


Discuss the Chief Financial Regulator Forum Referral and Response

Attachment B

Colton Schulz (ND)



Origin: Chief Financial Regulator Forum – August 2024

Topic: Lack of clear expectations for *Insurance Data Security Model Law* #668 (IDSM) compliance testing

Cybersecurity (H) Working Group Response:

- Acknowledged the need for formal guidance
- Developed two complementary documents

Goals:

- Avoid duplication across and within departments
- Promote regulatory convergence and standardization

Coordinated Oversight & Procedural Recommendations

- MDL #668 compliance testing conducted by a domestic regulator in adopting states
- Shared via regulator-only tools to inform supervisory planning across jurisdictions
- Avoiding Duplication through Coordination
- Training and Awareness developed to help examiners recognize when existing work satisfies compliance objectives

IDSM Compliance Guide

- Gap Analysis as a Core Tool
- Avoiding Duplication through Coordination
- Primary Reliance on Domestic Regulators
- Confidentiality and Infrastructure

Summary of Drafted Documents

IDSM Compliance Guide

- Provides practical tools for domestica regulators to assess IDSM compliance
- Emphasizes gap analysis to align IT reviews with IDSM requirements
- Encourages inter-departmental trust and collaboration
- Includes mapping tools for examiners

Insurance Data Security Model Law #668 – Compliance & Enforcement Guide

Introduction

The Insurance Data Security Model Law #668 (IDSM) provides many requirements of affected licensees. The enforcement of compliance is complicated by other, similar efforts across ~~America's~~ U.S. States' and Territories' departments of insurance, in both their financial and market regulation activities. As such, much of this guidance will focus on the reduction in the risk of duplicative and redundant work while enforcing compliance with the IDSM.

Commented [AV1]: Change made as suggested by SMead
- KS

To reduce duplicative and redundant work foreign regulators should generally ~~trust~~ place reliance on domestic regulators, especially if they have passed a version of the IDSM, to regulate their own market. A method to provide foreign regulators with adequate assurance will leverage Section 4(l) of the IDSM, allowing licensees from IDSM states to avoid duplicative and redundant scrutiny. Additionally, provisions for the work of domestic IT examiners to act in lieu of a specific IDSM examination will be discussed, as well as the performance of a gap analysis to maintain alignment among departments.

Commented [AV2]: Change made as suggested by SMead
- KS

Attached is a flow diagram providing a decision tree (attachment 1). The idea is to create a process by which IDSM compliance is ~~ensured~~ determined by relying on the work done by other ~~divisions~~ departments, where appropriate, but only from other IDSM states. While the work to pass a version of the IDSM in each ~~American~~ jurisdiction is not complete, the final state that this guide envisions is one where each IDSM state enforces ~~their~~ its law on their domestics without the need for additional scrutiny by foreign departments. With all states working together we can create a seamless regulatory environment for our licensees and maximal protection for our consumers.

Commented [AV3]: Change made as suggested by Connecticut

Commented [AV4]: Change made as suggested by SMead
- KS

Commented [AV5]: Change made as suggested by SMead
- KS

Commented [AV6]: Change made as suggested by SMead
- KS

Objective

The foundational element provided in this guidance is that the domestic regulator has multiple tools available to enforce compliance with the IDSM and should be trusted to perform that role. This guidance provides an IDSM compliance review processes for the domestic regulator that focuses on compiling all relevant work and performing a gap analysis between them and the requirements of the IDSM. This approach ensures consistent work across ~~the United States~~ jurisdictions without any duplicative work being performed by examiners.

Commented [AV7]: Change made based on feedback from Joint Trades

Further, using the attestation of compliance to determine a foreign licensee's compliance will allow a more a seamless regulatory environment once the IDSM is passed in all jurisdictions. However, since an accreditation process for IDSM compliance reviews has not yet been agreed upon, a gap analysis is still required to determine if any additional inquiry into the foreign department's area of concern is necessary.

Lastly, ~~department to department~~ collaboration becomes among departments is central to the task of reducing duplicative and redundant work by foreign regulators. By understanding what work was done by the domestic regulator the foreign regulator's requirements may be fully satisfied. Even if this is not the case, ~~in-depth~~ discussion between domestic and foreign regulator will ensure that any action taken by a foreign regulator is properly scoped and planned based on the work done to date.

Commented [AV8]: Changes made as suggested by SMead - KS

Commented [AV9]: Change made as suggested by SMead
- KS

State Collaboration

The IDSM provides a department's Commissioner with broad powers to investigate violations of the IDSM among licensees. This power can be found in the IDSM Section 7, and it applies to all licensees, presuming that there are situations where it is appropriate for a department to perform an examination action on a foreign licensee. This guide notes that this situation could result in substantial duplicative and redundant work and should be first approached collaboratively between departments.

It is possible that a department's concerns may have already been addressed by others during ~~their~~ ~~normal~~ ~~its routine~~ regulatory work. One particularly useful document in the hands of the domestic regulator in an IDSM state is the certificate (or affidavit) of compliance required under Section 4(l). For those states who have a mature approach to IDSM regulation, requesting this document may provide all the assurance a foreign regulator requires. This is not possible with New York (to be discussed later), but New York domiciled licensees can, themselves, provide a highly similar ~~document~~ that can be similarly leveraged by a foreign regulator.

For those situations where a foreign regulator requires deeper or additional review from what has already been performed, continued contact is key as the foreign regulator performs a gap analysis. As noted in the introduction, the most obvious source of compliance for the IDSM is the IT ~~review~~ Review performed at the beginning of a financial condition examination. However, other efforts by the domestic regulator may also provide IDSM assurances. This will be discussed further in the Practical Guidance.

Among the ways to engage with the requirements of the IDSM, effective communication among departments can provide the most robust defense against duplicative or redundant examination work.

Gap Analysis

The gap analysis references a process where one determines if there are any mismatches or gaps between what is being done and what should be done according to a given standard. The reason this step is required is because while IT Reviews are robust that look deeply into a licensee's IT environment, they are not perfectly aligned with the requirements of the IDSM.

It may be the case that the work done by the IT examiners during a financial condition examination provides everything required for an IDSM ~~review~~ Review. However, since this is not necessarily the case, it is incumbent upon the one performing an IDSM ~~review~~ Review to confirm that there are no gaps between the work done and their state's IDSM.

An important tool in performing a gap analysis is the mapping provided (attachment 2). This will provide the regulator with insight into how to connect Exhibit C to the IDSM, allowing for a shared approach to gap analyses across departments of insurance.

Licensees Regulated Under Health Insurance Portability and Accountability Act (HIPAA)

Section 9(A)(2) of the IDSM discusses HIPAA licensees' their exemption from Section 4 of the IDSM. This document primarily discusses Section 4 compliance and enforcement, which for those licensees who are regulated under HIPAA, does not apply. The reason is because the Department of Health and Human

Commented [AV10]: Change made as suggested by SMead - KS

Commented [AV11]: Change made based on feedback from Joint Trades

Commented [AV12]: Change made as suggested by SMead - KS

Commented [AV13]: Change made as suggested by SMead - KS

Commented [AV14]: Change made as suggested by SMead - KS

Services performs such work while determining compliance with HIPAA, and we expect our affected licensees to maintain such compliance. However, while HIPAA licensees are exempt from the requirements of Section 4, they are expected to provide a separate certificate of compliance (similar to the requirement found in Section 4(I)) certifying HIPAA compliance.

Commented [AV15]: Change made based on feedback from AHIP

Practical Guidance for Domestic Regulators in IDSM States

The primary regulatory authority for a licensee will be its domestic regulator who has a variety of tools available to determine compliance with the IDSM, most commonly the IT Review. During a financial condition examination by a domestic regulator, an IT Review is regularly performed. The IT Review is robust and generally covers all areas of interest to Section 4 of the IDSM. However, the IT Review is currently based on the COBIT framework, with future improvements focused on the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF), not the IDSM. Fortunately, there is a mapping between COBIT and Section 4 of the IDSM (attachment 2), which provides examiners with the necessary context to understand the work that's been completed. That being said, some jurisdictions will allow for other control frameworks beyond Exhibit C and as such, while this guide is framework agnostic, only a mapping between Exhibit C and the IDSM will be provided.

Commented [AV16]: Change made based on feedback from CIS

Another, less common tool, available to the domestic regulator is any target examination where the IT function is explored. Much like with the IT Review, it is expected that a target examination utilizes the current Exhibit C (COBIT based framework), and as such, can also be easily mapped to Section 4 of the IDSM. However, for those examinations that investigate areas of IT through other apertures, like the examination of an enterprise risk management program's operational and cybersecurity risk area, may be more challenging to map and care should be taken while doing so.

Commented [AV17]: Change made as suggested by MP

Commented [AV18]:

A focus for departments enforcing the IDSM is the alignment of efforts across divisions (e.g. market & financial regulation) so that the duplication of procedures does not occur. In general, the requirements set forth in Section 4 of the IDSM can be investigated and enforced effectively during an IT Review, but this may not always be the case. To fully determine compliance if a licensee is compliant with the IDSM, a gap analysis should be performed by the domestic state to ensure all applicable measures are in place. Lastly, the guidance to avoid duplication does not preclude the inclusion of procedures found necessary to investigate any violation of the IDSM (see Section 7), even if similar procedures had been performed during an IT Review or another examination.

Commented [AV19]: Change made as suggested by SMead - KS

Practical Guidance for IDSM States Examining Licensees in Foreign Jurisdictions

There are two categories of licensee of consideration to foreign regulators, those that are domesticated in an IDSM state and those that are not. Those licensees that are domesticated in IDSM states have a unique method by which they can communicate compliance, the annual certification (or affidavit) of compliance required by the IDSM's Section 4(I). Given the robust powers already in possession by the domestic regulator, any foreign regulator interested in the IDSM compliance should request this certification first.

The certification required under Section 4(l) requires extensive documentation of any remedial efforts required for ~~their~~the IT environment. Further, it is important to keep in mind that even if remedial actions are found within the certification, it is incumbent upon the domestic regulator in an IDSM state to manage the remediation ~~what's that's~~ been identified.

Under unusual circumstances, like where a foreign licensee does much of ~~their~~its business in the regulator's state, ~~it is recommended that~~ the two departments should first communicate with each other to avoid redundant efforts. It may be the case that the foreign regulator is best suited to perform the work, but this should be done with the knowledge and agreement of the domestic regulator of any IDSM state. Lastly, if a foreign regulator is performing IDSM examinations or follow up work for the domestic regulator, care should be taken to avoid duplication and ensure that only one regulator is ultimately responsible.

States without an IDSM usually, but not always, lack a unique method by which they can communicate compliance. Consider the outlier, New York, whose cybersecurity regulation, 23 NYCRR 500, which was what the IDSM was based on, contains exactly the kind of certification of compliance under their 500.17(b) as Section 4(l) ~~of the IDSM~~. Given such similarities, this guidance recommends that departments rely on New York's 23 NYCRR 500.17(b) certificate of compliance as they would an IDSM Section 4(l) certificate of compliance. However, there is a wrinkle, because New ~~York led the way, their~~ Confidentiality ~~York's confidentiality~~ responsibilities are not like everyone else's — meaning, you'll have to request the document from the licensee, not the New York Department of Financial Services.

The remaining jurisdictions, however, do not have as comparable of an artefact as does New York. This does not mean that assurance is not being attained, or that work is not being done, further emphasizing the need for communication among departments and for the performance of gap analyses.

At the time of this guide's initial publication, the IDSM has not been adopted across the ~~United States~~ U.S. States' and Territories. As such, consideration for those foreign licensees that are not domesticated in an IDSM state must also consider duplication and redundancy of work. As discussed, domestic regulators have the IT Review that ~~never covers~~ many or all areas required under the IDSM, and outreach among departments may unveil substantial work necessary for IDSM compliance. Further, other states may have their own cybersecurity or privacy laws that, while different than the IDSM, may contain requirements that are suitable. As such, it is important for the foreign regulator to reach out and understand the work done by the domestic regulator before utilizing Section 7 of the IDSM.

Examination Considerations

For those situations where a regulator has determined that an IDSM Review (see Section 7) is required, then the two primary considerations are alignment with existing efforts and the maintenance of confidentiality as required by the IDSM's Section 8. Since an objective of this guidance is to create an environment where the domestic regulator can generally be relied upon to enforce the IDSM among their domestic licensees, the following examination considerations will focus on domestic action. For those rare situations where a foreign regulator from an IDSM state is examining a non-domestic licensee's compliance with their IDSM, coordination with the domestic state to address the situation is the recommended first step.

Commented [AV20]: Change made as suggested by SMead - KS

Commented [AV21]: Change made as suggested by SMead - KS

Commented [AV22]: Change made as suggested by SMead - KS

Commented [AV23]: Change made as suggested by SMead - KS

Commented [AV24]: Change made as suggested by SMead - KS

Commented [AV25]: Change made as suggested by SMead - KS

Commented [AV26]: Change made as suggested by SMead - KS

Commented [AV27]: Change made as suggested by SMead - KS

Commented [AV28]: Change made as suggested by SMead - KS

Commented [AV29]: Change made as suggested by SMead - KS

The first task, alignment with existing efforts, asks the domestic regulator to determine what has already been done prior to developing their work plan. An IDSM Review, should take place only after a gap analysis has been completed. The gap analysis, as previously discussed, should take into consideration all sources of compliance, especially including any IT Review or other examination work with a significant IT element. Careful review by the examiner of this work will prevent any unnecessary procedures. The mapping document provided may also prove helpful in this situation, allowing for a clearer alignment of efforts.

The second task, maintaining confidentiality, is ~~a solved problem, but one whose solution must be implemented. The~~ addressed by the NAIC's ~~TeamMate+~~ exists ~~coordinated examination system existing~~ in a highly secure environment ~~that meet, which meets~~ or exceeds the highest security, confidentiality, and resilience standards in IT. Further, confidentiality and security standards continue when the targeted examination reports are uploaded to the Financial Examination Electronic Tracking System (FEETS). ~~Using~~ Departments of insurance already have significant responsibilities when it comes to confidentiality and ~~leveraging that capability by using~~ the two aforementioned tools will ensure the confidentiality expectation required by Section 8 of the IDSM.

Commented [AV30]: Change made as suggested by SMead - KS

Commented [AV31]: Change made as suggested by SMead - KS

AHIP

On behalf of AHIP, thank you for the opportunity to share some initial feedback on the Draft IDSM Compliance Guide under consideration by the NAIC Cybersecurity (H) Working Group.

AHIP appreciates the NAIC's effort to promote consistent and effective cybersecurity oversight through the Insurance Data Security Model Law (IDSM) Compliance Guide. The guidance provides a good foundation for minimizing duplication through gap analysis and improving coordination across states. However, we encourage continued dialogue to ensure alignment with existing federal healthcare data security laws, particularly HIPAA. As you know, health insurers are already subject to comprehensive privacy, security, and incident response requirements through the HIPAA Security Rule.

To enhance clarity, alignment, and ensure that IDSM implementation is consistent and coordinated with existing oversight, we encourage NAIC and this Working Group to further engage with healthcare stakeholders in the development of future resources for regulators. For health insurance-specific guidance related to the IDSM, we respectfully recommend NAIC consider the following:

1. Safe Harbor for HIPAA-Covered Entities – This recognition of HIPAA compliance provides a basis for streamlined IDSM review.
2. Deference to Existing Federal Oversight – This will increase regulatory efficiency by avoiding duplicating efforts when federal oversight addresses similar controls.
3. HIPAA Crosswalk & Gap Analysis Tools – We recommend the Working Group develop optional templates to help examiners align IDSM sections (such as the Cybersecurity Event Notification requirements of Section 6) with long-standing and proven HIPAA standards and requirements.

Again, thank you again for the opportunity to provide initial feedback and due to the abbreviated comment period, AHIP looks forward to supplementing and/or adjusting this response.

Miranda Creviston Motter, JD

Senior Vice President, State Affairs and Policy

c 202.923.7346

mmotter@ahip.org

AHIP – Guiding Greater Health

601 Pennsylvania Avenue, NW, South Building, Suite 500

Washington, D.C. 20004

ahip.org | [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [Instagram](#)

Written Comments
Submitted by the
Center for Internet Security
August 6, 2025

Regarding the
Referral Response Exposure Notice
Cybersecurity Compliance & Enforcement Guide
of the
NAIC Insurance Data Security Model Law (#668)
By the
Cybersecurity (H) Working Group
National Association of Insurance Commissioners

Introduction

Established in 2000 as an independent nonprofit organization, the mission of the Center for Internet Security (CIS) is to make the connected world a safer place by using open, collaborative deliberation processes to define, share, and sustain security best practices against cyber threats.

These best practices represent the consensus opinion of experts from across the global security community and are freely available to all enterprises. CIS has over a quarter century of success in developing, sharing, and sustaining security best practices, powered by a successful nonprofit business model. For example, CIS was instrumental in establishing the first public guidelines for security hardening of commercial IT systems (now known as CIS Benchmarks) when there was little online security leadership – and CIS is now the world’s largest independent source of security configuration hardening.¹

In addition, CIS is the home of the CIS Critical Security Controls,² (“CIS Controls”), which are the set of internationally recognized, prescriptive, prioritized operational security best practices that form the foundation of essential cyber hygiene providing defense protections that are demonstrated to prevent 80-90% of all known pervasive and dangerous cyberattacks. This data driven research is found within the *CIS Community Defense Model* and uses threat intel as well as known cyberattack techniques to drive the prioritization of the Controls and provide visibility into the defense posture achieved through implementation. To ease implementation of this data-driven guidance the CIS Controls and supporting Safeguards (sub-controls) are organized into Implementation Groups or “IGs.” This set of tactical recommendations are organized in a prioritized manner to support essential cyber hygiene (IG1) and ultimately provides a security roadmap to achieve maturity over time and addresses the most sophisticated threat landscapes as the adopter moves into IG2 and IG3. The IGs are designed based upon the risk profile of an organization and the resources available to them.

The insurance industry needs standardized, prescriptive guidance that ensures consistent compliance while reducing regulatory burden. The CIS Controls provide this foundation while enhancing regulatory oversight. By design, the CIS Controls help implement the goals of the NIST Cy-

¹ For more information about the Center for Internet Security, please see: www.cisecurity.org

² For more information about the CIS Critical Security Controls, please see: <https://www.cisecurity.org/controls>

bersecurity Framework (“NIST CSF”) by providing a clear roadmap for network operators to improve cybersecurity by identifying specific actions to be done in priority order based on the current state of the global cyber threat landscape. What results is the clearest, most definitive blueprint of how to protect an organization from cyberattacks. While the NIST CSF is the *what*--NIST defines the categories of cybersecurity and an organizational view of security risk management, the CIS Controls are the *how*--the prioritized technical pathway to achieve the NIST goals. Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.³

Recommendations

CIS commends the National Association of Insurance Commissioners (NAIC) for seeking to produce a Cybersecurity Compliance & Enforcement Guide of the NAIC Insurance Data Security Model Law (668) (IDSM). And while we believe that the CIS Controls are emerging as the international, de facto minimum standard of information security,⁴ we are *not* recommending that you add the CIS Controls to your proposed standard. Instead, **we respectfully recommend that NAIC not rely on a single framework.**

Discussion

The recommendation not to choose a single framework is particularly important as it allows for flexibility and adaptability in the rapidly evolving field of cybersecurity. Being open to various frameworks supports the gap analysis and workflow recommended by the NAIC compliance and enforcement guide, by allowing organizations to choose the framework that best fits their specific needs, rather than being constrained by a single set of one-size-fits-all approach to security controls. This inclusivity is crucial as it acknowledges the growing trend towards reciprocity and allows organizations that have chosen, or are required to be compliant with, different frameworks to measure compliance. This flexibility is essential for fostering innovation and ensuring that organizations can effectively respond to emerging threats. Further it moves the industry away from creating and having to maintain a set of security controls.

³ NIST Cybersecurity Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC" - Council on Cyber Security (the predecessor organization to CIS for managing the Critical Security Controls): <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

⁴ See Appendix 1, attached to this comment and incorporated by this reference. Appendix 1 is a reproduction of Appendix D of CIS's *Guide to Defining Reasonable Cybersecurity*.

In the United States, there is no national, statutory, cross-sector minimum standard for information security. No national law defines what would be considered reasonable security in matters involving data breaches. The federal and state governments have various statutes, regulations, policies, and case law covering elements of cybersecurity, like data breach notification and data privacy. But all these efforts fail to specify what an organization must do to meet the standard of reasonable cybersecurity. However, 19 American states have recently enacted comprehensive data privacy laws, each requiring all organizations that handle Publicly Identifiable Information (PII) to implement reasonable cybersecurity measures. Unfortunately, what qualifies as reasonable is unclear and often determined by the courts. Without prescriptive technical guidance, companies struggle to determine what constitutes “reasonable” cybersecurity measures. This could also result in regulatory examination variability if state examiners lack standardized assessment criteria.

Recently, however, CIS published its *Guide to Defining Reasonable Cybersecurity*, highlighting several states that are setting examples for identifying what constitutes reasonable cybersecurity. These Safe Harbor laws define the term “reasonable,” but also reference several specific industry standards that qualify as reasonable, including the NIST CSF and the CIS Critical Security Controls. The idea is that states should rely on existing minimum standards instead of reinventing the “reasonableness” standard. This emerging innovation will make America safer and provide a standard that can defend against breach-related litigation, reducing industry-wide legal exposure.

The Financial Services industry points to the Controls as an acceptable cybersecurity resource as cited in the below two examples:

- **Federal Financial Institutions Examination Council**, “FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness,” Aug. 28, 2019. Recommends the Critical Security Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. <https://www.ffiec.gov/press/pr082819.htm>
- **Conference of State Bank Supervisors**, “Cybersecurity 101, A Resource Guide for Bank Executives,” 2017. Recommends use of the Critical Security Controls at 8, 12, 24. https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf

The IDSM encourages leveraging existing regulatory work and performing gap analyses to maintain alignment and reduce redundant scrutiny. By incorporating existing cybersecurity industry frameworks and bolstering the ability of Risk Assessment, the effectiveness of Sections 4(C) and 4(I) can be enhanced. This integration of multiple frameworks allows for a more comprehensive and adaptable approach to cybersecurity compliance. The CIS Controls are mapped to other global policy and data frameworks, to easily demonstrate compliance with other industry standards and provide visibility into any overlap. Those CIS mappings are available at no cost, [here](#).

The integration of the *Guide to Defining Reasonable Cybersecurity* into the IDSM could lead to significant improvements in compliance and enforcement. By promoting the use of multiple cybersecurity frameworks and reducing redundant regulatory efforts, the IDSM can create a more efficient and effective regulatory environment. This approach not only supports the gap analysis and workflow referenced in the NAIC compliance and enforcement guide but also aligns with the industry's trend towards reciprocity and inclusivity. Additionally, or in the alternative, the *Guide to Defining Reasonable Cybersecurity* could be used as training material for the state examiners.

Conclusion

In conclusion, we recommend that NAIC not rely on a single framework. Instead, it should follow the example of the states that are already defining "reasonable" cybersecurity to include several existing industry standards like the NIST CSF and the CIS Controls. For the regulators, utilizing a standardized assessment criteria will reduce regulatory examination complexity, improve harmonization across the state regulated insurance entities, and enhance industry cybersecurity posture.

For the insurance companies, utilizing existing standards like the Implementation Groups (IGs 1,2,3) from the CIS Controls, will provide the business with clear implementation guidance and defensible security standards. And for the consumers this inclusivity will provide a stronger protection of personal information through proven cybersecurity best practices and regulatory oversight.

By following the example of several American states to include multiple industry standards, in-

cluding NIST CSF and CIS Controls, (which represent a solid, data-driven approach to cybersecurity hygiene and maturity that can significantly enhance IDSM #668 implementation) the NAIC can provide regulated insurance entities with the prescriptive guidance and measurability needed for effective cybersecurity program management while maintaining robust consumer protection standards.

We hope that these recommendations help inform the NAIC's ability to support state departments of insurance in their response to notifications of cybersecurity events at regulated insurance entities. Please feel free to contact us if we can answer any questions that you might have or assist you in this important aspect of defending our nation.

Appendix 1

CIS Guide to Defining Reasonable Cybersecurity, Appendix D,
Why the CIS Critical Security Controls are Becoming a Global De Facto Standard

A Guide to Defining Reasonable Cybersecurity



May 2024

Copyright © 2024 Center for Internet Security, Inc.

Why the CIS Critical Security Controls are Becoming a Global De Facto Standard

While there are some limited *policy* standards (e.g., NIST CSF) and industry or *data* standards (e.g., PCI, HIPAA, & ISO), there are no specific *operational* standards across all the economic sectors. The CIS Critical Security Controls are becoming the de facto, global reasonable standard for operational cybersecurity for six compelling reasons.

1 Prescriptive and prioritized by global experts. The CIS Controls, which are regularly compiled by cybersecurity experts around the world, help implement the goals of the NIST CSF by providing a blueprint for network operators to improve cybersecurity by identifying specific, prescriptive actions to be done in priority order based on the current state of the global cyber threat. While the NIST CSF is the *what*—NIST defines the categories of cybersecurity and an organizational view of security risk management—the CIS Controls are devised based on *how* malicious actors attack and are updated regularly. What results is the clearest, most definitive roadmap of how to protect an organization from cyber attacks.

2 Extremely effective and measurable. The CIS Controls are very effective against today's most pervasive attack vectors and this effectiveness has been quantified. CIS's Community Defense Model (CDM) establishes that the CIS Controls mitigate approximately 86% of attack techniques found in the MITRE ATT&CK Framework.²⁵

3 Scalable. The CIS Controls can be tailored by the size of the implementing organization. The CIS Controls introduce the concept of Implementation Groups (IGs), which provide both an onramp for organizations just starting out as well as a roadmap to greater cyber defense maturity by offering three tiers. These IGs tailor the controls to the size and maturity of the implementing organization. Even at the simplest level, IG1, the CIS Controls remain very effective, protecting against 74% of attack vectors identified in the MITRE ATT&CK model.²⁶

4 Cost-effective. Recognizing that cost of implementation is a huge unknown in security programs (especially for small- and medium-enterprises), CIS has been developing tools, models, and working aids to help enterprises understand and manage the cost of their cybersecurity program. For example, the CDM establishes the "security value" of individual practices,²⁷ which assists in priority-setting and also bounds the costing question to specific practices and tools. It also helps enterprises establish the baseline value of technology and practices that they already have. Further, CIS has also published a study to establish how much it will cost an organization to implement effective cybersecurity.²⁸

5 Mapped to other global policy and data frameworks. The CIS Controls are mapped to many existing frameworks.²⁹ Many enterprises must report progress against multiple security frameworks or sets of requirements, and so CIS develops freely available, industry-vetted mappings to and from CIS products to all major security frameworks (like the NIST CSF, NIST 800-53, PCI, etc.) This framework mapping is also available in Appendix F.

6 Widely adopted globally.

- The CIS Critical Security Controls have been downloaded over 400,000 times over the last few years—over half of these by organizations outside the U.S.
- Selected adoption and endorsements of the CIS Critical Security Controls include:
 - **NIST, “Framework for Improving Critical Infrastructure Cybersecurity Framework,” Version 1.1, Apr 16, 2018.** Cites and maps to “CIS CSC” throughout Appendix A, Framework Core at 22-44. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> The “CIS CSC” is a shorthand for the CIS Critical Security Controls, also referred to as the CIS Controls throughout this paper.
 - **Verizon, “DBIR Data Breach Investigations Report,” 2024.** Recommends the CIS Controls and maps them to industry challenges and vulnerabilities. <https://www.verizon.com/business/resources/reports/dbir/>
 - **National Aerospace Standard, NAS9933, Critical Security Controls for Effective Capability in Cyber Defense, Nov. 29, 2018.** Based on the CIS Controls. <https://store.accuristech.com/searches/41316943>
 - **Federal Financial Institutions Examination Council, “FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness,” Aug. 28, 2019.** Recommends the Critical Security Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. <https://www.ffiec.gov/press/pr082819.htm>
 - **Conference of State Bank Supervisors, “Cybersecurity 101, A Resource Guide for Bank Executives,” 2017.** Recommends use of the Critical Security Controls at 8, 12, 24. https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf
 - **FCC Notice of Proposed Rule Making, Dec 2022-Jan 2023):** FCC proposes measures to protect the nation’s critical communications systems from cyber threats by adoption the CISA Cybersecurity Baseline or the CIS Controls. FCC NPRM, No. 22-82, Appendix B, Section E, paragraph 66, page 52: <https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems>
 - **FCC, Communications Security, Reliability and Interoperability Council, CSRIC IV, Working Group 3, “Emergency Alert System (EAS) Initial Security Subcommittee Report,” May 2014.** Recommending CIS Controls (then known as the “SANS 20 Critical Security Controls”) as

part of its recommended Network and Operational Controls. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf

- **FCC, Communications Security, Reliability and Interoperability Council, CISRIC III, Working Group 11, “Consensus Cyber Security Controls Final Report,” March 2013.** This report finds that the “user community within Working Group 11 would prefer for the FCC to encourage industry to use the 20 Controls because they believe that the 20 Controls will protect the network infrastructure directly. The user group also believes that the 20 Controls have been demonstrated to be effective in protecting critical infrastructure from attacks that are likely to come through the enterprise systems and therefore the 20 Controls should be used by the communications industry.” Report at page 8. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013Final.pdf
- **NIST, U.S. Resilience Project, “Best Practices in Cyber Supply Chain Risk Management.”** Boeing’s IS team stated that its “primary standard is the Critical Security Controls.” See at 4. https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf
- **U.S. Department of Transportation, Federal Highway Administration, Transportation Management Center Information Technology Security, Final Report, Sep. 2019.** Critical Security Controls cited throughout as insight into basic practices that serve as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for Traffic Management Centers looking to increase their system maturity. <https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf>
- **State of California, “California Data Breach Report,” Feb. 2016.** Attorney General Kamala Harris’ report warns that failing to implement all relevant Controls in California “constitutes a lack of reasonable security.” The Report effectively constituted a ground-breaking minimum level of information security. See <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>. Subsequent analysis cites the endorsement of the Controls as reasonable security: https://www.littler.com/publication-press/publication/employers-receive-last-minute-relieve-most-onerous-ccpa-compliance?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
- **State of Colorado, Data Security Best Practices.** The Colorado Attorney General Data Security Best Practices guide states that: “While each entity’s data security needs and practices may differ, there are some common best practices that most, if not all covered entities can implement.” The guide recommends the CIS Critical Security Controls as part of Step 2, the written information security policy at 3. <https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf>
- **World Economic Forum (WEF), White Paper, Global Agenda Council on Cybersecurity, World Economic Forum, Apr. 2016.** Listed CIS Controls as the first best practice at 19, CIS cyber hygiene at Appendix A at page 26. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

- **ENISA (European Union Agency for Network and Information Security), “Technical Guidelines for the implementation of minimum security measures for Digital Service Providers,” Dec. 2016.** This document cited the CIS Controls as a means for meeting EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS). See page 10 and mapping throughout. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/at_download/fullReport
- **ETSI (European Telecommunications Standards Institute).** The ETSI transposed all of the CIS Critical Security Controls and Safeguards and associated facilitation mechanisms into formal international specifications for global citation and normative use within the European Union. The CIS Controls were also designated as the means of implementing most of the provisions of the of the original and recently adopted European Union (EU) Revised Network and Information Security (NIS2).
 - ETSI TR 103 305-1: “Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls,” https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/04.01.02_60/tr_10330501v040102p.pdf
 - ETSI TR 103 305-3: “CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations,” https://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/02.01.01_60/tr_10330503v020101p.pdf
 - ETSI TR 103 305-4: “Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms,” https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/02.01.01_60/tr_10330504v020101p.pdf
 - ETSI TR 103 305-5: “Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Part 5: Privacy and personal data protection enhancement,” https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/02.01.01_60/tr_10330505v020101p.pdf
 - ETSI TR 103 456: “CYBER; Implementation of the Network and Information Security (NIS) Directive,” https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
 - ETSI TR 103 866: “Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls,” https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf

CONNECTICUT INSURANCE DEPARTMENT

IDSMD Compliance Guide

Paragraph 3 of the IDSMD Compliance Guide includes:

"Attached is a flow diagram providing a decision tree (attachment 1). The idea is to create process by which IDSMD compliance is ensured by relying on the work done by other divisions, where appropriate, but only from other IDSMD states".

Compliance is Ensured

From a financial examination perspective, we have concerns with the terminology of "IDSMD compliance is ensured".

While conducting a review of data security laws during a financial examination, related control exceptions are noted as well as clear cases of non-compliance. We cannot conclude that "compliance is ensured". As an example, it is usually clear whether a Company has a written incident response program. However, during the review of the section "protect by encryption or other appropriate means, all nonpublic Information", the IT specialist could never say that a Company is encrypting all nonpublic information.

In conclusion, we would suggest utilizing wording that is consistent with what is currently used by IT specialists, noting any exceptions or non-compliance.

Flow Diagram (Attachment 1)

A review of the flow diagram appears to lead to limited scope (target) exams of Section 6 of the Model Law, by both domestic and non-domestic states. We would suggest further clarification of this flowchart with a recommendation that it should be at the discretion of the lead regulator (or non-lead regulators with a domestic in a group after consultation with the lead regulator) whether a limited-scope examination is necessary. We are also unclear of why Section 6 was specifically noted as the only section subject to a limited scope exam.

KANSAS DEPARTMENT OF INSURANCE

Insurance Data Security Model Law #668 – Compliance & Enforcement Guide

Introduction

The Insurance Data Security Model Law #668 (IDSM) provides many requirements of affected licensees. The enforcement of compliance is complicated by other, similar efforts across **America's departments of insurance**, in both their financial and market regulation activities. As such, much of this guidance will focus on the reduction in the risk of duplicative and redundant work while enforcing compliance with the IDSM.

To reduce duplicative and redundant work foreign regulators should generally **trust** domestic regulators, especially if they have passed a version of the IDSM, to regulate their own market. A method to provide foreign regulators with adequate assurance will leverage Section 4(l) of the IDSM, allowing licensees from IDSM states to avoid duplicative and redundant scrutiny. Additionally, provisions for the work of domestic IT examiners to act in lieu of a specific IDSM examination will be discussed, as well as the performance of a gap analysis to maintain alignment among departments.

Attached is a flow diagram providing a decision tree (attachment 1). The idea is to create a process by which IDSM compliance is ensured by relying on the work done by other **divisions**, where appropriate, but only from other IDSM states. While the work to pass a version of the IDSM in each ~~American~~ jurisdiction is not complete, the final state that this guide envisions is one where each IDSM state enforces **their** law on their domestics without the need for additional scrutiny by foreign departments. With all states working together we can create a seamless regulatory environment for our licensees and maximal protection for our consumers.

Objective

The foundational element provided in this guidance is that the domestic regulator has multiple tools available to enforce compliance with the IDSM and should be trusted to perform that role. This guidance provides an IDSM compliance review processes for the domestic regulator that focuses on compiling all relevant work and performing a gap analysis between them and the requirements of the IDSM. This approach ensures consistent work across the United States without any duplicative work being performed by examiners.

Further, using the attestation of compliance to determine a foreign licensee's compliance will allow a more a seamless regulatory environment once the IDSM is passed in all jurisdictions. However, since an accreditation process for IDSM compliance reviews has not yet been agreed upon, a gap analysis is still required to determine if any additional inquiry into the foreign department's area of concern is necessary.

Lastly, **department to department** collaboration becomes central to the task of reducing duplicative and redundant work by foreign regulators. By understanding what work was done by the domestic regulator the foreign regulator's requirements may be fully satisfied. Even if this is not the case, **in depth** discussion between domestic and foreign regulator will ensure that any action taken by a foreign regulator is properly scoped and planned based on the work done to date.

State Collaboration

The IDSM provides a department's Commissioner with broad powers to investigate violations of the IDSM among licensees. This power can be found in the IDSM Section 7, and it applies to all licensees, presuming that there are situations where it is appropriate for a department to perform an examination action on a foreign licensee. This guide notes that this situation could result in substantial duplicative and redundant work and should be first approached collaboratively between departments.

It is possible that a department's concerns may have already been addressed by others during **their normal** regulatory work. One particularly useful document in the hands of the domestic regulator in an IDSM state is the certificate (or affidavit) of compliance required under Section 4(l). For those states who have a mature approach to IDSM regulation, requesting this document may provide all the assurance a foreign regulator requires. This is not possible with New York (to be discussed later), but New York domiciled licensees can, themselves, provide a highly similar document.

For those situations where a foreign regulator requires deeper or additional review from what has already been performed, continued contact is key as the foreign regulator performs a gap analysis. As noted in the introduction, the most obvious source of compliance for the IDSM is the IT **review** performed at the beginning of a financial condition examination. However, other efforts by the domestic regulator may also provide IDSM assurances. This will be discussed further in the Practical Guidance.

Among the ways to engage with the requirements of the IDSM, effective communication among departments can provide the most robust defense against duplicative or redundant examination work.

Gap Analysis

The gap analysis references a process where one determines if there are any mismatches or gaps between what is being done and what should be done according to a given standard. The reason this step is required is because while IT Reviews are robust **that** look deeply into a licensee's IT environment, they are not perfectly aligned with the requirements of the IDSM.

It may be the case that the work done by the IT examiners during a financial condition examination provides everything required for an IDSM **review**. However, since this is not necessarily the case, it is incumbent upon the one performing an IDSM **review** to confirm that there are no gaps between the work done and their state's IDSM.

An important tool in performing a gap analysis is the mapping provided (attachment 2). This will provide the regulator with insight into how to connect Exhibit C to the IDSM, allowing for a shared approach to gap analyses across departments of insurance.

Practical Guidance for Domestic Regulators in IDSM States

The primary regulatory authority for a licensee will be its domestic regulator who has a variety of tools available to determine compliance with the IDSM, most commonly the IT Review. During a financial condition examination by a domestic regulator, an IT Review is regularly performed. The IT Review is robust and generally covers all areas of interest to Section 4 of the IDSM. However, the IT Review is currently based on the COBIT framework, with future improvements focused on the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF), not the IDSM. Fortunately, there is a

mapping between COBIT and Section 4 of the IDSM (attachment 2), which provides examiners with the necessary context to understand the work that's been completed.

Another, less common tool, available to the domestic regulator is any target examination where the IT function is explored. Much like with the IT Review, it is expected that a target examination utilizes the current COBIT framework, and as such, can be easily mapped to Section 4 of the IDSM. However, for those examinations that investigate areas of IT through other apertures, like the examination of an enterprise risk management program's operational and cybersecurity risk area, may be more challenging to map and care should be taken while doing so.

A focus for departments enforcing the IDSM is the alignment of efforts across divisions (e.g. market & financial regulation) so that the duplication of procedures does not occur. In general, the requirements set forth in Section 4 of the IDSM can be investigated and enforced effectively during an IT Review, but this may not always be the case. To fully determine **compliance** with the IDSM, a gap analysis should be performed by the domestic state to ensure all applicable measures are in place. Lastly, the guidance to avoid duplication does not preclude the inclusion of procedures found necessary to investigate any violation of the IDSM (see Section 7), even if similar procedures had been performed during an IT Review or another examination.

Practical Guidance for IDSM States Examining Licensees in Foreign Jurisdictions

There are two categories of licensee of consideration to foreign regulators, those that are domesticated in an IDSM state and those that are not. Those licensees that are domesticated in IDSM states have a unique method by which they can communicate compliance, the annual certification (or affidavit) of compliance required by the IDSM's Section 4(I). Given the robust powers already in possession by the domestic regulator, any foreign regulator interested in the IDSM compliance should request this certification first.

The certification required under Section 4(I) requires extensive documentation of any remedial efforts required for **their** IT environment. Further, it is important to keep in mind that even if remedial actions are found within the certification, it is incumbent upon the domestic regulator in an IDSM state to manage the remediation **what's** been identified.

Under unusual circumstances, like where a foreign licensee does much of **their** business in the regulator's state, ~~it is recommended that~~ the two departments first communicate with each other to avoid redundant efforts. It may be the case that the foreign regulator is best suited to perform the work, but this should be done with the knowledge and agreement of the domestic regulator of any IDSM state. Lastly, if a foreign regulator is performing IDSM examinations or follow up work for the domestic regulator, care should be taken to avoid duplication and ensure that only one regulator is ultimately responsible.

States without an IDSM usually, but not always, lack a unique method by which they can communicate compliance. Consider the outlier, New York, whose cybersecurity regulation, 23 NYCRR 500, which was what the IDSM was based on, contains exactly the kind of certification of compliance under 500.17(b) as Section 4(I). Given such similarities, this guidance recommends that departments rely on New York's 23 NYCRR 500.17(b) certificate of compliance as they would an IDSM Section 4(I) certificate of compliance. However, there is a wrinkle, because **New York led the way, their Confidentiality** responsibilities are not

like everyone else's – meaning you'll have to request the document from the licensee, not the New York Department of Financial Services.

The remaining jurisdictions, however, do not have as comparable ~~of~~ an artefact as does New York. This does not mean that assurance is not being attained, or that work is not being done, further emphasizing the need for communication among departments and for the performance of gap analyses.

At the time of this guide's initial publication, the IDSM has not been adopted across the **United States**. As such, consideration for those foreign licensees that are not domesticated in an IDSM state must consider duplication and redundancy of work. As discussed, domestic regulators have the IT Review that **cover** many or all areas required under the IDSM, and outreach among departments may unveil substantial work necessary for IDSM compliance. Further, other states may have their own cybersecurity or privacy laws that, while different **the** IDSM, may contain requirements that are suitable. As such, it is important for the foreign regulator to reach out and understand the work done by the domestic regulator before utilizing Section 7 of the IDSM.

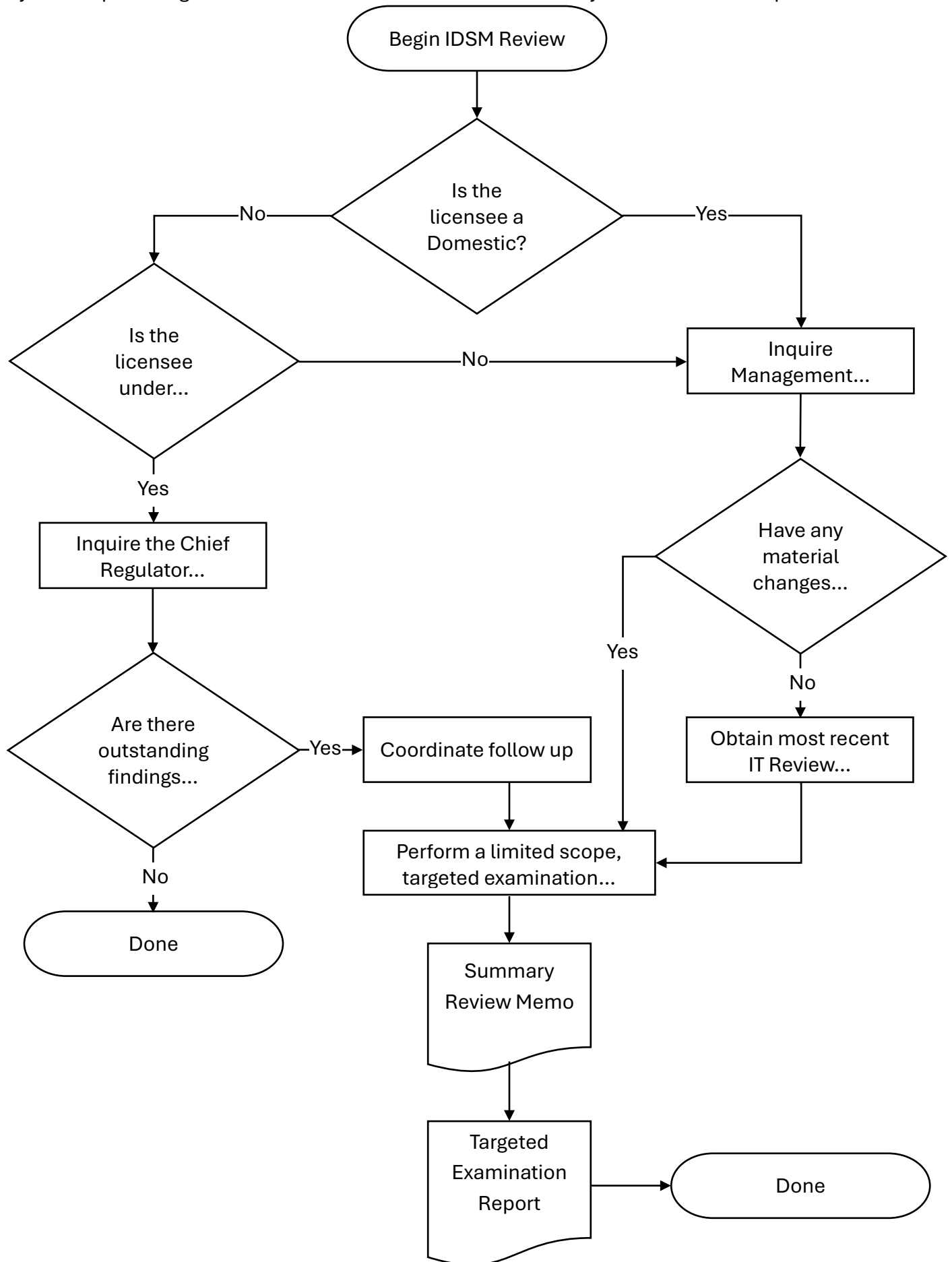
Examination Considerations

For those situations where a regulator has determined that an IDSM Review (see Section 7) is required, then the two primary considerations are alignment with existing efforts and the maintenance of confidentiality as required by the IDSM's Section 8. Since an objective of this guidance is to create an environment where the domestic regulator can generally be relied upon to enforce the IDSM among their domestic licensees, the following examination considerations will focus on domestic action. For those rare situations where a foreign regulator from an IDSM state is examining a non-domestic licensee's compliance with their IDSM, coordination with the domestic state to address the situation is the recommended first step.

The first task, alignment with existing efforts, asks the domestic regulator to determine what has already been done prior to developing their work plan. An IDSM Review, should take place only after a gap analysis has been completed. The gap analysis, as previously discussed, should take into consideration all sources of compliance, especially including any IT Review or other examination work with a significant IT element. Careful review by the examiner of this work will prevent any unnecessary procedures. The mapping document provided may also prove helpful in this situation, allowing for a clearer alignment of efforts.

The second task, maintaining confidentiality, is a solved problem, but one whose solution must be implemented. The NAIC's **TeamMate+** exists in a highly secure environment that **meet or exceeds the highest** security, confidentiality, and resilience standards in IT. Further, confidentiality and security standards continue when the targeted examination reports are uploaded to FEETS. Using the two aforementioned tools will ensure the confidentiality expectation required by Section 8 of the IDSM.

Suggestions: Use the decision symbol to include a question or an evaluation of a condition (but not the possible response) and label each corresponding flowline that exits the decision symbol. Use the document symbol to identify each report. Begin and end the flowchart with a terminator symbol. Crude example below.



August 5, 2025

NAIC Cybersecurity (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106
Via email: khenry@naic.org

RE: *Insurance Data Security Model Law #668 – Compliance & Enforcement Guide*

Dear Chair Peterson and Members of the Cybersecurity (H) Working Group,

On behalf of the American Property Casualty Insurance Association¹ (APCIA), the American Council of Life Insurers² (ACLI), and the National Association of Mutual Insurance Companies³ (NAMIC), we appreciate the opportunity to provide feedback on the exposed *Insurance Data Security Model Law Compliance & Enforcement Guide*. We applaud the NAIC's efforts to promote regulatory coordination and reduce unnecessary duplication in compliance assessments.

We understand that this guide is viewed by the Working Group as inoffensive, easily implemented, and helpful in reducing unneeded inquiry, and that accordingly, a 20-day comment period was deemed sufficient. While this brief window has limited the depth of feedback we are able to offer at this time, we are pleased to share the input we have received thus far from our members in the spirit of collaboration and to support continued progress on this important work.

We particularly appreciate the Working Group's emphasis on reducing redundant regulatory requests, which can divert resources away from the core objective of enhancing cyber resilience. We are also

¹ The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA membership consists of over 1,200 member companies (or over 300 member groups). APCIA member companies P&C countrywide market share is 65% (total 73% commercial lines, 55% personal lines).

² The American Council of Life Insurers is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 275 member companies represent 93 percent of industry assets in the United States.

³ The National Association of Mutual Insurance Companies consists of over 1,300 member companies, including six of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers. NAMIC member companies write \$383 billion in annual premiums and represent 61 percent of homeowners, 48 percent of automobile, and 25 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

encouraged by the guide's recognition of the domestic regulator's lead role in overseeing compliance review.

Below is the feedback we have compiled to date:

1. Clarify When and Why the Guide Should Be Used

The flowchart and compliance guide should clearly indicate that they apply only in instances where the examining state has adopted the NAIC Insurance Data Security Model Law (#668). Without this clarification, the guidance could be interpreted as encouraging non-adopting states to apply standards they have not formally enacted, potentially overstepping state authority. Clarifying this limitation would help preserve state autonomy while supporting consistent and appropriate implementation of the model where it has been adopted.

To avoid creating an unintended expectation that all states should conduct independent compliance assessments, we recommend the document explicitly state that this guidance is intended to support instances when a compliance review is appropriate. It should be made clear that such a review is generally triggered by (1) a financial examination conducted by the domestic state, (2) a market conduct examination, or (3) a specific infraction requiring investigation. While the guidance touches on this in various places, a more prominent explanation at the outset would help frame the appropriate use and scope of this tool. Likewise, we recommend revising the flowchart so that Step One includes identifying whether a regulatory trigger exists at all for a compliance inquiry.

2. Clarify Confidentiality Statement

The statement that "maintaining confidentiality is a solved problem" may inadvertently gloss over important considerations. We encourage the Working Group to expand on what safeguards are expected to ensure confidentiality, particularly in cross-state communication. This could include reference to contractual obligations, MOUs, or other mechanisms that must be in place to preserve the confidentiality of shared cybersecurity information.

3. Domestic Certification and New York's Role

The section on state collaboration correctly notes that reliance on a domestic certification may be sufficient in many cases and we appreciate this recognition. However, the reference to New York appears to suggest that certification from that jurisdiction may be insufficient on its own. We respectfully offer that New York does require a cybersecurity certification from all licensed insurers, not just domestics, and as such, its certification should be equally valid and sufficient for companies licensed in multiple states. Affirming the sufficiency of domestic certifications, including New York's, would further support the objective of reducing redundancy.

4. Clarify Expectations Around Documentation

In reviewing the practical guidance related to Section 4(l), we observed that the current language may be interpreted as suggesting that supporting documentation is required to accompany the certification. To support consistent implementation of the Model Law, we suggest clarifying that documentation is only required upon regulator request. While we appreciate the goal of ensuring transparency, avoiding language that implies a routine filing obligation would help manage expectations and streamline compliance efforts.

5. Request for More Information on Tools Referenced

Lastly, we would welcome additional detail regarding references to NAIC TeamMate+ and FEETS. It would be helpful to understand how these tools are used, their intended audience, and whether insurers or state regulators are expected to engage with them directly in the context of cybersecurity compliance reviews.

Conclusion

We hope these comments are helpful as the Working Group continues its important work. Should the exposure be reopened for additional input, we would welcome the opportunity to provide more detailed feedback informed by broader member engagement.

Thank you again for your thoughtful approach to cybersecurity oversight and for your continued partnership with industry stakeholders. The joint trades remain committed to supporting a balanced, effective framework and stand ready to further engage as needed.

Sincerely,

American Property Casualty Insurance Association

Kristin Abbott
202-828-7130
Kristin.abbott@apci.org

American Council of Life Insurers

Kirsten Wolfford
202-624-2059
kirstenwolfford@acli.com

National Association of Mutual Insurance Companies

Lindsey Klarkowski
317.876.4212
LKlarkowski@namic.org

Summary of Drafted Documents

CFRF Referral Response

- Endorses the Compliance Guide and recommends integration into:

Financial Condition Examiners Handbook (FCEH)

Market Conduct Examination Handbook (MCEH)

- Suggests training development with ITEWG and NAIC staff
- Reinforces the importance of communication and coordination among states

MEMORANDUM

To: Diana Sherman, Facilitator of the Chief Financial Regulator Forum

From: Michael Peterson, Chair, and Colton Schulz, Vice-Chair of the Cybersecurity (H) Working Group

Date: Pending

RE: Response to August 16, 2024 Referral on Data Security Model Compliance Testing

Thank you for your referral regarding Data Security Compliance Testing. We appreciate the Chief Financial Regulator Forum's attention to this critical issue and the detailed considerations provided. The observation that there lacks clear expectations for compliance testing and reporting made clear that what was required was formal guidance supported by a motion from the Cybersecurity (H) Working Group.

Ensuring consistent and effective compliance testing for the Insurance Data Security Model #668 (IDSM) is vital for maintaining robust cybersecurity practices across our market. As we developed our guide we had two primary goals: how to avoid the duplication of work across departments through improved communication, and within departments through the utilization of a gap analysis to tie in work from other sources.

Suggested Updates:

As adoption of the IDSM continues, so too does the need for clear, coordinated expectations for how compliance is assessed. To do so we have developed an IDSM Compliance Guide where to assist with compliance and enforcement. To frame our approach, we emphasize two distinct but complementary objectives: (1) avoiding duplication and redundancy across departments with improved communication, and (2) avoiding duplication and redundancy within departments by conducting a gap analysis prior to conducting an IDSM exam.

This approach supports the IDSM Compliance Guide's vision of a seamless regulatory environment where the domestic state is trusted to ensure the compliance of its licensees, while recognizing that there may be exceptions. However, because there currently lacks a process similar to accreditation for the IDSM, the IDSM Compliance Guide details how a department should utilize a gap analysis to reduce redundancy between IDSM compliance and financial solvency and market conduct examinations.

Our guide attempts to provide departments with an array of tools for understanding what is occurring across those states that have passed a version of the IDSM. This includes an

explanation of the artefacts created under Section 4(I) and how they can be used to ensure compliance with foreign licensees.

However, we took into careful consideration that while the IDSM and its requirements' overlap with much of the IT Review performed during financial examinations, the matchup isn't perfect. While departments may perform market conduct IT examinations, where there is more freedom to investigate beyond the confines of internal controls over financial reporting, there will likely remain gaps with the IDSM. Given this, in order to create a standardized IDSM examination across departments, a careful gap analysis looking at all relevant work over the period, must be completed prior to developing the work program of an IDSM examination.

In addition to the IDSM Compliance Guide, our recommendations and suggestions are as follows:

- **Consistency Across Guidance:** To enhance examiner awareness and promote leveraging of work, we recommend that the:
 - IT Examination (E) Working Group (ITEWG) consider providing a new mapping from the IDSM to Exhibit C as they complete future updates to the FCEH.
 - Market Conduct Examination Guidelines (D) Working Group consider incorporating both the IDSM Compliance Guide and the Cybersecurity Event Response Plan into the MCEH.
- **State-to-State Communication:** We support the consideration of updates to the relevant examination guidance that emphasizes the importance of communication among states, particularly where such insights can inform supervisory planning or reduce duplicative efforts.
- **Market Conduct Coordination:** We encourage the Market Conduct Examination Guidelines (D) Working Group to explore how the guidelines will benefit from the inclusion of the IDSM Compliance Guide and the Cybersecurity Event Response Plan, particularly in states that have adopted the IDSM.

We encourage working groups to continue to explore opportunities to work with the Cybersecurity (H) Working Group to find the best path forward for any other areas of intersection with the IDSM.

Conclusion and Path Forward

The Cybersecurity (H) Working Group appreciates the Chief Financial Regulator Forum's thoughtful referral and the opportunity to support a more unified approach to IDSM compliance. As adoption of the IDSM continues, we recognize the importance of fostering a regulatory environment that encourages convergence through communication and standardization.

We remain committed to supporting convergence across all areas of IDSM compliance among states and look forward to future discussion on this important issue.

For further discussion or clarification, please contact me or NAIC staff (Koty Henry at khenry@naic.org or Miguel Romero at maromero@naic.org).