

IFSEC India Awards 2026
Application form: Cybersecurity Leader of the Year (CISO)

AWARD CATEGORY	DESCRIPTION
Cybersecurity Leader of the Year (CISO)	Recognises a senior cybersecurity leader (CISO or equivalent) with at least 10 years of industry experience who has demonstrated excellence in safeguarding digital assets, information systems and cyber resilience.
ELIGIBILITY CRITERIA	
1. The nominee must be a CISO or equivalent senior cybersecurity leader with at least 10 years of industry experience as of 31 March 2026. 2. The nominee must have completed at least one year with the organisation being represented in the nomination as of 31 March 2026. 3. The nomination must demonstrate the nominee's relevant contributions, achievements or initiatives delivered during the eligibility period from 1 April 2024 to 31 March 2026. 4. Strategies or initiatives launched earlier may be included where the nomination demonstrates relevant implementation activity or measurable impact during the eligibility period.	

IMPORTANT RULES FOR PARTICIPATION
1. All mandatory fields and questions must be completed. Responses should be relevant to the category and supported by evidence where applicable. 2. Please indicate "Not Applicable" only for non-evaluation fields that do not apply. 3. Information presented for evaluation must relate to the nominee's contribution within the organisation being represented and during the eligibility period, unless expressly stated otherwise. 4. The final eligibility of the nomination is subject to the Terms and Conditions

APPLICANT INFORMATION (FOR CORRESPONDENCE) *			
Applicant/Primary Contact for Correspondence <i>(should be the authorised signatory)</i>		Designation	
Mobile Number		Email ID	

INDIVIDUAL GENERAL INFORMATION*
--

Name of the Nominee (same will appear on the trophy)	
---	--

Gender	☐ Male ☐ Female
Date of Joining the Organisation Being Represented (DD/MM/YYYY)	
Name of the Organisation	
Designation	
Current Role Start Date	(DD/MM/YYYY)
Company Address	
Company Website	
Contact Details	Telephone: Email:
Qualification	
Total Years of Experience in the Industry (as on 31 March 2026)	
Total Years of Experience in Current Organisation (as on 31 March 2026)	
Professional Profile / LinkedIn URL	
Primary Cybersecurity Areas of Responsibility <i>Select all that apply.</i>	☐ Cyber-risk management ☐ Security architecture ☐ Security operations ☐ Identity and access management ☐ Data protection and privacy ☐ Cloud security ☐ Application security ☐ Security engineering

	☐ DevSecOps ☐ Vulnerability management ☐ Threat intelligence ☐ Incident response and recovery ☐ Third-party cyber risk ☐ Governance and compliance ☐ Cyber-awareness and capability development ☐ Other, please specify
--	--

CASE STUDY:

(☐ ANSWER EACH QUESTION IN A MAXIMUM OF 150 WORDS.

☐ RESPONSES SHOULD FOCUS ON THE NOMINEE'S PERSONAL LEADERSHIP, DECISIONS, ACTIONS AND ATTRIBUTABLE CYBER-RELATED OUTCOMES DURING THE ELIGIBILITY PERIOD FROM 1 APRIL 2024 TO 31 MARCH 2026.

☐ CLEARLY DISTINGUISH THE NOMINEE'S CONTRIBUTION FROM ACHIEVEMENTS ATTRIBUTABLE TO THE WIDER ORGANISATION, OTHER TEAMS, TECHNOLOGY VENDORS OR CONSULTANTS.

☐ SUPPORT RESPONSES WITH RELEVANT EXAMPLES AND EVIDENCE.)

1. Describe the most significant cybersecurity strategy, transformation or cyber-risk management initiative led by the nominee during the eligibility period. Explain the cyber risk, business requirement or organisational priority addressed, the nominee's role in setting the direction, and the responsibilities or decisions directly attributable to the nominee

2. Explain how the nominee translated the strategy into implementation. Describe the principal actions taken, resources prioritised, implementation challenges addressed, governance and accountability arrangements, stakeholder engagement, capability-building activities and improvements in cyber-risk management, cyber awareness or incident readiness.

--

3. Demonstrate the cybersecurity and cyber-resilience outcomes attributable to the nominee's leadership during the eligibility period. Provide relevant evidence relating to cyber-risk reduction, security operations, incident management, resilience, compliance, protection of information assets or business continuity, and explain how the nominee's contribution and the reported outcomes were validated.

--

Please upload supporting documents relevant to the nomination. Each document should not exceed five pages or 5 MB. Only relevant extracts should be submitted.

S No.	Document Name	Description of document	Attachment
1	Individual Profile (CV / Profile highlighting career achievements) *		Upload file
2	Evidence Supporting the Nominee's Cybersecurity Leadership Contributions and Attributable Cyber-resilience Outcomes During the Eligibility Period*		Upload file
3	Awards / Citations / Accolades (if any)		Upload file
4	Any Other Supporting Document (if any)		Upload file

DECLARATION BY THE APPLICANT*

☐ I declare that the information provided in this application is correct and accurate, relates to the nominee and organisation represented in the nomination, and has been submitted with the necessary authorisation. I agree to abide by the applicable rules, terms and conditions of participation. ☐	
Name of Applicant / Authorised Representative	
Designation	
Organisation	
Date	