় পর্যন্ত সুরক্ষিতভাবে সংরক্ষণ করা হয় কি না?	H		

গ. তথ্য ব্যবস্থাপনা/পদ্ধতির প্রবেশাধিকার নিয়ন্ত্রণ (Access Control of Information System)

১. ব্যবহারকারীর প্রবেশাধিকার ব্যবস্থাপনা (User Access Management)				
১.১	আইসিটি সিস্টেম এবং নেটওয়ার্কে ব্যবহারকারীদের Need-to-use Basis-এ এবং প্রয়োজনের সময়ে প্রবেশাধিকার দেওয়া হয় কি না?	M		
১.২	প্রবেশাধিকার সংরক্ষণের জন্য অত্র প্রতিষ্ঠানের কর্মকর্তা/কর্মচারি নয় এমন ব্যক্তিদের (চুক্তিভিত্তি, আউটসোর্সড বা ভেন্ডর প্রতিনিধি) নিবিড়ভাবে পর্যবেক্ষণ করা হয় কি না?	H		
১.৩	প্রত্যেক ব্যবহারকারীর স্বতন্ত্র ব্যবহারকারী পরিচিতি (ID) এবং বৈধ পাসওয়ার্ড আছে কি না?	M		
১.৪	প্রবেশ সুবিধাসহ ব্যবহারকারীর ব্যবহারকারী পরিচিতি (ID) রক্ষণাবেক্ষণ ফরম যথাযথ কর্তৃপক্ষ কর্তৃক নিয়মানুগভাবে অনুমোদন করা হয়েছে কি না?	M		
১.৫	পরপর তিনবার লগইন করতে ব্যর্থ হলে ব্যবহারকারীর প্রবেশ বন্ধ হয় কি না?	M		
১.৬	চাকুরির ধরন পরিবর্তন হলে ব্যবহারকারীর প্রবেশ সুবিধা হালনাগাদ করা হয় কি না?	M		
১.৭	পরিদর্শন ও যাচাই বাছাই এর উদ্দেশ্যে ব্যবহারকারীদের প্রবেশাধিকার রেকর্ড অনন্যভাবে সনাক্তকৃত এবং লগকৃত কি না?	H		
১.৮	ব্যবহারকারীদের প্রবেশাধিকার সঠিকভাবে কাজ করছে কি না তা নিয়মিত পর্যবেক্ষণ/যাচাই করা হয় কি না?	M		
১.৯	ব্যবহারকারী সংযুক্ত/মুছে ফেলা/স্থগিত/হালনাগাদ করার ক্ষেত্রে ইউজার ম্যানেজমেন্ট ফর্ম ব্যবহার করা হয় কি না?	M		
১.১০	ইউজার ম্যানেজমেন্ট ফর্মে শুরু/শেষ তারিখ/সময়, সুবিধা ইত্যাদি প্রয়োজনীয় তথ্য আছে কি না?	M		
১.১১	নিরীক্ষা ও পর্যালোচনার জন্য ফর্ম বাস্তবায়ন ও সংরক্ষণের পূর্বে যথাযথ কর্তৃপক্ষ কর্তৃক অনুমোদিত হয়েছে কি না?	M		
১.১২	ব্যবহারকারী তাদের লগইন তথ্য (User ID, Password) গোপন রাখে কিনা এবং অন্যদের সাথে শেয়ার করে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)
২. পাসওয়ার্ড ব্যবস্থাপনা (Password Management)				
২.১	প্রথম লগইন-এ পাসওয়ার্ড পরিবর্তনের বাধ্যবাধকতা পাসওয়ার্ড কন্ট্রোল-এ অর্ন্তভুক্ত আছে কি না?	M		
২.২	সর্বনিম্ন (১০ অক্ষর) পাসওয়ার্ড ডেফিনেশন নিশ্চিত করে কি না?	M		
২.৩	পাসওয়ার্ড এবং এর মধ্যে ন্যূনতম তিনটি নির্ণায়ক (আপারকেস, লোয়ারকেস, নম্বর ও স্পেশাল ক্যারেক্টার) কে সম্বলিত করে কি না যা সিস্টেম নিশ্চিত করে?	H		
২.৪	পাসওয়ার্ড এর মেয়াদ স্বয়ংক্রিয়ভাবে ৯০দিন পর শেষ হয় কি না?	H		
২.৫	একই পাসওয়ার্ড কমপক্ষে তিনবার ব্যবহারের পর তা আবার ব্যবহারের বিষয়টি পাসওয়ার্ড হিস্টোরী সিস্টেম-এ এনাবল করা আছে কি না?	H		
২.৬	অপারেটিং সিস্টেম, ডাটাবেইজ এবং বিজিনেস এ্যাপ্লিকেশন এর প্রশাসনিক পাসওয়ার্ড সিলগালা করে নিরাপদ হেফাজতে রাখা হয় কি না?	H		
২.৭	ব্যবহারকারীরা যে কোনো এ্যাপ্লিকেশন-এর স্মৃতিসহায়ক পাসওয়ার্ড ফিচার পরিহার করে কি না?	H		
২.৮	সকল প্রশাসনিক পাসওয়ার্ড দুইমাস পর অথবা বড় ধরনের রক্ষণাবেক্ষণ কাজ করার পর পরিবর্তন করা হয় কি না?	H		
২.৯	কম্পিউটার-এর টেক্সট ফাইলে এনক্রিপশন ব্যতিত পাসওয়ার্ড সংরক্ষণ করা হয় কি না?	H		
২.১০	পাসওয়ার্ড কাগজে লিখে রাখা হয় কি না?	H		
৩. ইনপুট নিয়ন্ত্রণ (Input Control)				
৩.১	প্রত্যেক সিস্টেম এর জন্য ব্যবহারকারীদের সেশন টাইম-আউট ০৫ মিনিট সেট করা আছে কি না?	M		
৩.২	এ্যাপ্লিকেশন সফটওয়্যার-এ ব্যবহারকারীদের অপারেটিং টাইম শিডিউল ইনপুট বাস্তবায়ন করা হয় কি না?	M		
৩.৩	তথ্য সন্নিবেশ, অপসারণ এবং পরিবর্তনের ক্ষেত্রে ইউজার আইডি ও ডেট টাইম অডিট ট্রায়েল রিপোর্ট-এ পাওয়া যায় কি না?	H		
৩.৪	একই লেনদেনে একই ইউজার মেকার এবং চেকার হিসাবে উভয়ক্ষেত্রে কাজ করাকে সফটওয়্যার অনুমোদন করে কি না?	H		
৩.৫	কর্তৃত্ব হস্তান্তরের জন্য ব্যবস্থাপনা কর্তৃপক্ষের অনুমোদন নেয়া হয়েছে কি না?	H		
৩.৬	এ্যাপ্লিকেশন-এর স্পর্শকাতর তথ্য এবং ক্ষেত্রসমূহে প্রবেশাধিকার সংরক্ষিত কি না?	H		
৪. প্রিভিলেইজ একসেস ব্যবস্থাপনা (Privileged Access Management)				
৪.১	সুবিধাভোগী ব্যবহারকরীদের জন্য নিম্ন বর্ণিত নিয়ন্ত্রণ ও নিরাপত্তা ব্যবস্থা গ্রহণ করা হয়েছে কি না? ক) শক্তিশালী কর্তৃত্ব-প্রক্রিয়া বাস্তবায়ন; খ) দূরবর্তী স্থান থেকে প্রবেশের জন্য শক্তিশালী নিয়ন্ত্রণ বাস্তবায়ন; গ) সুবিধাভোগী ব্যবহারকারীদের সংখ্যা নিয়ন্ত্রণ; ঘ) "Need-to-have" ভিত্তিতে সুবিধাজনক প্রবেশ অনুমোদন; ঙ) সুবিধাভোগী ব্যবহারকারীদের কার্যক্রম নির্দিষ্ট সময়ান্তে পর্যালোচনা; চ) সুবিধাজনক হিসাবসমূহের ভাগাভাগি নিষিদ্ধকরণ; ছ) নিবিড় পর্যবেক্ষণ ও তদারকি ব্যতিত ভেন্ডরদের সুবিধাজনক প্রবিশাধিকার নিষিদ্ধকরণ;	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes)	না (No)

ঘ. অব্যাহত ব্যবসা এবং দুর্যোগে পুনরুদ্ধার ব্যবস্থাপনা (Business Continuity and Disaster Recovery Management)

১.১ অব্যাহত ব্যবসা পরিকল্পনা (Business Continuity Plan (BCP)				
১.১.১	দুর্যোগ থেকে পুনরুদ্ধারের জন্য অনুমোদিত Business Continuity Plan এর পরিকল্পনা আছে কি না?	H		
১.১.২	সকল সুবিধাভোগীর মধ্যে অনুমোদিত Business Continuity Plan এর পরিকল্পনা প্রচার করা হয়েছে কি না?	M		
১.১.৩	Business Continuity Plan এর পরিকল্পনা সংক্রান্ত দলিলাদি নিরাপদ অফ-সাইট লোকেশন-এ এবং তাৎক্ষণিক রেফারেন্স-এর জন্য অফিসে রাখা আছে কি না?	H		
১.১.৪	সিস্টেমের চাহিদা, প্রক্রিয়া ও পারস্পরিক নির্ভরশীলতা বিবেচনা করে ব্যবসার গুরুত্ব বিশ্লেষণ এবং দুর্যোগ পুন:ভরন পরিকল্পনা-এর সমন্বয়ে এবং সমর্থনে অব্যাহত Business Continuity Plan পরিকল্পনা করা হয়েছে কি না?	H		
১.১.৫	নিম্নে বর্ণিত অবস্থায় Business Continuity Plan পরিচালনা নির্ধারিত সময়ের মধ্যে পুনরুদ্ধার করার জন্য BCP তে কোনো কর্মপরিকল্পনা উল্লেখ করা আছে কি না? ক. অফিস চলাকালে সংঘটিত দুর্যোগ খ. অফিস সময়ের বাইরে সংঘটিত দুর্যোগ।	H		
১.১.৬	কর্মকর্তা-কর্মচারী, ভেন্ডর ও প্রয়োজনীয় এজেন্সিসমূহের জরুরি যোগাযোগ ব্যবস্থা, ঠিকানা এবং ফোন নম্বর ব্যবসা পরিকল্পনায় উল্লেখ করা আছে কি না?	H		
১.১.৭	ব্যাকআপ টেপ, ল্যাপটপ এবং ফ্লাস ড্রাইভ এর মত সামগ্রির তালিকা ব্যবসা পরিকল্পনায় আছে কি না?	H		
১.১.৮	অব্যাহত ব্যবসা পরিকল্পনায় দুর্যোগ উদ্ধার অঞ্চল ম্যাপ উল্লেখ করা আছে কি না?	H		
১.১.৯	অব্যাহত ব্যবসা পরিকল্পনার কার্যকারিতা নিশ্চিত হওয়ার জন্য বছরে অন্তত একবার তা পরীক্ষা এবং পর্যালোচনা করা হয় কি না?	H		
১.১.১০	ব্যবসা এবং আইটি ব্যক্তিদের সমন্বয়ে কোনো অব্যাহত ব্যবসা পরিকল্পনা দল গঠন করা হয়েছে কি না?	H		
১.২ অনলাইন অপারেশনের জন্য অব্যাহত ব্যবসা পরিকল্পনা Business Continuity Plan (BCP) for ICT Operations (Online Operation)				
১.২.১	সব ধরনের সার্ভার, গুদামজাত উপকরণ এসএএন, নেটওয়ার্ক ডিভাইস, তাপমাত্রা ও আর্দ্রতা নিয়ন্ত্রক ডিভাইস এবং অন্যান্য সংশ্লিষ্ট ডিভাইস-এর ক্ষেত্রে সিস্টেম নিরাপত্তা, পরিবেশগত নিরাপত্তা ও ভৌত/শারীরিক নিরাপত্তা নিশ্চিত এবং পরিপালন করা হয় কি না?	H		
১.২.২	সার্ভারের Load Balancing এর ক্ষেত্রে নিম্নোক্ত বিষয় নিশ্চিত করা হয়েছে কি না? ক) এ্যাপ্লিকেশন-এর পর্যাপ্ততা; খ) উপাত্তের পর্যাপ্ততা; গ) এ্যাপ্লিকেশন-এর নিবিড়তর সমন্বয়ের ব্যবস্থা এবং ঘ) এ্যাপ্লিকেশন মেট্রিক্স ও হেলথ চেক-এর উপর ভিত্তি করে বুদ্ধিমত্তা ও অভিযোজ্যতার সাথে ইউজার ট্রাফিক-এর বহন ভারসাম্য করা।	H		
১.২.৩	উৎকৃষ্ট পারফরমিং লিংক-এ ট্রাফিক প্রবাহিত করে WAN ঠিকানায় নির্ভরযোগ্য ভারসাম্য বজায় রাখতে লিংক বহন ভারসাম্য নিশ্চিত করা হয়েছে কি না?	H		
১.২.৪	ভৌগলিকভাবে ভিন্ন ভিন্ন স্থানে অবস্থিত ডাটা সেন্টার এবং ডিআরএস এর মধ্যে নির্ভরযোগ্যতার জন্য গ্রাফিক্যাল Load Balancing ভারসাম্য নিশ্চিত করা হয়েছে কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
১.২.৫	নিরাপদ এ্যাপ্লিকেশন ও সফটওয়্যার-এর মাধ্যমে সাপোর্ট ডেলিভারি নিশ্চিত করা হয়েছে কি না?	H		
১.২.৬	সর্বোচ্চ পর্যায়ের নিরাপত্তার জন্য সমসাময়িক হাইপারফরমেন্স হার্ডওয়্যার সরবরাহ/সংযোজন করা হয়েছে কি না?	H		
১.২.৭	সংশ্লিষ্ট ডিপার্টমেন্ট/সেল কর্তৃক ডিআরএস এর পরিচালন, নির্দিষ্ট সময়ান্তে পরীক্ষা এবং যথাযথ রক্ষণাবেক্ষণ নিশ্চিত করা হয় কি না?	H		
১.২.৮	অব্যাহত ব্যবসা পরিকল্পনা গুরুত্বপূর্ণ সম্পদের জন্য ঝুকি সৃষ্টিকারী হুমকিসমুহ চিহ্নিত এবং র‍্যাংকিং করে কি না?	H		
১.২.৯	সংশ্লিষ্ট কর্তৃপক্ষের অনুমোদন অনুযায়ী প্রয়োজনীয় সার্ভার, নেটওয়ার্ক ডিভাইস, এ্যাপ্লিকেশনস, ডাটাবেইজ-এর দৈনিক, মাসিক, ত্রৈমাসিক, অর্ধ-বার্ষিক এবং বাৎসরিক ডাটা ব্যাকআপ নিয়ে পৃথকভাবে নিরাপদ হেফাজতে সংরক্ষণ করা হয় কি না?	H		
১.২.১০	সকল শাখা প্রতিদিন হিসাবের স্থিতির সফট কপি নিরাপদ স্থানে সংরক্ষণ করে কি না?	H		
১.২.১১	ব্যাকআপ টেপ/ডিস্ক আগুন ও পানি নিরোধক লকার-এ রাখা হয় কি না?	H		
১.২.১২	ভেন্ডরসহ জরুরি যোগাযোগ, ঠিকানা এবং ফোন নম্বর দৃশ্যমান স্থানে রাখা হয় কি না?	M		
১.২.১৩	DC থেকে DR রিয়াল টাইম ডাটা সিঙ্ক্রোনাইজেশন প্রক্রিয়া নিশ্চিত করা হয়েছে কি না?	H		
১.২.১৪	যে কোনো নিরাপদ আর্থিক লেন-দেনের জন্য ভিপিএন মোবাইল নেটওয়ার্ক ব্যবহার করা হয় কি না?	H		
১.৩ লিগেসি অপারেশনের জন্য অব্যাহত ব্যবসা পরিকল্পনা Business Continuity Plan (BCP) for ICT Operations (Legacy Operation)				
১.৩.১	সকল সার্ভার, নেটওয়ার্ক ডিভাইস, ল্যান এবং অন্যান্য হার্ডওয়্যার আইটি কর্মকর্তা অথবা দায়িত্বপ্রাপ্ত কর্তৃপক্ষের মাধ্যমে রক্ষণাবেক্ষণ করা হয় কি না?	M		
১.৩.২	জরুরি প্রয়োজনের সময় ব্যবহারের জন্য ব্যাকআপ সার্ভার ও অন্যান্য সম্পদ প্রস্তুত রাখার বিষয়টি নিশ্চিত করা হয়েছে কি না?	H		
১.৩.৩	প্রয়োজনীয় বিদ্যুৎ সরবরাহ এবং সংশ্লিষ্ট অন্যান্য নিয়ন্ত্রণকারী সরঞ্জামাদি (অনলাইন ইউপিএস, স্ট্যান্ড এলোন ইউপিএস, জেনারেটর, এভিআর ইত্যাদি) পর্যাপ্ত রয়েছে কি না?	H		
১.৪ কম্পিউটার/ল্যাপটপের জন্য অব্যাহত ব্যবসা পরিকল্পনা Business Continuity official Plan (BCP) for ICT operations (Standalone PC/Laptop)				
১.৪.১	প্রয়োজনীয় অফিসিয়াল ডাটা এবং অন্যান্য তথ্য সুরক্ষিত রাখা হয় কি না?	H		
১.৪.২	প্রয়োজনীয় ডাটার ব্যাকআপ রাখা হয় কি না?	H		
১.৫ সকল টায়ারের জন্য সাধারণ অব্যাহত ব্যবসা পরিকল্পনা Common BCP Plan For ICT Operations (All TIERs)				
১.৫.১	তাক (টায়ার) অনুযায়ী পর্যাপ্ত বিদ্যুৎ সরবরাহ, তাপ নিয়ন্ত্রণ ব্যবস্থা এবং অন্যান্য সরঞ্জামাদির ব্যবস্থা নিশ্চিত করা হয়েছে কি হয় নাই ?	M		
১.৫.২	তাক (টায়ার) অনুযায়ী অগ্নি নির্বাপণ ব্যবস্থা নিশ্চিত করা আছে কি না এবং সময় সময় তা পরীক্ষা করা হয় কি না?	H		
১.৫.৩	সম্ভাব্য দুর্যোগের হুমকি ও বিদ্যমান দুর্বলতার কারণে সম্পদের ক্ষতির বিষয়টি চিন্তা করে ঝুঁকির অগ্রাধিকার নিরূপণ করা হয়েছে কি না?	M		
১.৫.৪	শুধু হার্ড ড্রাইভ থেকে কম্পিউটার বুট করার জন্য বায়োস কনফিগার করা আছে কি না?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
১.৫.৫	অনুমতি ব্যতিত বায়োস এ যাতে কোন প্রকার পরিবর্তন করা না যায় সে জন্য বায়োস পাসওয়ার্ড দ্বারা সুরক্ষিত করা হয়েছে কি না?	M		
১.৫.৬	ডাটাতে প্রবেশাধিকার নিয়ন্ত্রিত কি না?	H		
১.৫.৭	যে সব কম্পিউটারে স্পর্শকাতর তথ্য আছে তা নিরাপদে বা তালাবদ্ধ কক্ষে রাখা হয় কি না ?	H		
১.৫.৮	Guest Account অকার্যকর করা হয়েছে কি না?	M		
২. দুর্যোগ-পুনরুদ্ধার পরিকল্পনা Disaster Recovery Plan (DRP)				
২.১	অনুমোদিত কোনো দুর্যোগে পুনরুদ্ধার পরিকল্পনা আছে কি না?	H		
২.২	পদ্ধতিগত ত্রুটির কারণে বড় ধরনের বিভ্রাট, হার্ডওয়্যারের অকার্যকারিতা, পরিচালন গত ত্রুটি বা নিরাপত্তা সংশ্লিষ্ট ঘটনা এবং প্রাইমারি ডাটা সেন্টার এর সম্পূর্ণ ধারণ অক্ষমতার মত বিভিন্ন অনিশ্চিত পরিস্থিতি DRP সমাধান করে কি না?	H		
২.৩	প্রাইমারি সাইট থেকে ডিআরএস ভৌগোলিকভাবে আলাদা স্থানে (অন্তত ১০ কি.মি. ব্যাসার্ধব্যাপী দূরবর্তী স্থানে এবং আলাদা ভূকম্পীয় এলাকায়) স্থাপন করা হয়েছে কি না?	H		
২.৪	যদি আলাদা ভূকম্পীয় এলাকায় ডিআরএস স্থাপন করা না হয় তাহলে ভিন্ন ভূকম্পীয় এলাকায় তৃতীয় একটি ডিআরএস স্থাপন করা আছে কি না?	H		
২.৫	দুর্যোগ মুহূর্তে ব্যবসায়িক কার্যক্রম পরিচালনার মত উপযুক্ত হার্ডওয়ার ও টেলি কমিউনিকেশন সরঞ্জাম ডিআরএস এ আছে কি না ?	H		
২.৬	ডিআরএস এবং/অথবা কাছের ডিসি-এর জন্য বাহ্যিক এবং পরিবেশগত নিরাপত্তা রক্ষা করা হয় কি না ?	H		
২.৭	আইসিটি সিস্টেমস এবং এ্যাপ্লিকেশন-এর জন্য রিকভারি টাইম অবজেক্টিভ (RTO) এবং রিকভারি পয়েন্ট অবজেক্টিভ (RPO) নির্ধারণ করা আছে কি না?	H		
২.৮	হালনাগাদ ও পরীক্ষিত ডিআর প্লান এর কপি নিরাপদ অফ-সাইট লোকেশন-এ রাখা হয়েছে কি না?	H		
২.৯	তাৎক্ষণিক রেফারেন্স এর জন্য হালনাগাদ ও পরীক্ষিত ডিআর প্লান এর কপি অফিসে সংরক্ষণ করা হয় কি না?	M		
২.১০	পুণরুদ্ধার প্রয়োজনে কার্যকারিতা ও জরুরি মুহূর্তে পুনরুদ্ধার প্রক্রিয়া বাস্তবায়নে কর্মীদের সামর্থ্য মূল্যায়নে বছরে অন্তত একবার ডিআর পুন পরীক্ষা করা হয় কি না?	H		
২.১১	পুণরুদ্ধারকৃত ব্যবস্থা যথাযথভাবে কাজ করছে কি না তা ব্যাপকভাবে পরীক্ষা করার জন্য বিজনেস ইউজার সম্পৃক্ত করা হয় কি না?	H		
২.১২	ডিআর টেস্ট ডকুমেন্টেশন-এ অন্তত পক্ষে সুযোগ, পরিকল্পনা ও পরীক্ষার ফলাফল অন্তর্ভুক্ত থাকে কি না?	H		
২.১২	ব্যবস্থাপনা কর্তৃপক্ষ এবং অন্যান্য সুবিধাভোগীকে ডিআর টেস্টের ফলাফল অবহিত এবং ভবিষ্যৎ প্রয়োজনের জন্য সংরক্ষণ করা হয় কি না?	H		
২.১৪	সম্পূর্ণ সিস্টেমকে স্বাধীনভাবে চালানোর যোগ্যতা দুর্যোগ পুনরুদ্ধার দলের আছে কি না?	H		
২.১৫	দুর্যোগ পুনরুদ্ধার দলের সদ্যসদেরকে ডিআর-এর উপর কোনো প্রশিক্ষণ দেয়া হয় কি না?	M		
২.১৬	দুর্যোগ পুনরুদ্ধার দলের সদ্যসদের ডিআর প্লান সরবরাহ করা হয় কি না?	M		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
২.১৭	পরিকল্পনার আলোকে ডিআর-দলের সদ্যসদের প্রশিক্ষণ দেয়া হয় কি না?	H		
২.১৮	ফায়ার সার্ভিস ও পুলিশ বিভাগের ফোন নম্বর রাখা হয় কি হয় না?	H		
২.১৯	অতিরিক্ত টেপ, সিডি, ডিভিডি বা অন্য কোনো ফ্লাস ড্রাইভ-এ নেয়া ব্যাকআপ এমন স্থানে রাখা হয় কি না যাতে সংশ্লিষ্ট ব্যক্তিরা তা সবসময় পেতে পারে?	M		
২.২০	রিড এন্ড রিস্টোর কনসিসটেন্সি-এর জন্য সিডি, ডিভিডি এবং ফ্লাস ড্রাইভ ও ডিআরএস ব্যাকআপ এর পরীক্ষা নিশ্চিত করা হয় কি না?	H		
২.২১	ওয়ার্ক পাওয়ার ডাউন থাকলে সকল এলার্ম এবং অন্যান্য জরুরি হার্ডওয়ারের জন্য ব্যাটারী ব্যাকআপ নিশ্চিত করা হয় কি না?	M		
২.২২	প্রয়োজনীয় লিখিত দলিলিকরণ, খসড়া, ম্যানুয়াল, ফর্ম, নির্দেশনা এবং ফোন নম্বরসহ একজন এম এল এস এস অফসাইট লোকেশন-এ রাখা হয় কি না?	M		
২.২৩	সার্ভার রুম, পাওয়ার রুম, গ্যাস সাপ্রেশন সিস্টেম, ফোন এবং ইলেকট্রিক্যাল সার্ভিস রুম দুর্ঘটনার সাধারণ কারণ "পানি পড়া" থেকে সুরক্ষিত কি না?	H		
২.২৪	ইমারজেন্সি কেবিনেট-এ মোমবাতি, দিয়াশলাই, ফ্লাশ লাইট, টুল বক্স এবং ফাস্ট-এইড কিট সংরক্ষণ করা আছে কি না?	M		
২.২৫	ডিসি এবং ডিআরএস এ ন্যূনতম একটি বহিঃগমণ পথ আছে কি না যা চাবি ছাড়া ব্যবহার করা যায়?	H		
২.২৬	গ্যাস সাপ্রেশন সিস্টেম এবং অন্যান্য সিকিউরিটি সিস্টেম এর পিরিয়ডিক্যাল/ডামি টেস্ট করা হয় কি না?	M		
২.২৭	দুর্যোগ পুনরুদ্ধারের জন্য পূর্ণ কর্তৃত্ব সম্পন্ন একজন বিকল্প ব্যাক্তি প্রস্তুত থাকেন কি না? (যখন ইনচার্জ অনুপস্থিত থাকেন)	M		
২.২৮	কম্পিউটার সামগ্রির পরিবর্তনের তথ্য সংরক্ষণ করা হয় কিনা?	M		
৩. ব্যাকআপ ও রিস্টোর পরিকল্পনা Backup and Restore Plan (BRP)				
১. ডাটা ব্যাকআপ ও রিস্টোর ব্যবস্থাপনা Data Backup and Restore Management				
২.১	ডাটা ব্যাকআপ এবং পুনরুদ্ধার নীতি আছে কি না?	M		
২.২	প্রত্যেক বিজনেস এ্যাপ্লিকেশন এর অনলাইন এবং অফলাইন ব্যাকআপ তৈরি করা এবং নিরাপদ অফসাইট স্টোরেজ এ তা সরিয়ে নেয়াসহ পরিকল্পিত, নির্ধারিত এবং ডকুমেন্টেড ব্যাকআপ কৌশল আছে কি না?	M		
২.৩	বিজনেস এপ্লিকেশন এর শ্রেণীবিন্যাস অনুযায়ী পরিকল্পিত ব্যাকআপ শিডিউল আছে কি না? (পূর্ণ, আংশিক, ইনক্রিমেন্টাল, পার্থক্যমূলক, রিয়েল টাইম মনিটরিং)।	M		
২.৪	তথ্যের জন্য নেয়া ব্যাকআপের ফ্রিকুয়েন্সি তথ্যের শ্রেণীবিন্যাস ও প্রত্যেক এপ্লিকেশনের ব্যবসা চালু রাখার পরিকল্পনা অনুযায়ী নির্ধারণ করা হয়েছে কি না?	M		
২.৫	রিটেনশন পিরিয়ড এবং আর্কাইভ তথ্যসহ প্রত্যেক এপ্লিকেশনের জন্য পরিকল্পিত ব্যাকআপ সিডিউল আছে কি না?	M		
২.৬	ব্যাকআপ ইনভেন্টরি এবং লগ শিট সংরক্ষণ, সুপারভাইজার কর্তৃক যাচাই এবং স্বাক্ষর করা হয় কি না?	H		
২.৭	স্পর্শকাতর ও গোপনীয় তথ্য সম্বলিত টেপ বা ডিস্ক সংরক্ষণের জন্য অফ-সাইট এ প্রেরণের আগে এনক্রিপ্ট করা হয় কি না?	H		
২.৮	জরুরি মুহূর্তে সেবা অব্যাহত রাখতে ব্যাকআপের অন্তত এক কপি অন-সাইট লোকেশনে রাখা হয় কি না?	H		
২.৯	অন-সাইট ও অফ-সাইট উভয় ব্যাকআপ স্টোরেজ থেকে তথ্য পুনরুদ্ধার করার প্রক্রিয়া দলিলায়ন করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
২.১০	ব্যাকআপ মিডিয়ার পুনরুদ্ধার সক্ষমতা সময়ে সময়ে পরীক্ষা এবং এর ভেলিডেশন করা হয় কি না?	H		
২.১১	অন-সাইট ব্যাকআপ মিডিয়া এর লগ-এ নিম্নলিখিত তথ্যগুলো রাখা হয় কি না? ক. ব্যাকআপ নেয়ার তারিখ ; খ. মিডিয়ার বিষয়বস্তু (যেমনঃ লেনদেনের ব্যাকআপ, এপ্লিকেশনের ব্যাকআপ, সম্পূর্ণ সিস্টেমের ব্যাকআপ); গ. অফ-সাইট লোকেশনে মিডিয়া স্থানান্তরের তারিখ ; ঘ. ব্যাকআপের ধরন (যেমনঃ সম্পূর্ণ ব্যাকআপ অথবা ডাটাবেইজ অথবা ফাইল কপি); ঙ. অন-সাইট লোকেশনের দায়িত্বপ্রাপ্ত ব্যাক্তির নাম ও স্বাক্ষর; চ. অন্য কোনো লেভেলের তথ্য ।	M		
২.১২	অফ-সাইট ব্যাকআপ মিডিয়া এর লগ এ নিম্নলিখিত তথ্য রাখা হয় কি না? ক. অফ-সাইট লোকেশনে মিডিয়া গ্রহণের তারিখ; খ. মিডিয়ার বিষয়বস্তু (যেমনঃ লেন-দেনের ব্যাকআপ, এপ্লিকেশনের ব্যাকআপ, সম্পূর্ণ সিস্টেমের ব্যাকআপ); গ. ব্যাকআপের ধরন (যেমনঃ সম্পূর্ণ ব্যাকআপ অথবা ডাটাবেইজ অথবা ফাইল কপি); ঘ. বাহকের নাম ; ঙ. আসল লোকেশনের নাম ; চ. অফ-সাইট লোকেশনে মিডিয়া গ্রহণের দায়িত্বপ্রাপ্ত ব্যক্তির নাম ও স্বাক্ষর ; ছ. অন্য কোনো লেভেলের তথ্য।	M		
২.১৩	ব্যাকআপ এ নিম্নলিখিত রিটেনশন পিরিয়ড পলিসি অনুসরণ করা হয় কি না? ক. প্রতি কার্যদিবসে ব্যাকআপ নেয়া; খ. গৃহিত ব্যাকআপ প্রধান কার্যালয়ের ডাটা সেভ লকারে রাখা ; গ. প্রতিদিনের ব্যাকআপ আইসিবিরি লোকাল অফিসে প্রেরণ করা; ঘ. মাসিক ভিত্তিতে বগুড়া শাখায় ব্যাকআপ প্রেরণ করা।	M		
২.১৪	ব্যাকআপ মিডিয়া প্রেরণা ও গ্রহণের রেজিস্টার সংরক্ষণ করা হয় কি না?	M		
১.১ ডাটা সেন্টার ও দুর্যোগ পুনরুদ্ধার সাইট এর ব্যাকআপ পলিসি (টায়ার-১) **Backup policy for Data Center and Disaster Recovery Site (Tier-1)**				
১.১.১	অপারেটিং সিস্টেম, সকল এপ্লিকেশন, ডাটা (ডাটাবেজসহ), ইউজার কনফিগারেশনের তথ্য, নেটওয়ার্ক ডিভাইস কনফিগারেশন এবং হার্ডওয়্যার কনফিগারেশনের তথ্য, ইমেজ কপি, পূর্ণ ব্যাকআপ, ইনক্রিমেন্টাল ব্যাকআপ, পার্থক্যমূলক ব্যাকআপ, সিস্টেম লগস, ট্রানজেকশনাল লগস, ডাটাবেজ লগস বা অন্যান্য কৌশলের সমন্বয়ে ব্যাকআপ রাখা হয় কি না?	H		
১.১.২	ডাটা সেন্টারে সংঘটিত কোন দুর্যোগের ক্ষতি থেকে ব্যাকআপ রক্ষা করার জন্য ডাটা সেন্টার থেকে পর্যাপ্ত দূরত্বে ব্যাকআপ সংরক্ষণ করা হয় কি না?	H		
১.১.৩	গুরুত্বপূর্ণ ডাটার সকল দৈনিক, সাপ্তাহিক, মাসিক, ত্রৈমাসিক এবং বাৎসরিক ব্যাকআপ টেপ এর সম্পূর্ণ পুনরুদ্ধারযোগ্য ভার্সনের অন্তত দুই কপি রাখা হয় কি না?	M		
১.১.৪	ডাটা সেন্টারে ব্যাকআপের একটি কপি সংরক্ষণ করা হয় কি না?	M		
১.১.৫	ব্যাকআপের একটি কপি অফ-সাইট লোকেশনে সংরক্ষণ করা হয় কি না?	M		
১.১.৬	একটি সমন্বিত সিডিউল অনুযায়ী সিস্টেম/নেটওয়ার্ক এডমিনিস্ট্রেটর কর্তৃক অপারেটিং সিস্টেম, ডাটাবেজ, ইউজার কনফিগারেশন, নেটওয়ার্ক ডিভাইস,সংশ্লিষ্ট এপ্লিকেশন এবং হার্ডওয্যার কনফিগারেশনের তথ্যের ব্যাকআপ নেয়া হয় কি না?	H		
১.১.৭	সফলভাবে ব্যাকআপ নেয়া নিশ্চিত করতে সিস্টেম এডমিনিস্ট্রেটর/দায়িত্বপ্রাপ্ত কর্মকর্তা। ডাটা ও অন্যান্য অপারেশনের ব্যাকআপ নেয়ার প্রক্রিয়া অনুসরণ করেন কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
১.১.৮	প্যাচ, ব্যাচ ইন্সটল বা আপগ্রেড অথবা সিস্টেম কনফিগারেশনে কোন পরিবর্তনের আগে ও পরে সিস্টেম/নেটওয়ার্ক এডমিনিস্ট্রেটর কর্তৃক ব্যাকআপ নেয়া হয় কি না?	H		
১.১.৯	গোপনীয় ব্যাকআপ ডাটা এনক্রিপ্ট করে/সেফটি লকার/আগুন ও পানি নিরোধক লকারে সংরক্ষণ করা হয় কি না?	H		
১.১.১০	ব্যাকআপ মিডিয়ার পরীক্ষা নিশ্চিত করা হয় কি না?	H		
১.১.১১	ব্যাকআপ মিডিয়া (যথা: সিডি, ডিভিডি, টেপ ইত্যাদি) এর গুণগতমান ও নিয়মিতভাবে পুণঃব্যবহারের শর্ত সংশ্লিষ্ট কর্তৃপক্ষ কর্তৃক পরীক্ষা করা হয় কি না	M		
১.১.১২	ব্যাকআপ পরীক্ষার পর টেস্ট এনভায়রনমেন্ট হতে তা নিরাপদভাবে মুছে ফেলা হয় কি না?	M		
১.১.১৩	পরীক্ষা শেষে একটি পরীক্ষা প্রতিবেদন প্রস্তুত করে সংশ্লিষ্ট কর্তৃপক্ষের কাছে জমা দেয়া হয় কি না?	M		
১.২ টায়ার-১, টায়ার-২ এবং টায়ার-৩ এর জন্য সাধারণ ব্যাকআপ নীতিমালা General Backup Policy for Tier-1, Tier-2, Tier-3				
১.২.১	একটি সমন্বিত সূচি অনুযায়ী প্রয়োজনীয় ব্যবসায়িক তথ্য, ডাটা ও সফটওয়্যার এবং অপারিটিং সিস্টেমের দৈনিক, সাপ্তাহিক, মাসিক, ত্রৈমাসিক ও বাৎসরিক ব্যাকআপ নেয়া হয় কি না?	M		
১.২.২	সফলভাবে ব্যাকআপ নেয়া নিশ্চিত করতে সিস্টেম এডমিনিস্ট্রেটর কর্তৃক ব্যাকআপ ডাটা যাচাই বাছাই প্রক্রিয়া অনুসরণ করা হয়কি না?	H		
১.২.৩	সার্ভারসহ কয়েকটি ডেস্কটপ এর হার্ড ডিস্ক ড্রাইভে প্রাইমারি ব্যাকআপ রাখা হয় কি না?	M		
১.২.৪	তাৎক্ষণিকভাবে পেতে সিডি/ডিভিডি/টেপ এ সেকন্ডারি ব্যাকআপ ধারণ করে এর কপি ব্যবস্থাপক/প্রধান কার্যালয়/শাখাপ্রধানের কাছে সংরক্ষণ করা হয় কি না?	M		
১.২.৫	দুর্যোগ কিংবা মিডিয়া ব্যর্থতার পর সকল প্রয়োজনীয় ব্যবসায়িক তথ্য ও সফটওয়্যার পুনরুদ্ধারের বিষয়টি নিশ্চিত করতে পর্যাপ্ত ব্যাকআপ সুবিধা রাখা হয়েছে কি না?	M		
১.২.৬	ব্যবসা অব্যাহত রাখা পরিকল্পনার চাহিদা পূরণে ইনডিভিজুয়াল সিস্টেমস ও সংশ্লিষ্ট ডাটার ব্যাকআপ নেয়ার ব্যবস্থা ফরমাল সিডিউল মেনে পরীক্ষা করা হয়েছে কি না?	M		
১.২.৭	ব্যাকআপ এবং পুনরুদ্ধার প্রক্রিয়া মোতাবেক সকল এপ্লিকেশন, অপারেটিং সিস্টেম, ডাটা (ডাটাবেজসহ), ইউজার কনফিগারেশন তথ্য, নেটওয়ার্ক ডিভাইস কনফিগারেশন এন্ড হার্ডওয়্যার কনফিগারেশন তথ্যের ব্যাকআপ নেয়া হয় কি না?	M		
১.২.৮	যথাযথ দলিলায়নসহ সিস্টেমের চাহিদা এবং ভেন্ডরের সুপারিশ অনুযায়ী পৃথক সিস্টেম স্পেসিফিক ব্যাকআপ ও রিটেনশন পদ্ধতি তৈরি করা হয়েছে কি না?	M		
১.৩ ব্যাকআপ রেস্টোরেশন প্রক্রিয়া (Backup Restoration Procedures)				
১.৩.১	কোনো পুনরুদ্ধার প্রক্রিয়া তৈরি করা হয়েছে কি না?	L		
১.৩.২	পরীক্ষা পরিবেশে আনুষ্ঠানিক সূচি অনুযায়ী একটি ব্যাকআপ নমুনা রেস্টোর করার মাধ্যমে সিস্টেম এডমিনিস্ট্রেটর কর্তৃক সিস্টেম সফটওয়্যার এবং ডাটা ব্যাকআপ পরীক্ষা করা হয় কি না?	H		
১.৩.৩	পুনরুদ্ধার প্রক্রিয়ার কার্যকারিতা এবং পরিচালন প্রক্রিয়ায় পুনরুদ্ধারের জন্য বরাদ্দকৃত সময়ের মধ্যে এটি সম্পন্ন হওয়ার বিষয়টি নিশ্চিত হতে এ পদ্ধতি নিয়মিত (অন্তত বাৎসরিক ভিত্তিতে) যাচাই এবং পরীক্ষা করা হয় কি না?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
চ. অধিগ্রহণ ও তথ্য পদ্ধতির উন্নয়ন (Acquisition and Development of Information System)				
১. আইসিটি প্রকল্প ব্যবস্থাপনা (ICT Project Management)				
১.১	এমন কোনো প্রকল্প ব্যবস্থাপনা কাঠামো আছে কি না যাতে প্রকল্পের সাথে জড়িত কর্মীদের দায়িত্ব ও কর্তব্য সুনির্দিষ্টভাবে উল্লেখ করা হয়?	M		
১.২	সকল আইসিটি প্রকল্পের প্রকল্প পরিকল্পনা স্পষ্টভাবে নথিভুক্ত করা এবং অনুমোদন নেয়া হয়েছে কি না?	H		
১.৩	ইউজার ফাংশনাল রিকয়ারমেন্টস, বিজনেস কেসেস, কস্ট-বেনিফিট এনালাইসিস, সিস্টেম ডিজাইন, টেকনিক্যাল স্পেসিফিকেশন, টেস্ট প্লানস এবং সার্ভিস পারফর্মেন্স এক্সেপশন সংশ্লিষ্ট ব্যবসায়িক ইউনিট এবং আইসিটি ব্যবস্থাপনা কর্তৃপক্ষ কর্তৃক অনুমোদিত কি না?	H		
১.৪	লক্ষ্য বস্তুতে পৌছানো এবং যথাসময়ে ডেলিভারেবল প্রাপ্তি নিশ্চিত করতে প্রকল্পে ব্যবস্থাপনা কর্তৃপক্ষের তদারকি জোরদার করা হয়েছে কি না?	H		
২. সিস্টেম অধিগ্রহণের জন্য ভেন্ডর নির্বাচন (Vendor Selection for System Acquisition)				
২.১	ভেন্ডর নির্বাচনের জন্য ফাংশনাল ডিপার্টমেন্ট, আইসিটি ডিপার্টমেন্ট এবং আইসিসি ডিপার্টমেন্ট থেকে জনবল নিয়ে মূল দল গঠন করা হয়েছে কি না?	H		
২.২	আইসিবির ক্রয়নীতির সাথে সামঞ্জস্য রেখে ভেন্ডর নির্বাচন প্রক্রিয়া সম্পন্ন করা হয়েছে কি না?	H		
২.৩	এপ্লিকেশনের জন্য ভেন্ডর নির্বাচনের মানদন্ড বিচারে নিম্নলিখিত বিষয়সমূহ মেনে চলা হয় কি না? ক. বাজারে উপস্থিতি; খ. কত বছর ধরে কার্যক্রম চলছে; গ. প্রযুক্তি সম্পৃক্ততা; ঘ. কাস্টমাইজেশনের ব্যাপ্তি এবং সমাধানের কাছাকাছি কাজ; ঙ. অর্থনৈতিক শক্তি/অর্থবল; চ. কর্মক্ষমতা এবং পরিমাপযোগ্যতা; ছ. স্থাপনের সংখ্যা; জ. বর্তমান গ্রাহকের রেফারেন্স ; ঝ. সমর্থন ব্যবস্থা; এ. বিদেশি ভেন্ডরদের ক্ষেত্রে স্থানীয় সমর্থনের ব্যবস্থা; ট. অর্থনৈতিক ও কারিগরী প্রস্তাবের গভীরতা।	M		
৩. ইন-হাউজ সফটওয়্যার উন্নয়ন (In-House Software Development)				
৩.১	বিস্তারিত ব্যবসায়িক চাহিদা দলিলায়িত এবং কর্তৃপক্ষ কর্তৃক অনুমোদিত কি না?	H		
৩.২	বিস্তারিত কারিগরি চাহিদার নকশা প্রস্তুত করা ও দলিলায়িত করা হয়েছে কি না?	H		
৩.৩	এপ্লিকেশনের নিরাপত্তা এবং প্রাপ্যতার প্রয়োজনীয়তা চিহ্নিতকরা হয়েছে কি না?	M		
৩.৪	এপ্লিকেশনের উন্নয়ন কাজ নকশা নির্দিষ্ট করণ ও দলিলায়ন অনুযায়ী হয় কি না?	M		
৩.৫	উন্নয়ন ও বাস্তবায়ন পর্যায়ে ইউজার এক্সেপটেন্স টেস্ট (UAT) সহকারে সফটওয়্যার ডেভেলপমেন্ট লাইফ সাইকেল (SDLC) অনুসরণ করা হয়েছিল কি না?	M		
৩.৬	উন্নয়নের পর ইউজার ভেরিফিকেশন টেস্ট (UVT) করা হয় কি না?	H		
৩.৭	ব্যবস্থা/পদ্ধতি দলিলায়ন এবং ইউজার ম্যানুয়াল তৈরি করে সংশ্লিষ্ট কর্তৃপক্ষের কাছে হস্তান্তর করা হয়েছে কি না?	L		
৩.৮	ইন-হাউস সফটওয়্যারের সোর্স কোড নিরাপদে সংরক্ষণ করা হয় কি না?	H		
৩.৯	সোর্স কোডে লেখকের নাম, তৈরির সময়, মডিফিকেশন এর শেষ তারিখ এবং অন্যান্য প্রাসঙ্গিক তথ্যসহ টাইটেল এরিয়া আছে কি না?	M		
৩.১০	আইসিটি নিরাপত্তা নীতি/আইটি নীতির সংশ্লিষ্ট নিয়ন্ত্রণের সাথে এপ্লিকেশনসমূহ সামঞ্জস্যপূর্ণ কি না?	M		
৩.১১	প্রয়োজনীয় নিয়মানুগ পরিপালন চাহিদা বিবেচনায় রাখা হয় কি না?	H		
৩.১২	সফটওয়্যার বাস্তবায়নের পূর্বে ICT Audit করা হয় কিনা?	H		

ক্রমিক নং (SL No)	বিশদ বিবরণ (Particulars)	ঝুঁকি (Risk)	হ্যাঁ (Yes	না (No)
৪. সফটওয়্যার ডকুমেন্টেশন (Software Documentation)				
৪.১	সফটওয়্যারের ডকুমেন্টেশন সহজলভ্য ও নিরাপদে সংরক্ষণ করা হয় কি না?	H		
৪.২	সফটওয়্যারের ডকুমেন্টেশন এ নিম্নের বিষয়গুলো থাকে কি না? ক. কার্যকারিতা; খ. নিরাপত্তা বৈশিষ্ট্য; গ. অন্যান্য সিস্টেমের সাথে পারস্পরিক সমন্বয়মুখীতার জন্য প্রয়োজনীয় বিষয়; ঘ. সিস্টেম ডকুমেন্টেশন; ঙ. ইন্সটলেশন ম্যানুয়াল; চ. ইউজার ম্যানুয়াল।	M		
৫. সংবিধিবদ্ধ চাহিদা (Statutory Requirement)				
৫.১	সংশ্লিষ্ট ডিপার্টমেন্ট সকল ক্রয়কৃত ও সংযোজিত সফটওয়্যারের বৈধ লাইসেন্স ও রেকর্ড সংরক্ষণ করে কি না?	M		
৫.২	সফটওয়্যার সংযোজনের পূর্বে সংশ্লিষ্ট ডিপার্টমন্টে একটি আলাদা পরীক্ষণ পরিবেশ এর কার্যকারিতা পুরোপুরিভাবে পরীক্ষা করে কি না?	H		
৫.৩	লাইভ কার্যক্রম শুরুর আগে সংশ্লিষ্ট ব্যবসায়িক প্রতিষ্ঠান/ডিপার্টমেন্ট কর্তৃক ইউজার এক্সেপটেন্স টেস্ট করত: তা স্বাক্ষর করা হয় কি না?	H		
৫.৪	প্রক্রিয়া ও কর্মকান্ডের জন্য প্রয়োজনীয় বিধি বিধান পরিপালনের বিষয় এবং এর সাথে সংশ্লিষ্ট বাংলাদেশ সরকারের আইন বিবেচনায় নেয়া হয়েছে কি না?	H		
৫.৫	নকশায় দুর্বলতার কারনে সফটওয়্যারে পাওয়া ত্রুটি (Bug) সফটওয়্যার ভেন্ডর প্রতিষ্ঠানের ও আইসিবির উর্ধতন কর্তৃপক্ষের কাছে উপস্থাপন করা হয় কি না?	H		
৫.৬	গোপনীয়তা চুক্তির সাথে উৎপাদনে ব্যবহৃত এপ্লিকেশন সফটওয়্যার সরবরাহকারীর সাথে সহায়তা চুক্তি রক্ষা করা হয় কি না?	M		