साइबर सुरक्षा ढाँचे की प्रयोज्यता

नेशनल इंस्टिट्यूट ऑफ स्टैंडर्ड्स एंड टेक्नोलॉजी (एनआईएसटी) के अनुसार, साइबर सुरक्षा के महत्वपूर्ण ढाँचे में बेहतरी के लिए, साइबर सुरक्षा ढाँचे के विभिन्न उप-अध्यायों की प्रयोज्यता निम्नानुसार है:

1. चिह्नित करना (आईडी)
2. सुरक्षा (पीआर)
3. पता लगाना (डीई)
4. प्रतिक्रिया (आरएस)
5. पुनर्प्राप्ति (आरसी)

इनके अलावा, ऐसे कुछ नियंत्रणात्मक उपाय हैं, जिनकी दूरस्थ स्थान से कार्य एवं सूचना प्रौद्योगिकी (इन्टरमीडियरी गाइडलाइंस एंड डिजिटल मीडिया ईथिक्स कोड) नियम, 2021 (आईजीडीएम) के एक अंश के मूल्यांकन के लिए आवश्यकता होती है।
इनके अधीन आने वाली संस्थाएँ हैं:

1. बीमाकर्ता (जीवन, गैर-जीवन, स्वास्थ्य, पुनर्बीमाकर्ता एवं विदेशी पुनर्बीमाकर्ता शाखाएँ)
2. मध्यस्थ (दलाल)
3. निगमित एजेंट
4. वेब एग्रिगेटर्स
5. तृतीय पक्ष प्रशासक
6. बीमा विपणन फर्में (आईएमएफ)
7. बीमा संग्राहक
8. बीमा सूचना ब्यूरो (आईआईबी)
9. निगमित सर्वेक्षक
10. बीमा स्व-नेटवर्किंग पोर्टल (आईएसएनपी)
11. मोटर बीमा सेवा प्रदाता (एमआईएसपी)
12. सामान्य सेवा केन्द्र (सीएससी)

आईआरडीएआई विनियमित संस्थाएँ, जिन पर साइबर सुरक्षा ढाँचा प्रयोज्य है, उनके लिए एनआईएसटी साइबर सुरक्षा ढाँचे की विभिन्न श्रेणियाँ:

सारणी 1

श्रेणी	प्रयोज्यता
1. बीमाकर्ता (जीवन, गैर-जीवन, स्वास्थ्य, पुनर्बीमाकर्ता एवं विदेशी पुनर्बीमाकर्ता शाखाएँ)	सभी उप-अध्याय (आईडी, पीआर, डीई, आरएस, आरसी एवं डबल्यूएफआरएल)
2. मध्यस्थ (दलाल)	
3. निगमित एजेंट	

4. वेब एग्रिगेटर्स	निम्नांकित सारणी देखें
5. तृतीय पक्ष प्रशासक	
6. बीमा विपणन फर्में (आईएमएफ)	
7. बीमा संग्राहक	
8. बीमा सूचना ब्यूरो (आईआईबी)	
9. निगमित सर्वेक्षक	
10. बीमा स्व-नेटवर्किंग पोर्टल	
11. मोटर बीमा सेवा प्रदाता	
12. सामान्य सेवा केन्द्र	

उपरोक्त सूचित 2-12 संस्थाएँ बीमाककर्ता की प्रणाली में पहुँच के आधार पर वर्गीकृत हैं:

सारणी 2

श्रेणी	प्रयोज्यता
क. ऐसी संस्थाएँ, जिन्हें बीमाकर्ता की प्रणाली में जाकर डाटा को देखने, प्रस्तावों को प्राप्त करने, रिपोर्टों को डाउनलोड करने आदि के लिए पहुँच प्राप्त हो (3य पक्ष डाटा को अपलोड करने अथवा डाटा का सम्पादन करने में सक्षम नहीं होना चाहिए, पर, वे उत्पादों/प्रस्तावों /दस्तावेजों/रिपोर्टों को केवल देख सकेंगे)।	पीआर उप-अध्याय
ख. तृतीय पक्ष वो हैं जो कि: 1. ऑटोमेटेड इन्टरफेस [एप्लिकेशन प्रोग्रामिंग इन्टरफेसेस (एपीआई), इलेक्ट्रॉनिक डाटा इन्टरचेंज (ईडीआई) आदि] के द्वारा बीमाकर्ता की प्रणाली से जुड़े हों। 2. बीमाकर्ताओं के लिए डाटा की प्रोसेसिंग या तो तृतीय पक्ष की प्रणालियों अथवा बीमाकर्ता की अपनी प्रणालियों द्वारा करते हों। 3. बीमाकर्ता की प्रणालियों में या तो दूरस्थ प्रकार से अथवा <u>बीमाकर्ता द्वारा नियंत्रित वातावरण में</u> ही डाटा एवं प्रणालियों का सम्पादन करने हेतु पहुँच रखते हों।	सभी उप-अध्याय (आईडी, पीआर, डीई, आरएस, आरसी एवं डबल्यूएफआरएल), जहाँ बीमाकर्ता <u>अपनी नियंत्रित सुविधाओं के अंदर से ही</u> कार्य करते हैं। जिन खंडों की "प्रयोज्य नहीं बनाए जाने" की आवश्यकता हो, उन्हें बीमाकर्ता के बोर्ड द्वारा अनुमोदित किया जाएगा।
ग. ऐसी संस्थाएँ जो कि डाटा को अपलोड करने अथवा पूर्व-निर्धारित प्रारूप (जैसे कि - किसी एक्सेल अथवा टेक्स्ट फाइल, इमेजों, एक्सएमएल आदि) में डाटा को साझा करने हेतु बीमाकर्ता की प्रणालियों से जुड़ी हों। टिप्पणी: बीमाकर्ता को ऐसी अपलोडेड फाइलों को प्रसंस्कृत (प्रोसेस) करना अथवा उनका रिपॉज़िटरी में रख-रखाव करना होगा।	पीआर, डीईई उप-अध्याय

घ. ऐसी संस्थाएँ जो कि पॉलिसीधारकों, निवेशों आदि जैसे बीमाकर्ताओं के डाटा का भंडारण करती हैं (जो कि सार्वजनिक मंच पर उपलब्ध नहीं है)। टिप्पणी: उन्हें बीमाकर्ता की प्रणालियों तक पहुँचने अथवा ऐसे डाटा के सम्पादन अथवा रख-रखाव करने का अधिकार नहीं होगा।	पीआर, डीईई, आरएस उप-अध्याय
ङ. ऐसी संस्थाएँ जो कि केवल भौतिक रूप में ही बीमाकर्ता के डाटा को रखती हैं तथा बीमाकर्ता के डाटा का कोई इलेक्ट्रॉनिक डाटाबेस नहीं रखती हैं अथवा बीमाकर्ता की प्रणालियों तक नहीं जाती हैं।	उप-अध्याय प्रयोज्य नहीं
च. ऐसी संस्थाएँ जो कि एप्लिकेशनों के रख-रखाव, आईटी सहायता सेवाओं आदि जैसी उत्पादन प्रणालियों, डाटाबेस आदि तक पहुँच हेतु बीमाकर्ता की प्रणालियों एवं एप्लिकेशनों को जोड़ती हैं।	सभी उप-अध्याय (आईडी, पीआर, डीई, आरएस, आरसी एवं डबल्यूएफआरएल)

संस्थाओं (उपरोक्त सारणी - 1 में 2 - 12 तक सूचीबद्ध) का वर्गीकरण उनके सकल बीमा राजस्व के आधार पर भी किया जाता है। अत: प्रयोज्य निर्दिष्ट चेकलिस्ट नियंत्रण के बारे में उपरोक्त अध्यायों के अनुलग्नक-II से संदर्भ लें।

APPLICABILITY OF CYBERSECURITY FRAMEWORK

The applicability of different Sub Chapters in Cybersecurity Framework as per National Institute of Standards and Technology (NIST) in respect of Framework for Improving Critical Infrastructure Cybersecurity are as under:

1. Identify (ID)
2. Protect (PR)
3. Detect (DE)
4. Respond (RS)
5. Recover (RC)

Additionally, there are some controls that are required to be evaluated as part of a work from remote location (WFRL) and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM).

The entities which are to be covered are as under:

1. Insurers (Life, Non-Life, Health, Re-insurer and Foreign Re-Insurance Branches)
2. Brokers
3. Corporate Agents
4. Web Aggregators
5. Third Party Administrators
6. Insurance Marketing Firms (IMFs)
7. Insurance Repositories
8. Insurance Information Bureau (IIB)
9. Corporate Surveyors
10. Insurance Self-Networking Portal (ISNP)
11. Motor Insurance Service Provider (MISP)
12. Common Service Centres (CSC)

The various Categories of NIST Cyber Security Framework for IRDAI Regulated Entities to whom the Cybersecurity framework is applicable:

Table 1

Category	Applicability
1. Insurers (Life, Non-Life, Health, Re-insurer and Foreign Re-Insurance Branches)	All Sub-Chapters (ID, PR, DE, RS, RC and WFRL)
2. Brokers	See Table Below
3. Corporate Agents	
4. Web Aggregators	
5. Third Party Administrators	
6. Insurance Marketing Firms (IMFs)	
7. Insurance Repositories	
8. Insurance Information Bureau (IIB)	
9. Corporate Surveyors	
10. Insurance Self Networking Portal	
11. Motor Insurance Service Provider	
12. Common Service Centres	

The entities listed 2-12 above are classified as under based on access to Insurer's Systems:

Table 2

Category	Applicability
a. Entities having access to Insurer's internal systems to view data, get proposals,download reports etc. (3rd party must not be able to upload or edit data, but can only view products / proposals /documents / reports	PR Sub-Chapter
b. 3rd parties who: 1. connect to Insurer systems through automated interfaces [Application Programming Interfaces (APIs), ElectronicData Interchange (EDI) etc.,] 2. do processing of data for Insurers either through 3rd party systems or insurers' own systems. 3. access Insurers' systems either remotely or from within Insurer controlled environment to edit data and systems	All Sub-Chapters (ID, PR, DE, RS, RC and WFRL). Where, Insurers operate from within their controlled facility, sections that need "not be made applicable", shall be approved by the Board of the Insurer.
c. Entities connected to Insurer's Systems to upload data or sharing data in predefined formats (such as from an excel or text file, images, xml etc.) Note: The Insurer must process such uploaded files or maintain in its repository.	PR, DE Sub-Chapters
d. Entities which store Insurer's data (which is not in public domain) as those relating to Policyholders, investment etc. Note: They do not have right to access insurer systems to edit or maintain such data	PR, DE, RS Sub-Chapters
e. Entities which retain only insurer data in physical forms and do not hold any electronic database of the insurers' data ordo not access insurer systems	Sub-Chapters not applicable
f. Entities which connect insurers' systems and applications to access production systems, database etc. such as Application Maintenance, IT Support services etc.,	All Sub-Chapters (ID, PR, DE, RS, RC and WFRL).

The entities (listed 2 - 12 in the Table - 1 above) are further classified on the basis of gross insurance revenue. The specific checklist controls applicable therefore should be read from Annexure-II within the chapters indicated above.