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

Introduction

The Insurance Data Security Model Law #668 (IDSM) ~~provides~~ establishes many requirements of affected licensees. The enforcement of compliance is complicated by other, similar efforts across 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.

To reduce the risk of duplicative ~~and redundant~~ work, ~~foreign~~ regulators should generally place reliance on ~~domestic~~ the work of a foreign licensees' domestic regulators, especially if they have passed a version of the IDSM, to regulate their own market. A method to provide ~~foreign~~ non-domestic regulators with adequate assurance will leverage Section 4(I) of the IDSM, allowing licensees from IDSM ~~states~~ jurisdictions 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 determined by relying on the work done by other departments, where appropriate, but only from other IDSM states. While the work to pass a version of the IDSM in each jurisdiction is not complete, the final state that this guide envisions is one where each IDSM state enforces its law on their domestics without the need for additional scrutiny by ~~foreign departments~~ other jurisdictions in which the licensee operates. With all ~~states~~ jurisdictions working together we can create a seamless regulatory environment for our licensees and maximal protection for our consumers.

How to Use this Guide

Departments of Insurance whose legislatures have passed version of the IDSM will gain access to new avenues of examination and investigation. However, the IDSM does not create a new form of examination and instead, Section 7(A) points to existing applicable statutes governing the investigation or examination of insurers. As such, for the purpose of this guide, an IDSM Review can take the form of a market regulation examination, in particular Standard 17 and the IDSM supplement found in the Market Regulation Handbook (MRH), or the IT Review performed during a financial condition examination, which is described in the Financial Condition Examiner's Handbook (FCEH). This guide is not prescriptive regarding the timing or frequency of IDSM Reviews and does not recommend which examination team (e.g. IT, Financial, Market) should complete them.

Both the MRH and the FCEH have created specific references to the IDSM, and both sets of guidance stress the importance of communication so that existing work can be effectively leveraged. This guide continues in that tradition but applies it to the entire market. However, the diversity of potential exams and investigations into a licensee's IT function, as well as the growing number of empowered state regulators raises the risk of duplicative work. This guide will help departments implement the IDSM after it is passed, as well as those seeing more information to streamline existing regulatory efforts related to the IDSM.

Commented [KH1]: Section added per multiple stakeholder comments.

Formatted: Font: Not Bold

Objective

The foundational element provided in this guide~~ance~~ 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~~ guide provides an IDSM compliance review processes for the domestic regulator ~~that~~ which focuses on compiling all relevant work and performing a gap analysis ~~between them and~~ against the requirements of the IDSM. This approach ensures consistent work across jurisdictions without any ~~duplicative~~ work being redundantly 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~~ adopted in all jurisdictions. However, ~~since~~ until an accreditation process for IDSM compliance reviews has not yet been agreed upon, a gap analysis ~~is still~~ will be required to determine if any additional inquiry into ~~the foreign~~a non-domestic ~~department's area of concern~~licensee is necessary.

Lastly, collaboration among departments is central to the ~~task~~ aim of reducing duplicative ~~and redundant~~ work by ~~foreign~~ non-domestic regulators. By understanding what work was done by the domestic regulator, the ~~foreign~~ non-domestic regulator's requirements may be fully satisfied. Even if this is not the case, in-depth discussion between domestic and ~~foreign~~ non-domestic ~~regulator~~regulators 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 ~~its~~ routine regulatory work. One particularly useful document in the hands of the domestic regulator in an IDSM ~~state~~ jurisdiction is the certificate (or affidavit) of compliance required under Section 4(I). For those ~~states~~ jurisdictions ~~who~~that have a mature approach to IDSM regulation, requesting this document may provide all the assurance a ~~foreign~~ non-domestic regulator requires. This is not possible with New York (to be discussed later), but New York domiciled licensees can, themselves, provide a ~~highly similar~~comparable document that can be similarly leveraged by a ~~foreign~~ non-domestic regulator.

For those situations where a ~~foreign~~ non-domestic regulator requires deeper or additional review from what has already been performed, continued contact is key as the ~~foreign~~ non-domestic 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~~ and 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 IT Review work done and ~~their state's~~that jurisdiction'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~~various sections 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 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~~ required to provide a separate certificate of compliance (similar to the requirement found in Section 4(I)) certifying HIPAA compliance, which can be relied upon identically to a certificate from a licensee that is not subject to HIPAA.~~.~~

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)~~, 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. Notwithstanding~~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 [SM2]: I don't think this has been established. Only the breakout of cybersecurity controls review into a separate Exhibit C Part Three will use the NIST CSF 2.0 as its framework, while the ITGC review will remain aligned with the COBIT framework but updated to its current version.

Another, less common ~~tool,~~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's ~~utilizes~~ utilization of the current Exhibit C (COBIT based framework)~~, and~~ can also be 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 if a licensee is compliant with the IDSM, a gap analysis should be performed by the domestic ~~state~~ regulator to ensure all applicable measures are in place. Lastly, the guidance to avoid duplication does not ~~preclude~~ prohibit 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~~ Non-domestic Jurisdictions

There are two categories of licensee of consideration to ~~foreign~~ non-domestic regulators, those that are domesticated in an IDSM ~~state~~ jurisdiction 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~~ non-domestic 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 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~~ jurisdiction to manage the remediation that's been identified.

Under unusual circumstances, like where a ~~foreign~~ licensee ~~does~~ writes much of its business in ~~the~~a non-domestic regulator's state, the two departments should first communicate with each other to avoid redundant efforts. It may be the case that the ~~foreign~~ non-domestic 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~~ non-domestic 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 does Section 4(I) 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(I) certificate of compliance. However, ~~there is a wrinkle, because~~ New York's confidentiality responsibilities are ~~not like everyone else's, you'll~~unlike those of IDSM jurisdictions, so regulators in IDSM jurisdictions will have to request have to request the compliance certification 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~~New York does. This does not mean that assurance is not being ~~attained~~obtained, 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~~ all U.S. States~~'~~ and Territories'. As such, consideration for those foreign licensees that are not domesticated in an IDSM ~~state~~ jurisdiction must also consider duplication and redundancy of work. As discussed, domestic regulators have the IT Review that covers many or all areas required under the IDSM, and outreach among departments may unveil substantial work necessary for determination of IDSM compliance. Further, other ~~states~~ jurisdictions 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~~ non-domestic 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~~ its domestic licensees, the following examination considerations will focus on domestic action. For those rare situations where a regulator in an IDSM jurisdiction is examining a foreign licensee's compliance with its IDSM, coordination with the licensee's domestic regulator to address the situation is the recommended first step. ~~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 [SM3]: To maintain consistency with the FCEH, the word *foreign* should be applied only to the licensee and not the regulator.

The first task, alignment with existing efforts, asks the domestic regulator to determine what has already been done prior to developing ~~their~~ its 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 addressed by the NAIC's coordinated examination system hosted in a highly secure environment that meets the confidentiality, integrity, and availability standards of FedRAMP Moderate authorization. ~~The second task, maintaining confidentiality, is addressed by the NAIC's coordinated examination system existing in a highly secure environment, which meets or exceeds the highest security, confidentiality, and resilience standards in IT. F~~Further, confidentiality and security standards continue when the targeted examination reports are uploaded to the Financial Examination Electronic Tracking System (FEETS). 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 [SM4]: The NAIC coordinated examination database is hosted in a FedRAMP authorized public cloud deployment environment that meets Impact Level - Moderate. There are other security standards and frameworks that exceed FedRAMP standards, including FedRAMP High (for unclassified data), DoD IL5, and ultimately DoD IL6, but FedRAMP Moderate is presumed to be the highest security standard for commercial public SaaS providers.

Regardless, some jurisdictions subscribe to the SOC 2 compliance hosting environment, instead of the FedRAMP environment. The IDSM review files for these states will not have the stated security level.