Government of West Bengal
Department of Information Technology & Electronics
Moni Bhandar, 5th and 6th Floor, Sector V, Block EP&GP,
Salt Lake, Kolkata 700091.
Phone: 2357-2545, Fax: 2357-2534.

NOTIFICATION

No-1280-Estt/ITE-20013/3/2023 Dated: 17.11.2023.

WHEREAS, in today's world of rapid digitalization and increasing dependencies on technology and ensuring the security of the digital assets and safeguarding the sensitive information of the citizens which has become a paramount concern for the State Government ;

AND WHEREAS, recognising the critical need for a comprehensive cyber security approach, the State Government has felt the need to develop cyber security strategy which will address unique challenges that Government faces;

AND WHEREAS, these strategies are designed to fortify digital defences of public assets, protect citizens and ensure the continued growth and development of the State in an ever evolving digital landscape;

NOW THEREFORE, the Governor is pleased to notify the 'West Bengal Cyber Security Strategy, 2023'(attached herewith) that will implement various Cyber Security Strategies enumerated therein through WBEIDC Ltd. (Webel), being the State Implementing Agency and State Level Nodal Agency (SLNA) by way of requisite means that include but not restricted to Awareness and Skilling, Cybersecurity Assurance, Incident Response and Mitigation (IR&M), Investigation and Forensic Studies and Research and Development;

This has the approval of the competent authority of this Department vide Diary No. 213 dated 17.11.2023.

Enclosure: As stated.

By order of the Governor,

Principal Secretary to the
Government of West Bengal

O/C

No. 1280/1(85)–Estt/ITE-20013/3/2023 Dated: 17.11.2023

Copy forwarded for kind information and necessary action to:-

- The Secretary to the Government of India, Department of Telecommunications, Sanchar Bhawan, New Delhi.
- The Secretary to the Government of India, Ministry of Electronics & Information Technology, 6, CGO Complex, New Delhi-110003.
- The Additional Chief Secretary/ Principal Secretary/ Secretary,______________Department(all), Government of West Bengal.
- The Managing Director, WBEIDC Ltd., Webel Bhavan, Block: EP & GP, Sector-V, Salt Lake City, Kolkata- 700091.
- The Managing Director, WBIDC, 23, Abanindranath Tagore Sarani, 'Protiti', Kolkata- 700017.
- The Managing Director, WBIIDC, Block- DJ, Plot No. 10, Sector-II, Salt Lake City, Kolkata-700091.
- The Managing Director, WBSIDCL, 31, Black Burn Lane, 4th Floor, Shilpa Bhavan, Kolkata-700012.
- The Managing Director, WBHIDCO, Premises No. 35-1111, Biswa Bangla Sarani, 3rd Rotary, New Town, Kolkata- 700156.
- The Chief Executive Officer, Webel Technology Limited, BP-5, Sector-V, Salt Lake City, Kolkata- 700091.
- The District Magistrate,_________________________, District (all), West Bengal.
- The OSD to the Chief Secretary, Government of West Bengal.
- The PS to the Hon'ble MIC, IT&E Department, Government of West Bengal.
- The SPA to the Principal Secretary, IT&E Department, Government of West Bengal.

17/11/2023.

Additional Secretary to the
Government of West Bengal

No. 1280/1(85)/2(13)–Estt/ITE-20013/3/2023 Dated: 17.11.2023

Copy forwarded for information only to:

- The Director General, Digital Infrastructure Providers Association (DIPA), 2nd& 3rd Floor, 7, Bhai Veer Singh Marg, Gole Market, New Delhi- 110001.
- The Director General, COAI, Sector- 2, Bhai Veer Singh Marg, Gole Market, New Delhi- 110001.
- The Director, STPI, Kolkata, Webel STP 2 Building, 2nd Floor, DN-53, Sector-V, Salt lake, Kolkata- 700091.
- The Regional Director (East), NASSCOM RO East, Infinity Business Centre, Infinity Benchmark, Room No. 605, 6th Floor, Block-EP&GP, Plot- G1, Sector-V, Salt lake, Kolkata- 700091.
- The President, BCC&I, 6, Netaji Subhas Road, Kolkata- 700001.
- The President, COMPASS, 37, Shakespear Sarani, Kolkata- 700017.
- The President, TIE, Infinity Benchmark, Infinity Business Centre, 6th Floor, Suite# 607, Plot-GP, Sector-V, Salt lake, Kolkata- 700091.
- The Associate Vice President, Internet & Mobile Association of India, 232-B, Ground Floor, Okhla Industrial Estate, Phase-III, New Delhi- 110020.
- The Director, FICCI, Dhanseri House, 4A, Woodburn Park, Kolkata- 700020.
- The Director, CII, 6, Netaji Subhas Road, Kolkata- 700001.
- The Director General & CEO, AMCHAM, PHD House, 4th Floor, 4/2, Siri Institutional Area, August Kranti Marg, New Delhi- 110016.
- The Director (East &North East), ASSOCHAM, 18, Ballygunge Circular Road, Kolkata- 700019.
- The Chairman, Electronics and Computer Software Export Promotion Council, Ground Floor, Building No. DN-53, STP-II Building, Salt lake, Kolkata- 700091.

17/11/2023.

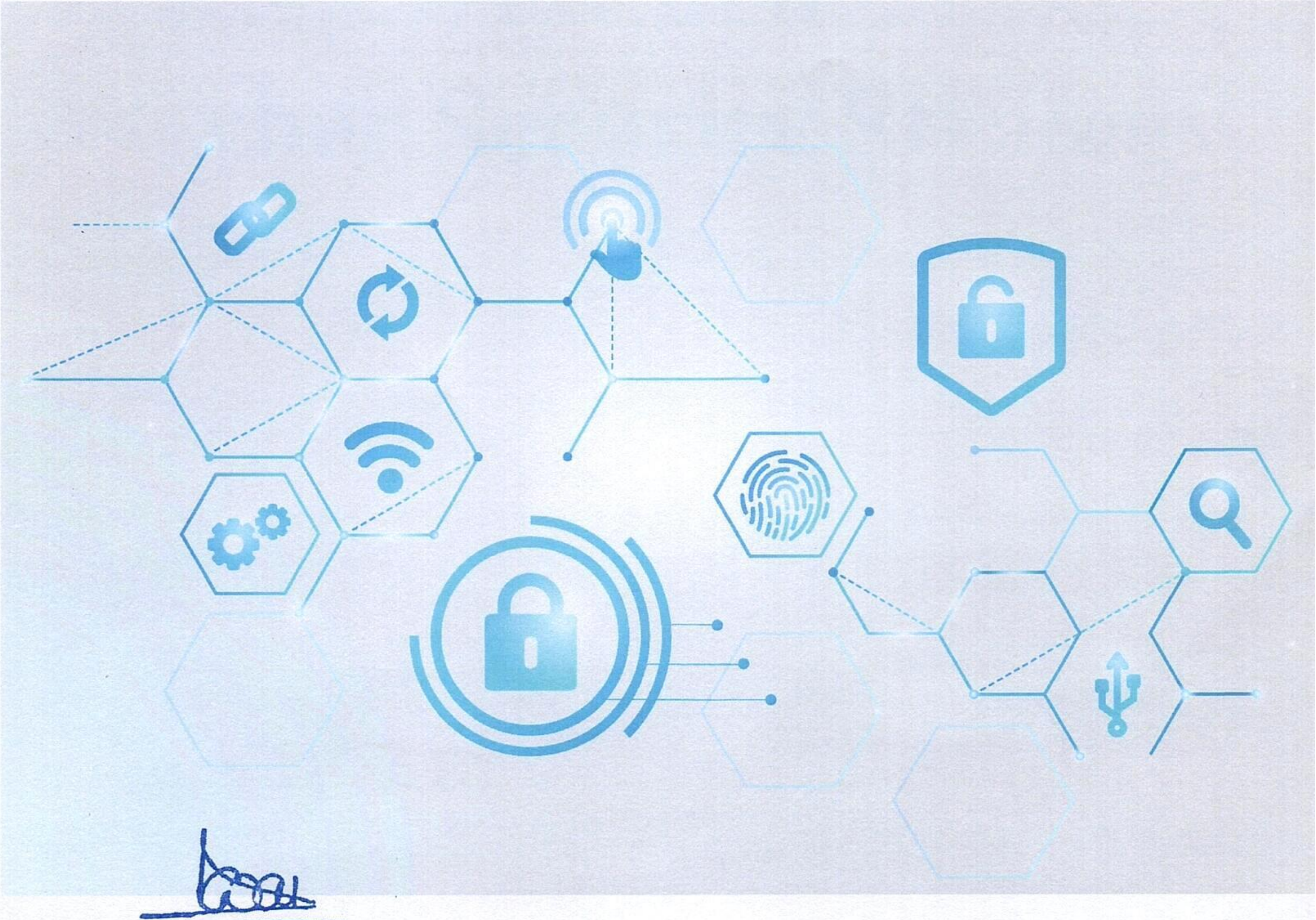
Additional Secretary to the
Government of West Bengal

Department of Information Technology & Electronics

Government of West Bengal

West Bengal Cyber Security Strategy 2023

Notified Vide No. 1280-Estt/ITE-20013/3/2023 dated 17.11.2023



West Bengal Cyber Security Strategy:

In an era characterized by rapid digitization and increasing dependence on technology, ensuring the security of digital assets and safeguarding the sensitive information of its citizens has become a paramount concern for the government of West Bengal. Recognizing the critical need for a comprehensive cyber security approach, the state government is poised to implement a range of cyber security strategies that address the unique challenges it faces. These strategies are designed to fortify its digital defences, protect its citizens, and ensure the continued growth and development of the state in an ever-evolving digital landscape.

The West Bengal cyber security strategy comprises five different pillars:

01

Awareness& Skilling

02

Cyber Security Assurance

03

Incident Response Management

04

Investigation and Forensic

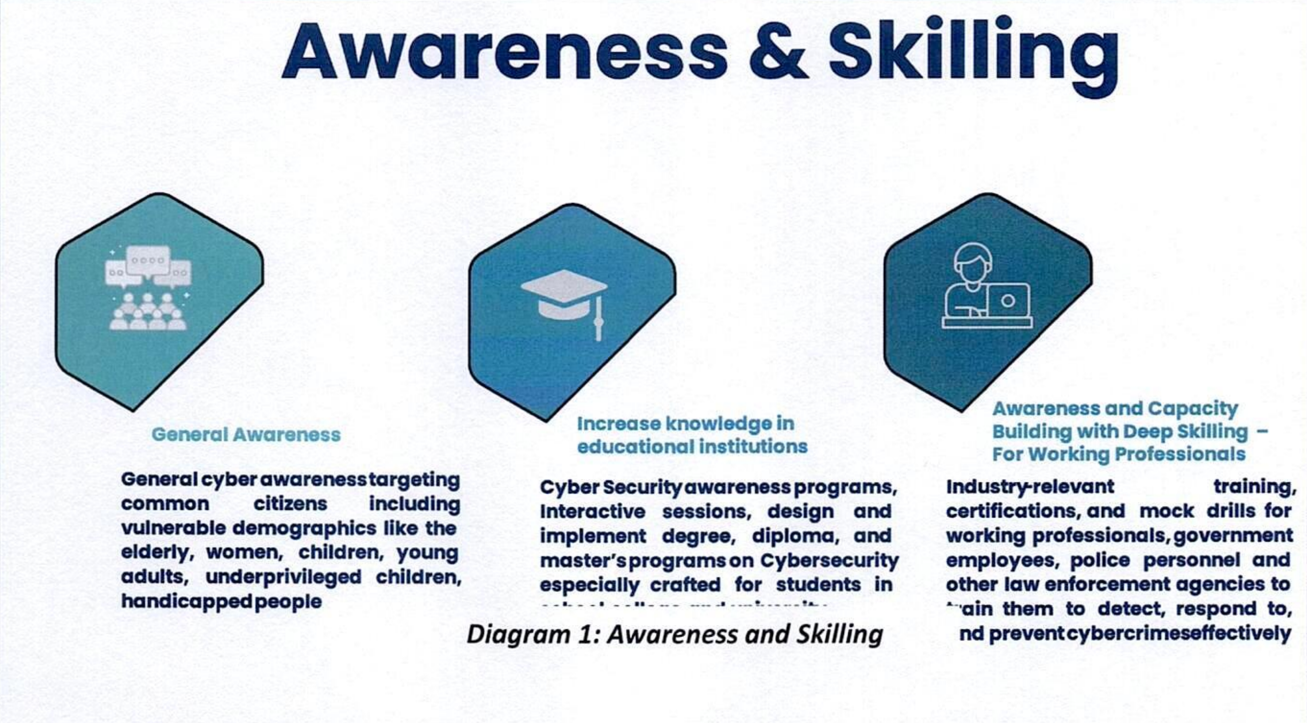
05

Research and Development

(R&D)

Pillar 1: Awareness & Skilling

Awareness generation and skilling are crucial for building a resilient and well-prepared cyber security ecosystem. This pillar focuses on educating, training, and raising awareness among various stakeholders, including government employees, businesses, and the general public.



Awareness & Skilling

General Awareness

General cyber awareness targeting common citizens including vulnerable demographics like the elderly, women, children, young adults, underprivileged children, handicapped people

Increase knowledge in educational institutions

Cyber Security awareness programs, Interactive sessions, design and implement degree, diploma, and master's programs on Cybersecurity especially crafted for students in

Awareness and Capacity Building with Deep Skilling – For Working Professionals

Industry-relevant training, certifications, and mock drills for working professionals, government employees, police personnel and other law enforcement agencies to train them to detect, respond to, nd prevent cybercrimes effectively

Diagram 1: Awareness and Skilling

hygiene and safe internet practices, especially for vulnerable demographics like the elderly, women, children, young adults, etc.

b. The State Cyber Security Centre of Excellence (CS-CoE) web portal should broadcast cyber security-related news, advisories, guidelines, and audio-visual messages for the public.

c. Cyber awareness-related training on Cyber Security, Cyber Hygiene Practices, knowledge of recent trends in Cyber Crime, and Cyber Law should be provided to government employees of various departments.

d. The government should conduct various awareness generation sessions like awareness camps, seminars, hackathon competitions, exhibitions, quiz/case-study challenges etc. aimed at common citizens to raise awareness about cyber threats and best practices.

e. Awareness sessions should be conducted in association with NGOs for audience groups like underprivileged children,differently abled people etc.

2. Increase knowledge in educational institutions – school, college, university:

a. Cyber Security awareness programs should be arranged for students in schools, colleges, and universities.

b. Interactive sessions on Cyber Security and Digital Forensics should be organized for the students.

c. To create a pool of skilled Cyber security professionals, CS-CoE should partner with leading educational institutions of the State Government to design and implement degree, diploma, and master's programs on Cyber security.

d. The state will **develop more Cyber security skilled manpower at the diploma level.** The Cyber security Centre of Excellence (CoE) has successfully crafted a comprehensive **diploma course on "Cyber Forensic & Information Security"anda certification course on "Cyber Guard"** which are currently undergoing a pilot phase in various Polytechnics and Vocational Training Centre(s). Through rigorous testing, assessment, and feedback, the CS-CoE will fine-tune the curriculum and develop new courses as required.Upon the successful conclusion of the pilot phase, the government is primed to initiate the rollout of the diploma and vocational courses at the state level.

3. Awareness Generation and Capacity Building with Deep Skilling – For Working Professionals:

a. **Cyber Security Certification**: The Cyber Security CoE shall develop Industry-ready certification courses and training accredited by organizations like **CERT-In, DSCI, NCIIPC, National Skill Development Corporation India, EC-Council and Indian School of Ethical Hacking-ISOEH** for working professionals of Corporate/Government/PSU sectors to upgrade their skills in Cyber Security.

b. **Next Generation Cyber Security Skilling shall be provided to the Police personnel** for effective Cyber Crime Management. This will equip them to detect,respond to and prevent cybercrimes effectively, handle digital evidence, and adapt to evolving threats, ensuring a proactive and proficient response to cyber incidents.

c. On-the-job cyber awareness training should be provided to all government employees.

d. The Cyber Security CoE should train the police and other law enforcement agencies of the state government on responding to cybercrimes, handling digital evidence, etc.

e. All police personnel up to the rank of Sub-Inspectors should be given First Responder Training (FRT) on various IT laws, Basics of IT Systems, Networks and Digital evidence.

f. The state should provide hands-on Detailed Responder Training (DRT) to investigating officers of any cyber-related crime so that they are well aware of collecting and analyzing digital evidence for the investigation process.

g. Cyber Forensic preparatory training should be provided to CID Officials of WB Police.

h. Respective police personnel should get training on CDR/IPDR forensic tools.

i. **Acquiring Cyber Range:** The state is planning to have a Cyber Range which is a simulated platform resembling the actual infrastructure in a miniature form. This Cyber Range can be used for advanced hands-on training and offensive and defensive exercises.

j. **Mock Phishing Drills:** Mock Phishing Drills should be conducted for the employees of different government departments to check their cyber security awareness.

k. **Training on Secure Coding Practice and Application Development Framework:**The state is already conducting a training workshop on the **Secure Coding Practice Framework** for all the Application Developers and System Integrators of all the government departments. Now the plan is to upgrade it by combining the principles of Secure Coding Practice Framework, **Guidelines for Indian Government**

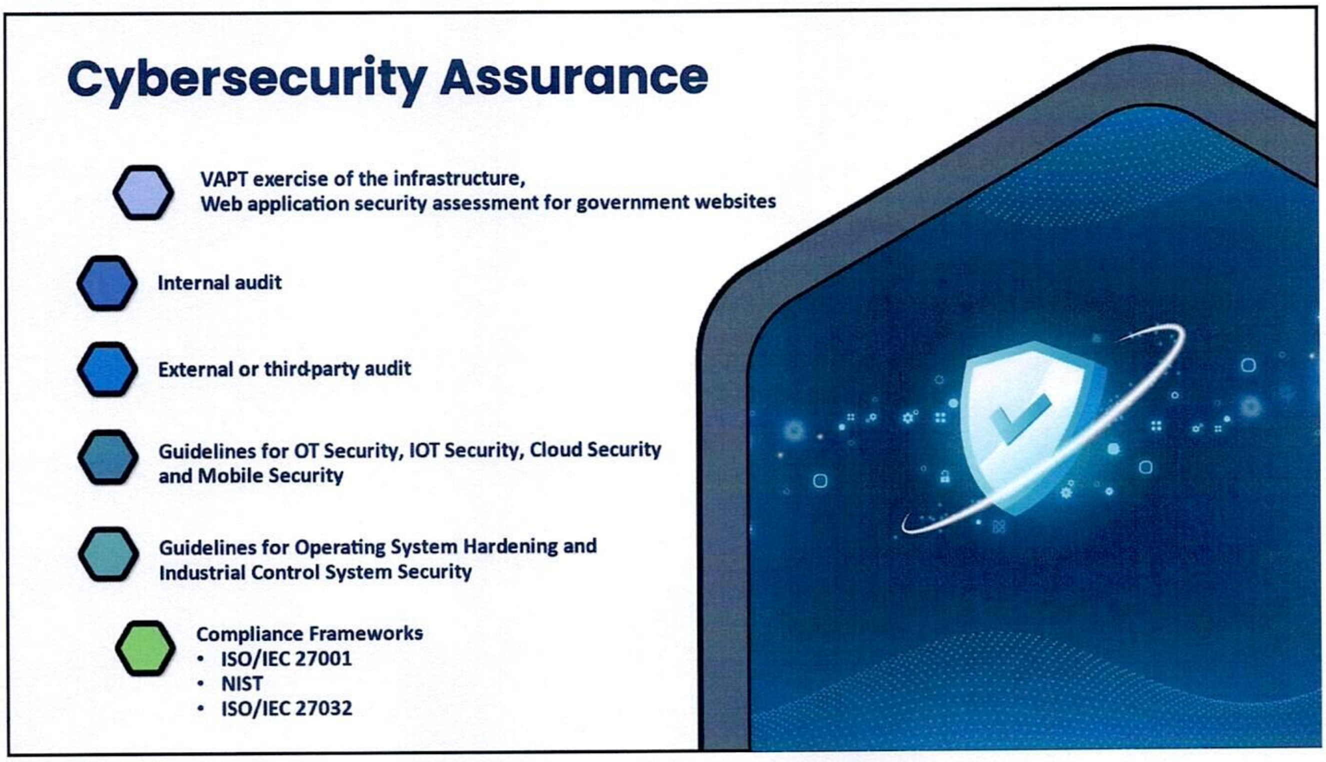
Websites (GIGW), Digital Personal Data Protection Act 2023 (DPDBA) and Secure Application Development Framework.

The state will work to get this approved by **CERT-In** and then circulate the same to different government departments within the state and also at the national level.

I. **Software Bill of Materials (SBOM)**: The state should make it compulsory to submit the Software Bill of Materials (SBOM) at the completion of every development project. Software Bill of Materials(SBOM)is a list of all the components (open source/ proprietary/ third-party libraries) used or present in a codebase. It also lists the licenses that govern those components including the versions of the components.It helps to quickly identify the vulnerabilities that exist inside the components and their patch status and also helps to identify any other associated security or license risks.

Pillar 2: Cyber Security Assurance

The Cyber Security Risk Assurance includes assessing and confirming the security of ICT Infrastructure Resources which includes hardware, websites and other online resources, applications, tools and software, telecommunications, automation and business communication resources and IT Services.



Cybersecurity Assurance

- VAPT exercise of the infrastructure,
  Web application security assessment for government websites
- Internal audit
- External or third-party audit
- Guidelines for OT Security, IOT Security, Cloud Security and Mobile Security
- Guidelines for Operating System Hardening and Industrial Control System Security
- Compliance Frameworks
  - ISO/IEC 27001
  - NIST
  - ISO/IEC 27032

Diagram 2: Cyber Assurance and Compliance

Web Application Security Assessment and VAPT Exercises:

- Web Application Security Assessment and Vulnerability Assessment should be conducted regularly for all websites and portals of different government departments for different software vulnerabilities.
- To check the exploitability of the vulnerabilities Penetration Testing of the Websites and portals should be performed.
- For all Operating Systems and required software, VAPT should be conducted at agreed intervals.
- For OS and Software regular patch updates should be done on a chosen interval and for all the devices firmware upgrades should be done.

Third-Party Audit:

A thorough Cyber Security Audit by any third-party auditor should be conducted to identify the risks associated with the systems, processes of the state infrastructure and verify the efficiency of the mitigation measures. For the same, an Auditor Firm who is well recognized and has a good reputation in the industry should be assigned.

Conducting Third-Party Cyber Security Audits has various benefits for an organization-

- It provides a fresh and unbiased perspective on the security strengths and weaknesses of the organization.
- They help to comply with the industry standards and regulations. To achieve the certification of any well-known cyber security standard or framework like ISO27001 or NIST, a third-party audit is mandatory.
- Conducting third-party audits and compliance with renowned industry standards, assuring all the stakeholders about security, transparency, and best practices.

Internal Audit:

- The state government should conduct an Internal Audit of the public ICT infrastructure of the stateonspecific agreed intervalsi.e.,annually, or half-yearly by an independent team within the government and appointed by the appropriate authorities.
- The Internal Audit team, which is an independent team from the same body or organization, does a holistic review of the security measures and performance. Internal audits should play an integral role in assessing and identifying opportunities to strengthen enterprise security.
- Before going for any external or third-party audit, conducting an internal audit is a wise decision.

Compliance Frameworks:

Compliance with well-known Cyber security frameworks or standards recognized globally is important for any organization. It helps to understand the ideal practices followed at the international level for Cyber security risk management, helps to understand the gaps in the current practices and to identify the areas that need focus.

ISO/IEC 27001:2022 Framework:

ISO/IEC 27001:2022 is a very popular international framework for Information Security and it talks about the Information Security Risk Management Process (ISMS) of the organization which has multiple steps like identifying the assets of the organization and their respective criticalities, then in the next step deciding the threats and vulnerabilities concerning those assets and thirdly documenting the risks based on the previous details found and generating the risk score based on their impact and probability. Italso suggests the required controls to mitigate the risks and assess the efficacy of the existing controls.

NIST Cyber Security Framework:

Drafted by the National Institute of Standards and Technology (NIST), this framework addresses the lack of standards when it comes to cyber security and provides a uniform set of rules, guidelines, and standards for organizations to use across industries. It is a very well-known standard when it comes to Cyber Security having the following five core functions- Identify, Protect, Detect, Respond and Recover.

ISO/IEC 27032 Framework:

The ISO/IEC 27032 standard is about 'Cyber security' or 'Internet Security'. The updated 2023 version emphasizes the term Internet Security. Cyber security is defined as the protection of privacy, integrity, and accessibility of data information in the Cyberspace or Internet

The state government should make its public ICT environment compliant with the three widely known Cyber security frameworks mentioned above to standardize the systems and processes and to increase trust and transparency.

Guidelines for Hardening of Operating Systems:

The state should take the initiative to conduct Operating System Hardening regularly for all the computer systems in the government departments. The hardening guideline should take care of Baseline Configuration, Patch Management,User Account Management, Access Control, Authentication and Authorization, provisions of Security Policies, Backup and Recovery support etc. It should mention all the parameters of the Operating System which need to be hardened.

Guidelines for OT Security, IOT Security, Cloud Security and Mobile Security:

Operational Technology (OT) devices are hardware and software to control and monitor the infrastructure, devices and processes that are not connected to the internet. On the other hand, **IoT devices** are interconnected and create a smart system to seamlessly control various processes and tasks. Also, most organizations are migrating to the cloud rather than having anon-premises architecture for its inherent advantages.

The state government prepare defined guidelines for OT Security, IOT Security, Cloud Security and Mobile Security to ensure the secure use of these technologies.

Guidelines for Industrial Control System Security (ICS):

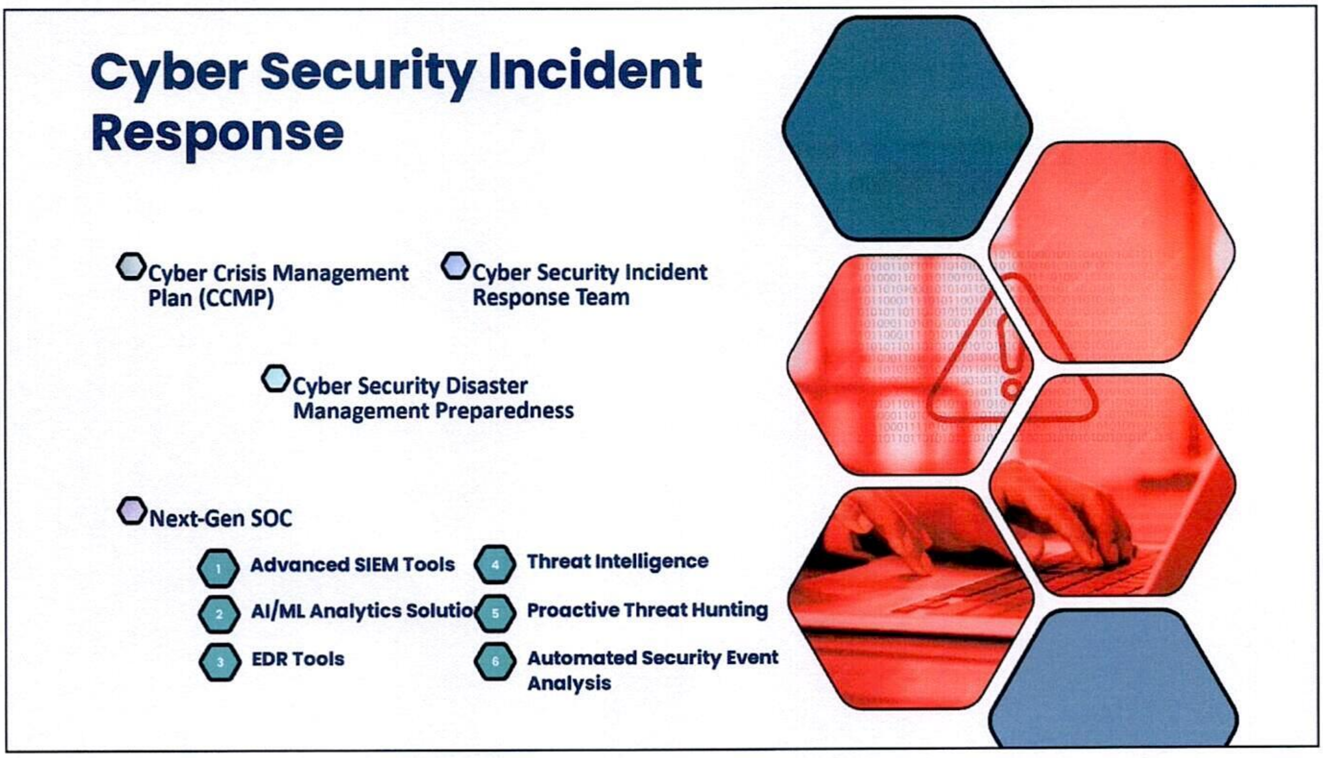
Industrial Control System includes a wide range of systems sometimes referred to as "factory automation" or "distributed control systems", and typically includes DCS, SCADA, and IIOT. To secure the use of its proper security guidelines should be created. Target beneficiaries include Govt. Sectors, Private Sectors, PSUs, Banking and Financial Institutions of West Bengal.

WBEIDC Ltd. will act as the State Level Nodal Agency (SLNA) & State Implementing Agency (SIA)for all activities related to West Bengal Cyber Security. It will be responsible for translating the strategies/policies into actionable plans, managing the implementation of Cyber security solutions, incident response, and ensuring the security of critical information infrastructure within the state.

Pillar 3: Cyber Security Incident Response Strategy

Cyber Security Incident Response indicates how an organization reacts when becomes aware of a cyber security incident. First, it should be confirmed if the attacker is successful in conducting the attack and if any data breach has happened. The next course of action of the Incident Response team will depend on various factors if the attacker was able to compromise any system within the enterprise network and moved laterally to other systems if it was able to escalate its privilege, it has compromised any critical resource like Database Server or Active Directory If it has exploited any particular service of the system etc.

To effectively deal with Cyber Incidents these days most organizations have a Security Operation Center (SOC) and a dedicated Incident Response Team.



Cyber Security Incident Response

- Cyber Crisis Management Plan (CCMP)
- Cyber Security Incident Response Team
- Cyber Security Disaster Management Preparedness
- Next-Gen SOC

1. Advanced SIEM Tools
2. AI/ML Analytics Solutio
3. EDR Tools
4. Threat Intelligence
5. Proactive Threat Hunting
6. Automated Security Event Analysis

Diagram 3: Cyber Security Incident Response Strategy

Security Operation Centre:

Security Operations Center (SOC) generally indicates a team of IT security professionals responsible for monitoring an organization's entire IT infrastructure 24/7 to detect Cyber security events in real-time and respond promptly. The SOC manages the organization's Cyber security technologies, conducts continuous threat analysis, and strives to enhance the overall security posture.

Consolidation of all the Security Tools and Perimeter Devices: The key advantage of having a SOC lies in the consolidation and coordination of an organization's security tools, practices, and incident response.

Accelerated Threat Identification and Response: This integration typically leads to better preventative measures and security policies, accelerated threat identification, and a more efficient and cost-effective response to security threats.

Currently, the state has its own State Data Centre (SDC) where the physical hardware resources of all the Government websites and web resources are hosted. There is currently one SOC operating which monitors the servers, network, and perimeter devices for the State Data Centre for any security Threat.

Also, the state is currently working on a project to build a combined and more advanced SOC, which will monitor all the resources in the Primary State Data Centre and also the newly inaugurated Disaster Recovery Data Centre at Purulia and other proposed Data Centers at different locations.

Next-Generation SOC:

The traditional SIEM tools have evolved now and the Next Generation SOCs give more emphasis to behavioral analytics than having only static rules for threat detection.

Features that Next-Gen SOC should have-

- The Next-Gen SOC will not work as a stand-alone tool, instead **it should be closely connected to the entire security architecture i.e. the central repository of the security logs** which in many organizations called **'The Data Lake'**, should be capable of leveraging technologies like Big Data in its underlying processor to process and retrieve huge volume of the log data, it should be able to intake high volume of Threat Intelligence data regularly and should analyze and use that for threat detection
- It should have **integration with other security tools Endpoint Detection and Response System (EDR) or Extended Endpoint Detection and Response System (XDR) and SOAR Systems** to automate the entire security operation.
- Next-gen SOC should have **in-build Machine Learning algorithms** to automatically detect anomalies and have capabilities for User Entity Behavior Analytics (UEBA) which can learn the normal behavior

To have an Umbrella SOC for all the Government and Private Organizations of the State:

The state has a plan to build a connected and single gateway network architecture for the entire state infrastructure and to create an **'Umbrella SOC'** that will monitor the network traffic of all the Public, Private and Educational Institutions of the state. As proposed in this, at a later point the internet or intranet traffic of the organizations in the state, either live or legacy must **pass through the next-generation umbrella SOC**.

As we say **Cyber Security is a joint task for the government and private institutions**, instead of having only stand-alone security controls, this initiative will enhance the security of the state infrastructure and taking precautions against major cyber-attacks will be easier.

The new Security Operation center will be supported by **Splunk, Log Ingestion, Searching and Querying Logs**, and Alerting and Notifications at real time situations.

Enforcing a Cyber Crisis Management Plan (CCMP):

West Bengal State Cyber Crisis Management Plan (CCMP) has been created for all Critical Information Infrastructure (CII) assets and operationalized which is in sync with global standards and best practices.

The existing CCMP serves as the foundation for effectively addressing Cyber security incidents. To enhance its efficiency and comprehensiveness**, the Government will develop a standardized template based CCMP,** which will be meticulously crafted to cater to the specific needs of all Critical Information Infrastructure (CII) under the jurisdiction of the Government of West Bengal. This template will be used across **all Critical Information Infrastructures (CII) under the Government of West Bengal.** The goal is to ensure consistent and effective Cyber security crisis management, tailored to the specific needs of each CII, and in compliance with relevant regulations.

Information Sharing Platform for Data Intrusive Management:

The state will develop an **Information sharing platform for better intrusion management within the state revamping the CyberYoddha portal initiative.** This portal will consolidate diverse data sources, including government alerts, cryptocurrency analyses, court records, publicly available materials and more. This will help analysts identify vulnerabilities, enhance law enforcement and intelligence efforts, and facilitate a better understanding of cybercriminal groups. It ultimately aims to combat cybercrime more effectively and reduce its economic impact while promoting the continued growth of online services.

West Bengal Cyber Security Incident Response Team (WB-CSIRT):

To ensure the security of critical information infrastructure of the State Government, the WB-CSIRT has been set up in West Bengal which shall operate in sync with the Cyber Emergency Response Team- India**(CERT-In).**

- WB-CSIRT primarily ensures Cyber Assurance and Threat Mitigation for IT Infrastructure in government establishments, in consultation with CERT-In and the West Bengal Cyber Security Centre of Excellence **(CS-CoE).**
- WB-CSIRT has its own functional Chief **Information Security Officer (CISO)** and there are other Information Security Officers in place.
- It receives advisories from **NIIPC and CET-In** about the presence of various vulnerabilities in the websites and applications of different government departments and also the vulnerabilities that are present in the infrastructure and ensures their on-time closure.

- Also conducts the ICT Infrastructure Audit of Public Infrastructure and ensures that the gaps which are found in the audit are closed and the recommendations are enforced.
- The West Bengal State Computer Incident Response Team (WBSCIRT) will ensure adequate **ISO/ISTO and IST** officials in all government departments for the execution of emergency measures tohandle cyber security incidents. For this, WBSCIRT will arrange all the necessary training and curriculum for the officials.
- For **Cybercrime management at the district level**, WBCSIRT will be responsible for the identification of officials and organizing essential training programs to ensure that every government department has sufficient ISO/ISTO and IST-qualified personnel.

Mock Drill for Cyber Security Disaster Management Preparedness and Business Continuity:

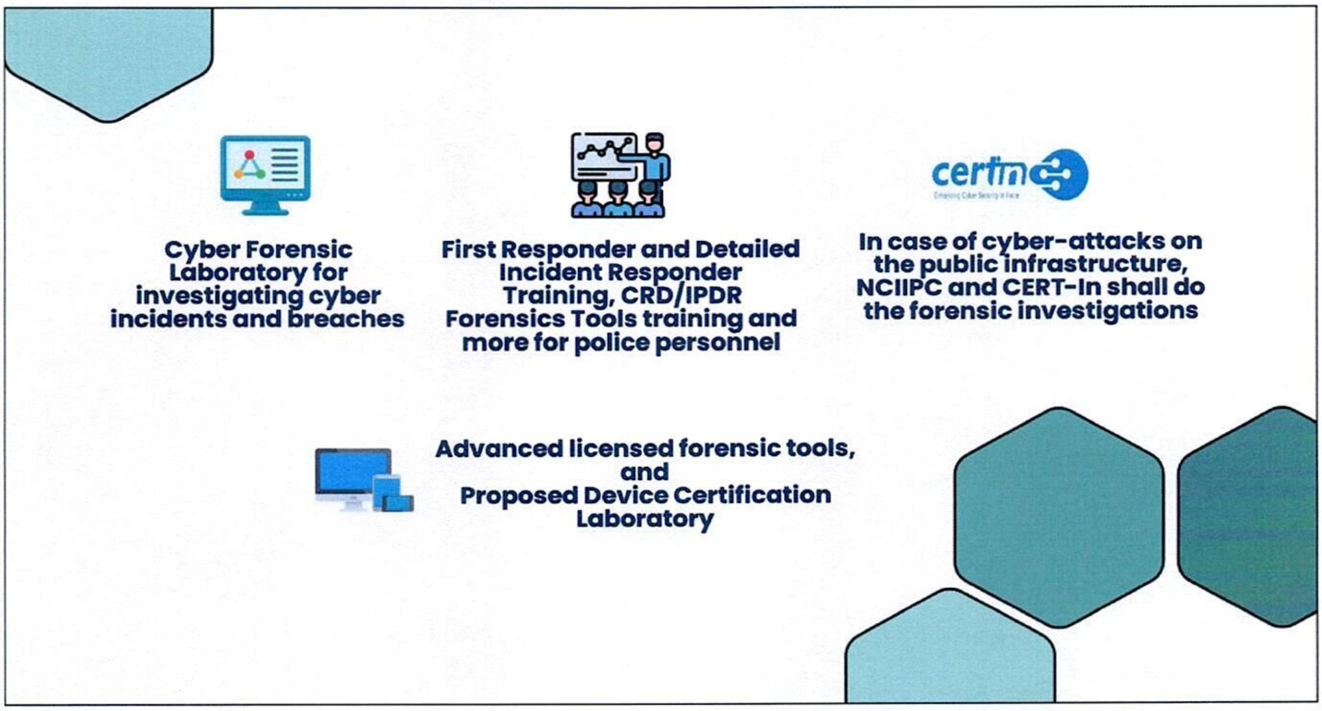
The state should conduct mock drills to check the preparedness for any kind of disaster including the cyber-attacks.

- **Business Continuity Plan:** Business Continuity Plans (BCP) should be created to document the necessary steps and functions in case of a business disruption event like a natural disaster, pandemic, or cyber-attack. BCP identifies the most crucial or essential functions of the business or organization and decides which systems and processes must be sustained and how to achieve them.
- **Disaster Recovery:** Also, generally the critical Infrastructure of the organization and data is replicated at another location which is called Disaster Recovery (DR) so that the entire operation can be switched to that location in case operation at the primary location is disrupted and the required data backup is also available.

In the Mock Business Continuity Drill exercise, it is checked if the steps mentioned in BCP can be followed with synchronization among all the teams. Once the BCP is documented it should be shared with all government departments and for each department Mock BCP Drill should be conducted periodically.

Pillar 4: Investigation and Forensic

Post Incident Response Initiatives: Enforcing Cyber Forensics as a part of Cyber Strategy:



Cyber Forensic Laboratory for investigating cyber incidents and breaches

First Responder and Detailed Incident Responder Training, CRD/IPDR Forensics Tools training and more for police personnel

In case of cyber-attacks on the public infrastructure, NCIIPC and CERT-In shall do the forensic investigations

Advanced licensed forensic tools, and
Proposed Device Certification Laboratory

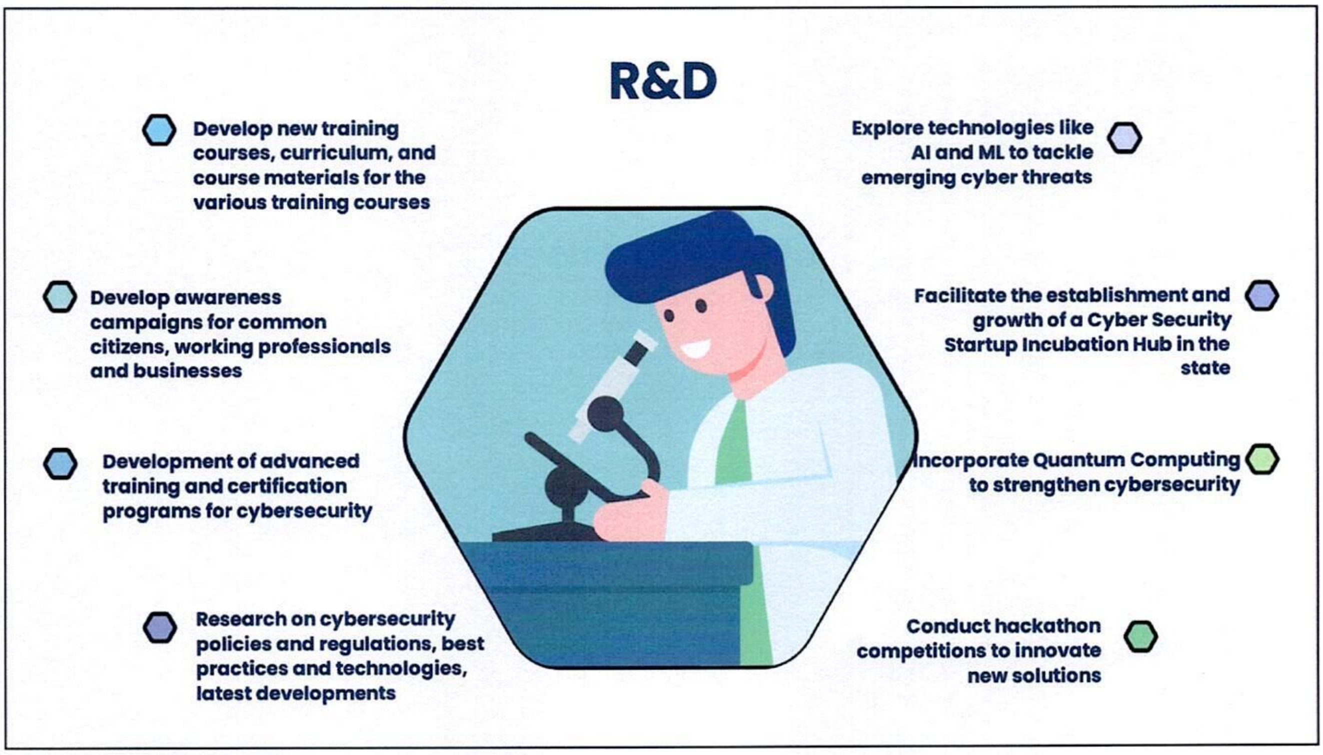
Diagram 4: Investigation and Forensic

A Cyber Forensic Laboratory for investigating cyber incidents and breaches has already been set up in the state and currently doing its operations. The Crime Investigation Department (CID) also has a Forensic Laboratory.

- In case of a Cyber Crime Police should be doing the required forensic investigation. They should be supported with the help of advanced training. Currently, the state conducts training like First and Detailed Incident Responder Training, CRD/IPDR Forensics Tools training and more for police personnel.
- In case of cyber-attacks on the public infrastructure, NCIIPC and CERT-In should do the forensic investing ations.
- Currently, the state has taken the initiative to augment the forensic laboratory with more advanced licensed forensic tools.
- Also, currently work is going on for a proposed Device Certification Laboratory.

Pillar 5: Research and Development (R&D)

Research and Development (R&D) plays a critical role in advancing the state's Cyber security capabilities and staying ahead of evolving cyber threats. The Research and Development effort will support all the other four pillars in terms of advancing knowledge, developing new products and technologies, and improving existing ones.



R&D

Develop new training courses, curriculum, and course materials for the various training courses

Develop awareness campaigns for common citizens, working professionals and businesses

Development of advanced training and certification programs for cybersecurity

Research on cybersecurity policies and regulations, best practices and technologies, latest developments

Explore technologies like AI and ML to tackle emerging cyber threats

Facilitate the establishment and growth of a Cyber Security Startup Incubation Hub in the state

Incorporate Quantum Computing to strengthen cybersecurity

Conduct hackathon competitions to innovate new solutions

Diagram 5: Research and Development Initiatives

The R&D will support the overall cyber strategy in the following ways-

- Develop new training courses, curriculum, and course materials for the various training courses.
- Develop and test Cyber security awareness campaigns for common citizens, working professionals and businesses.
- R&D will support the development of advanced training and certification programs for Cyber security professionals.
- Support the development of ethical hacking challenges and CTF competitions, which will serve as training grounds for individuals interested in Cyber security.
- R&D will contribute to research on Cyber security policies and regulations, helping to shape effective laws and standards that encourage Cyber security awareness and compliance.
-

- Explore technologies **like AI and ML to analyse emerging cyber threats**, understand the threat landscape, and facilitate and expedite detection and responses to cyber-attacks.
- R&D will help identify vulnerabilities in critical infrastructure, government systems, and public services.
- Support the development of cutting-edge security tools and technologies for incident detection, analysis, and response.
- Explore best practices and technologies for preserving digital evidence in a manner that ensures its integrity and admissibility in legal proceedings.
- Focus on the development of advanced digital forensic tools and techniques for data recovery, evidence collection, and analysis.
- Enhance data recovery and reconstruction techniques to piece together digital evidence from damaged or compromised systems.
- Facilitate the establishment and growth of a **Cyber Security Start-up Incubation Hub** in the state that will foster innovation, entrepreneurship, and the development of new Cyber security products and services.
- Conduct **hackathon competitions** to encourage collaboration, innovate new solutions, identify talent and promote awareness.

Incorporate quantum computing to strengthen cybersecurity:

The experts are predicting that the recent advancement of Quantum Computing is going bring some drastic changes in many fields as well in the computing and software industry and the conventional methods used for the cyber security measures will no longer be valid. Very complex models or problems that depend on many parameters like- financial analytics, and cryptographic algorithms can be easily solved with the help of Quantum computers. Some critical impacts of the same will be

Making Asymmetric Cryptography Obsolete: Once Quantum Computing reaches its maturity level, most of the asymmetric cryptography methods like RSA, and Diffie-Hellman (DH) will become unsafe, and the data can be decrypted.

Render blockchain technology and cryptocurrencies vulnerable: The block chain technology depends on public-key cryptography for its function, which can be exploited and decrypted using quantum computing. This study has made the information preserved using blockchain technology and cryptocurrencies i.e., twenty-five percent of all Bitcoins and sixty-five percent of 'Ether — the tokens in the Ethereum network' vulnerable.

Research works on Quantum Computing should be supported: For the reasons mentioned above the state should encourage and support research works on quantum-resistant algorithms and requirements for critical infrastructure based on post-quantum cryptography selections.

Definitions:

Term	Meaning
Vulnerability	A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Risk	The probability of exposure or loss resulting from a cyber-attack or data breach on your organization. Cyber security Risk depends on the probability of a threat exploiting any particular vulnerability and also the impact of that event.
Compliance Framework	Compliance and regulatory frameworks are sets of guidelines and best practices. Organizations follow these guidelines to meet regulatory requirements, improve processes, strengthen security, and achieve other business objectives.
Security Guidelines	Guidelines detailed step-by-step documentation for the implementation of a particular policy.
Cyber security Strategy	A Cyber security strategy is a high-level plan for how your organization will secure its assets during a pre-defined period.

References:

1. ET CISO.in, The SOC of Tomorrow from https://ciso.economictimes.indiatimes.com/soc-of-tomorrow
2. Robert Burns (February 22, 2023), The Cyber security implications of quantum computing, Security Infowatch.com, URL-https://www.securityinfowatch.com/Cyber security/information-security/managed-network-security/article/53012965/the-Cyber security-implications-of-quantum-computing
3. IT Governance, ISO/IEC 27001:2022 and ISO/IEC 27002:2022: Key Updates and Insights, URL-https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates
4. National Institute of Standard and Technology, NIST Cyber security Framework version 1.1, https://www.nist.gov/cyberframework
5. ISO.org, ISO/IEC 27032:2023- Cyber security Guidelines for Internet security, URL-https://www.iso.org/standard/76070.html

Document Owner:

Shri Sanjay Kumar Das, WBCS(Executive),
Additional Secretary,
Dept of IT & Electronics, Govt of West Bengal, Webel
Bhawan Complex, Moni Bhandar,
Block EP & GP, Sector- V,

Salt Lake, Kolkata- 700091

Email: adlsit@wb.gov.in