An Actuarial Report for Cyber Risk Losses prepared by

SIGMA Actuarial Consulting Group, Inc.

SIGMA ACTUARIAL CONSULTING GROUP, INC.

March 1, 2025

Samantha Jackson - Director of Risk Management
CC: John Doe – CISO and Director of Cyber Security
XYZ, Inc.
123 Lafayette Avenue, Suite 456
Atlanta, GA 30303

Re: Actuarial Analysis – Cyber Loss Projection

Mrs. Jackson,

Enclosed are the results of an actuarial analysis prepared by SIGMA Actuarial Consulting Group, Inc. Your comments and questions are welcome.

It has been a pleasure working on this assignment, and we look forward to future opportunities to work together.

Regards,

L. Michelle Bradley, ACAS, MAAA, ARM, CERA, CCIS
Consulting Actuary

Qualification Statement: I, L. Michelle Bradley, am associated with the firm of SIGMA Actuarial Consulting Group, Inc. I am a member of the American Academy of Actuaries and meet its qualification standards, and I am an Associate of the Casualty Actuarial Society.

Final Report: This final report replaces any draft reports for this analysis.

Table of Contents

Section 1: Executive Summary

Section 2: Exhibits

Executive Summary

Introduction

This actuarial analysis is prepared by SIGMA Actuarial Consulting Group, Inc. (SIGMA) for XYZ, Inc. (XYZ). The conclusions represent a professional analysis and opinion of XYZ's cyber liability loss experience and claim exposure. The scope of this analysis is:

1. Project losses for the 2025 period at various retentions
2. Provide a confidence level analysis for the 2025 projected losses.

The uses of this report could also include the following:

- Actuarial support for determination of potential captive premium
- Input for pro-forma financial statements in captive feasibility

Immediately following this introduction is a summary of the **loss simulation assumptions and input parameters** used to simulate and project the cyber losses. The **coverage components and proposed retention levels** section further defines the scope of the cyber loss projections. The **projected losses by proposed retentions** section details the projected losses for the various proposed retentions at the expected level and several confidence levels. The **glossary of terms** includes detailed definitions of the cyber coverage components considered within the analysis. The **qualifying statements** add important comments concerning the data and assumptions used to complete the analysis. The **data reliance and review** section discusses the sources of all data utilized for this analysis. The **exhibit summary** section presents detailed descriptions of the exhibits included in section 2.

This report is intended for the use of XYZ. If released to any third party it should be released only in its entirety. Please advise the authors at SIGMA of the release of this report to any other parties. SIGMA reserves the right to supplement this report with additional explanations and qualifications as it deems appropriate for the particular user.

Executive Summary

Loss Simulation Assumptions and Input Parameters

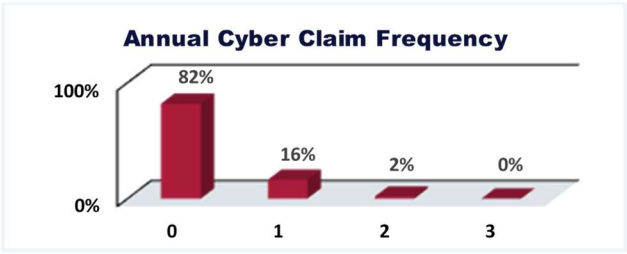
The **Loss Simulation Assumptions and Input Parameters** exhibit details the assumptions and input parameters used within the loss simulation. This includes the number of simulations used, the projected period exposures, and the selected distributions and parameters used to model loss frequency, severity, and the number of days of any business interruption.

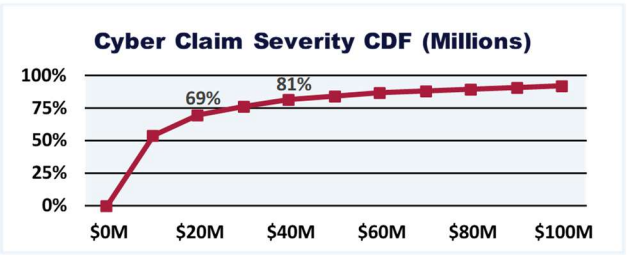
The **Annual Cyber Claim Frequency** graph displays the probability of 0, 1, 2, or 3 cyber claims occurring in the projected period.

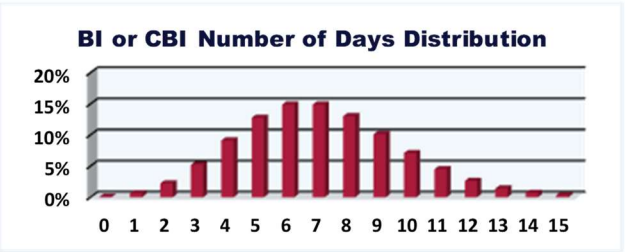
The **Cyber Claim Severity CDF** graph displays the cumulative probability of a cyber claim severity. For example, it indicates that 81% of the time that a cyber liability claim occurs the total loss severity for that claim will be less than or equal to $40,000,000.

The **BI or CBI Number of Days Distribution** graph displays the probability of the numbers of days for which business interruption will occur given that a business interruption claim has occurred.

Losses are simulated using a Monte Carlo simulation with 10,000 iterations.	
Estimated Policy Period Revenue:	$13,000,000,000
Projected Annual Cyber Liability Occurrence Count:	0.200
Distribution Assumed for Occurrence Frequency:	Poisson
Unlimited Average Claim Severity:	$38,694,000
Coefficient of Variation for Claim Severity:	4.5
Distribution Assumed for Claim Severity:	Lognormal
Average BI and CBI Number of Days of Interruption:	7
Distribution Assumed for Number of Days of Interruption:	Poisson
Historical Number of Claim Occurrences:	1
Historical Total Unlimited Loss Experience:	$33,800,000
Historical Number of Days of BI Due to Claim Occurrence:	7







Executive Summary

Coverage Components and Proposed Retention Levels

The **Coverage Components and Proposed Retention Levels** exhibit details the cyber liability coverage components and proposed retention levels included within the projected losses. A glossary of terms for each of the coverage components has been included in a later section.

Cyber Coverage Components Included:	Proposed Retention Levels:
Technology Errors and Omissions Liability	$10M Per Occurrence
Cyber Incident Response Team	$10M Excess of $10M
Non-Panel Response Provider	$10M Excess of $20M
Business Interruption Loss & Extra Expenses	$10M Excess of $30M
Contingent Business Interruption Loss & Extra Expenses	$10M Excess of $40M
Digital Data Recovery	$25M Excess of $50M
Network Extortion	
Cyber, Privacy and Network Security Liability	
Payment Card Loss	
Regulatory Proceeding	
Ransomware	

Executive Summary

Projected Losses by Proposed Retentions

The **Projected Losses by Proposed Retentions** exhibit details the projected aggregate cyber liability losses for the various proposed retention levels at the expected, 75th, 85th, and 95th percentiles of the loss simulation. For example, at the $10M excess of $10M per occurrence retention level it indicates that an aggregate loss amount of $4,990,000 should be adequate to pay all losses that occur during the projected period 85% of the time. This means that 85 out of 100 times, losses will be less than or equal to $4,990,000. Larger dollar amounts relate to higher probability levels. For example, there is a 95% chance that losses will not exceed $10,000,000.

	Expected Level	75th Percentile	85th Percentile	95th Percentile
$10M Per Occurrence	$1,930,000	$0	$10,000,000	$10,000,000
$10M Excess of $10M	1,590,000	0	4,990,000	10,000,000
$10M Excess of $20M	890,000	0	0	10,000,000
$10M Excess of $30M	450,000	0	0	2,650,000
$10M Excess of $40M	270,000	0	0	0
$25M Excess of $50M	370,000	0	0	0

Executive Summary

Glossary of Terms - First Party Insuring Agreements

- **Cyber Incident Response Team**

  A cyber incident response team is a team of providers responsible for responding to a cyber incident that occurs to the insured. The team is usually comprised of pre-approved response providers from the insurer that are independent contractors. Covered expenses may be costs incurred by the insured that are deemed reasonable and necessary because of a cyber incident. Specific expenses may include retaining the services of a law firm, crisis communications firm, forensic firm, licensed investigator, or any other services deemed necessary. Depending on the insurer, this team may be part of a breech response type coverage. Some companies have internal cyber response teams.

- **Non-Panel Response Team**

  A non-panel response team is a team of providers responsible for responding to a cyber incident that occurs to the insured that are not on the insurer's pre-approved response provider list. Covered expenses may be costs incurred by the insured that are deemed reasonable and necessary because of a cyber incident. Specific expenses may include retaining the services of a law firm, crisis communications firm, forensic firm, licensed investigator, or any other services deemed necessary. Depending on the insurer, this team may be part of a breech response type coverage or may not be covered.

- **Business Interruption Loss and Extra Expenses**

  Business interruption loss and extra expenses coverage provides reimbursement for the loss of business income of the insured during the interrupted period and extra expenses to determine the amount of the loss caused by a cyber incident experienced by the insured. The interruption period is the earliest date the system was interrupted through the end date of when the insured's system is or could be restored. The number of covered interruption days and waiting period before the coverage starts may vary depending on the insurer. A cyber incident may be classified as an interruption in the insured's computer system which is owned, leased, or operated by the insured to run their business.

- **Contingent Business Interruption Loss and Extra Expenses**

  Contingent business interruption loss and extra expenses coverage provides reimbursement for the loss of business income of the insured during the interrupted period and extra expenses to determine the amount of the loss caused by a cyber incident experienced by a partner company or service provider to the insured. The interruption period is the earliest date the system was interrupted through the end date of when the insured's system is or could be restored. The number of covered interruption days and waiting period before the coverage starts may vary depending on the insurer. A cyber incident may be classified as an interruption in the insured's shared computer system, a third-party system other than the insured's own computer system used by the insured, that is used to operate their business.

- **Digital Data Recovery**

  Digital data recovery provides coverage for data recovery expenses incurred by an insured from a cyber incident. A cyber incident may be classified as any network security failure or failure to protect, manage, or store payment card data and protected information. Data recovery expenses may be necessary and reflect the reasonable cost to recreate, retore, or replace an insured's damaged data or software.

- **Network Extortion**

  Network extortion coverage provides reimbursement for extortion expenses when the insured has a network extortion threat. A network extortion threat occurs when the hackers have the insured's data and threaten to publicly release, destroy, or use their data unless they receive some amount of payment from the insured. Extortion expenses may include money or other considerations of payment to the hackers or necessary and reasonable expenses to help mitigate additional loss.

- **Ransomware**

  Ransomware coverage provides reimbursement for ransomware expenses when the insured has a ransomware threat. A ransomware threat occurs when the hackers have blocked access to, corrupted, or encrypted the insured's computer system. The hacker will then demand some form of payment or ransom in exchange for restoring or decrypting the insured's computer system. Ransomware expenses may include money or other considerations of payment to the hackers or necessary and reasonable expenses to help mitigate additional loss. Depending on the insurer, this coverage may be combined with a network extortion type coverage.

Glossary of Terms - Third Party Insuring Agreements

- **Technology Errors and Omissions Liability**

  Technology errors and omissions liability provides coverage for expenses and damages incurred from a technology incident claim filed against the insured. A technology incident claim may be classified as any error, omission, misleading statement, or breach of duty in some technology product or service provided by the insured which resulted in a third-party alleging financial injury. Expenses and damages covered may include attorneys' fees, settlement amounts, compensatory damages, and any amounts where the insured is legally obligated to pay.

- **Cyber, Privacy and Network Security Liability**

  Cyber, privacy and network security liability provides coverage for expenses and damages incurred from a cyber incident claim filed against the insured. A cyber incident claim may be classified as any data breach, privacy violation, or network security failure of the insured. Expenses and damages covered may include attorneys' fees, settlement amounts, compensatory damages, and any amounts where the insured is legally obligated to pay.

- **Payment Card Loss**

  Payment card loss provides coverage for the payment card loss expenses owed by the insured when a cyber incident occurs. A cyber incident may be classified as any network security failure or failure to protect, manage, or store payment card data and protected information. Payment card losses may include payment card industry (PCI) fines or penalties, reimbursements, monetary assessments, or chargebacks that are owed to the payment card brand. A payment card brand is any payment provider such as MasterCard Worldwide, American Express Company, etc. Depending on the insurer, this coverage may be part of a cyber, privacy and network security liability type coverage.

- **Regulatory Proceeding**

  Regulatory proceeding provides coverage for defense costs or regulatory fines and penalties resulting from a data breech or security failure. Depending on the insurer, this coverage may be part of a cyber, privacy and network security liability type coverage.

Executive Summary

Qualifying Statements

1. We have relied without audit or verification on historical data and qualitative information supplied by XYZ. It is our understanding we have been provided with all information which would materially affect the loss estimates and that all information furnished to us has been accurate and complete.

2. The following information sources were used to compile the parameters used within this analysis. A) Information pertaining to the proposed book of business was provided by XYZ. Note that this information represents current management expectations but may not be indicative of XYZ's actual future book of business. B) Information pertaining to the proposed cyber coverage components was determined based on cyber coverage in place for XYZ during the 07/01/2024 - 07/01/2025 policy period. C) Information pertaining to claim frequency, severity, and variability for cyber losses and business interruption losses due to cyber events were derived from a review of qualitative and quantitative data provided by XYZ as well as data obtained from various company rate filings and industry publications. D) SIGMA has compared our resulting loss projections to XYZ current and historical market premium estimates and theoretical premium estimates based on insurance company rate filing data as a reasonableness check.

3. We have assumed that historical operations (nature of operations) are representative of current and future operations. Limited historical data was available, and SIGMA supplemented this information with industry data, where available and reasonable. SIGMA has considered the available loss and expense data as well as qualitative information to determine the loss projections for each risk. It is possible that results could vary significantly from year to year and that actual results could vary from the projections for any specific year. At least two Actuarial Statement of Principles (ASOP) are relevant in this situation, which are highlighted below:

   ASOP 23, Section 3.1 states that:

   Appropriate data that are accurate and complete may not be available. The actuary should use available data that, in the actuary's professional judgment, allow the actuary to perform the desired analysis. However, if significant data limitations are

known to the actuary, the actuary should disclose those limitations and their implications.

ASOP 23, Appendix 1 states that:

Data frequently contain errors, are not complete, and are not precisely appropriate for the intended analysis. Actuaries deal with these limitations, the majority of which are non-critical. However, actuaries are often called upon to perform actuarial services in situations where data limitations may be critical. Actuaries use professional judgment when determining whether and how to refine data or make modifications within the analysis.

4. We have assumed there are no factors which would cause patterns in the underlying data to be unrepresentative of the current or future situation.

5. SIGMA can provide no guarantee that estimates will prove adequate or not excessive. The proposed retentions are significantly higher than the indicated loss projection due to the high-severity/low-frequency nature of the risks.

6. The methodology used in this analysis is primarily based on a frequency and severity model. Standard incurred and paid loss development methods are not used because of the limited unique historical data. The determination of the annual frequency and severity estimates are based on industry data, the limited unique data, direct input from XYZ, and current and past policy data. SIGMA completed sensitivity testing throughout the simulation process in relation to the selected frequency and severity of the model. The selected frequency and severity models were used as input for Monte Carlo simulation which has been used to determine the projected losses. These assumptions should be monitored over time as additional claims experience emerges.

7. The purpose of the loss simulation used within the analysis is to compute projected cyber liability losses in total based on reasonable industry and similar entity data to estimate variation by layer and confidence.

8. The unlimited loss parameters are selected for modeling purposes only, which SIGMA is using to determine loss estimates for the selected policy structure. The intended purpose of this analysis is to calculate expected loss amounts for the proposed policy structures outlined above. Within SIGMA loss simulations, the $25M excess $50M layer was reached for less than two and a half percent out of ten thousand iterations. The occurrence of a catastrophic loss for multiple coverage

components in a single year, while extremely unlikely, does have some small probability and the occurrence of an event of this magnitude would significantly impact the estimates within the report.

9. The loss projections in this report are based on the preliminary anticipated policy structures provided to SIGMA. If the final policy structure significantly differs from the structure outlined in this analysis, consideration should be given to modifying the projections in this analysis. In addition, these loss projections are based on XYZ's estimated 2025 revenue. Estimates of the total revenue should be confirmed as reasonable based on the actual policy inception date.

10. Changes in any of the information or assumptions upon which SIGMA's estimates of ultimate losses are based will require a reevaluation of the results of this report and possibly a revision of these projections.

If alternative risk transfer programs are considered, including, but not limited to, captive insurance, then the additional following qualifying statements are applicable:

11. The loss projections shown at the expected level and at various confidence levels are for pure losses and ALAE associated with each risk. These amounts are calculated on a net basis and reflect the per occurrence limits in effect for each period. Allocated loss adjustment expense (ALAE) is included and is defined as expense assignable to specific claims, such as legal costs. We have not analyzed unallocated loss adjustment expense which we define as expense not assigned to individual claims. If alternative risk transfer programs are considered, SIGMA is not opining on risk transfer related to premiums or whether the risks contained in this report are business risks or insurable risks for tax purposes. SIGMA is not offering any tax deductibility advice or other tax advice related to the loss projections and accounting for related premiums. It is our understanding that XYZ has provided us with all relevant retentions and coverage descriptions for the upcoming period.

12. This analysis provides actuarial loss projections. We are not issuing an opinion on future items related to risk transfer, tax issues, optimal program structure, optimal insured layers, optimal reinsurance structure, or contract wording. XYZ should seek appropriate expertise related to detailed questions or concerns that are beyond the scope of actuarial expertise and considerations.

This report should be released only in its entirety. SIGMA actuaries will be available for consultation should anyone reviewing this report have questions or require further analysis.

Executive Summary

Data Reliance and Review

The company-specific loss, exposure, and other data used in this report is supplied by XYZ. It is our understanding we have been provided with all information which would materially affect this analysis. The historical data is assumed to be accurate and complete and should be reconciled with internal records. We have considered XYZ's own loss and exposure data to the extent this data is credible and available. It is important to note however that XYZ has limited cyber liability loss experience in its history. SIGMA was provided quantitative and qualitative information related to this loss experience. All supplementary industry data reflects the characteristics of XYZ's type of business, to the extent possible.

Our consulting engagement does not include an audit of the data provided to us. An audit of the data is defined in an actuarial standard of practice as "a formal and systematic examination of data for the purpose of testing its accuracy and completeness." SIGMA does not provide accounting or auditing services, and these services are normally completed by independent accounting firms.

We have reviewed the data for overall reasonableness. As part of this review, we did not find any material issues in the data. However, such issues could be revealed by an audit.

Executive Summary

Exhibit Summary

Exhibit 1 – Projected Loss by Confidence Level – Total Cyber Losses 1 Year

Projected losses for the various cyber liability loss layers have been included at the expected level as well as at various confidence levels. These projected losses have been determined using loss simulations that consider the unlimited loss severity parameters, annual projected revenues, and loss frequency parameters which have each been listed in the **Loss Simulation Assumptions and Input Parameters** section.

The aggregate loss distribution column indicates the aggregate losses at various confidence levels. For example, at the $10M excess $10M per occurrence retention level an aggregate loss amount of $4,990,000 should be adequate to pay all losses that occur during the projected period 85% of the time. This means that 85 out of 100 times, losses will be less than or equal to $4,990,000. Larger dollar amounts relate to higher probability levels. For example, there is a 95% chance that losses will not exceed $10,000,000.

A limitation of the statistical model is that a concept known as parameter risk is not included in the calculation of the aggregate distribution. Parameter risk is the risk associated with the possible incorrect estimate of the projected losses. There is always the possibility that the estimate of projected loss is wrong. However, we have made our best estimate of the assumptions regarding the exposure to loss.

Exhibit 2 – Summary of Projected Premium – Total Cyber Losses

Understanding the potential premium associated with a risk can facilitate comparison of current market premium quotes to alternative risk strategies including captive insurance. Exhibit 2 has been included for informational purposes only to assist in the discussion of alternative risk development strategies.

This table calculates projected premium for losses limited to the per occurrence retention levels based on projected losses included in Exhibit 1. Projected losses at the expected level are used to determine a pure loss rate which, when applied to projected revenue, produces an estimate of ultimate incurred losses. The pure loss rate can be defined at the expected dollar loss cost per $100,000 of revenue.

The projected pure loss rate of $14.85 per $100,000 of revenue is multiplied by the projected revenue to forecast losses of $1,930,000 at the $10,000,000 per occurrence level. Note, actual losses for the projected period will differ from projected losses based on actual revenues and loss experience.

Projected losses are then adjusted for expense load, risk load, and a profit margin. These adjustments have been selected by SIGMA judgmentally using assumptions based on reasonable industry practices, and this projected premium is for informational purposes only.

SIGMA is a property casualty actuarial consulting firm. There are many components related to the calculation of premium. Some of the components require detailed expertise related to underwriting of the risk. This conceptual analysis comes from an actuarial perspective. XYZ should seek appropriate expertise related to detailed questions or concerns that are beyond the scope of actuarial expertise and considerations.

Exhibits

Exhibit 1 – Projected Loss by Confidence Level – Total Cyber Losses 1 Year

Probability Level	Total - $10M Retention	Total - $10M xs $10M	Total - $10M xs $20M	Total - $10M xs $30M	Total - $10M xs $40M	Total - $25M xs $50M
Expected	$1,930,000	$1,600,000	$890,000	$460,000	$270,000	$380,000
50.0%	$0	$0	$0	$0	$0	$0
55.0%	0	0	0	0	0	0
60.0%	0	0	0	0	0	0
65.0%	0	0	0	0	0	0
70.0%	0	0	0	0	0	0
75.0%	0	0	0	0	0	0
80.0%	0	0	0	0	0	0
85.0%	10,000,000	4,990,000	0	0	0	0
90.0%	10,000,000	10,000,000	2,210,000	0	0	0
95.0%	10,000,000	10,000,000	10,000,000	2,650,000	0	0
97.5%	10,000,000	10,000,000	10,000,000	10,000,000	6,440,000	0
99.0%	20,000,000	17,220,000	10,000,000	10,000,000	10,000,000	25,000,000

Exhibits

Exhibit 2 – Summary of Projected Premium – Total Cyber Losses

Description	Losses Limited to $10,000,000 Per Occurrence	Losses $10,000,000 xs $10,000,000 Per Occurrence	Losses $10,000,000 xs $20,000,000 Per Occurrence	Losses $10,000,000 xs $30,000,000 Per Occurrence	Losses $10,000,000 xs $40,000,000 Per Occurrence	Losses $25,000,000 xs $50,000,000 Per Occurrence	Comment
(1) Projected Pure Loss Rate (per $100,000 of Revenue)	$14.85	$12.31	$6.85	$3.54	$2.08	$2.92	Based on Monte Carlo Loss Simulation
(2) Projected Revenue	$13,000,000,000	$13,000,000,000	$13,000,000,000	$13,000,000,000	$13,000,000,000	$13,000,000,000	Provided by Management
(3) Projected Expected Losses	$1,930,000	$1,600,000	$890,000	$460,000	$270,000	$380,000	Exhibit 2
(4) Loss Ratio	65%	65%	65%	65%	65%	65%	Assumption
(5) Expense Load	$1,040,000	$860,000	$500,000	$500,000	$500,000	$500,000	Assumption [1]
(6) Risk Load	$190,000	$160,000	$90,000	$50,000	$30,000	$370,000	Assumption [2]
(7) One Year Premium	$3,160,000	$2,620,000	$1,480,000	$1,010,000	$800,000	$1,250,000	(3) + (5) + (6)
(8) Profit Margin	$158,000	$131,000	$74,000	$50,500	$40,000	$62,500	Assuming 5% Margin
(9) One Year Premium With Profit Margin	$3,318,000	$2,751,000	$1,554,000	$1,060,500	$840,000	$1,312,500	(7) + (8)

[1] The Expense Load is determined based on the the expenses suggested by the loss ratio applied to Projected Expected Losses with the expense amount not to fall below the minimum expense amount of $500,000
[2] The Risk Load has been assumed to be 10% of expected Projected Expected Losses with the risk load amount not to fall below the minimum risk load required so that the premium exceeds a 5% Rate on line.

Notes:
This premium indication is shown for illustrative purposes only.

About SIGMA

Founded in 1995, SIGMA Actuarial Consulting Group, Inc. is an independent property and casualty actuarial firm located in Brentwood Tennessee. SIGMA provides casualty actuarial consulting services to captive managers, risk managers, brokers, risk management consultants, TPAs, and CPAs. Our credentials cover a broad spectrum from actuarial credentials and advanced academic degrees to risk management and captive insurance specialty credentials. SIGMA is dedicated to offering professional services to its clients and prides itself in the method used to communicate the results of the analysis. We are known for providing an easy to read and understandable analysis free of actuarial jargon. The findings are presented in such a way that individuals not necessarily familiar with actuarial principles and procedures can follow and reasonably understand how the calculations are made and the implications of the results. The analyses of loss data are objective and reference the most recently available insurance industry statistics when necessary and appropriate. SIGMA has won numerous industry awards that highlight our commitment to excellence and education.

SIGMA Actuarial Consulting Group, Inc.
5301 VIRGINIA WAY, SUITE 111, BRENTWOOD, TENNESSEE 37027 | 866.ACTUARY | 866.228.8279 | SIGMAACTUARY.COM