

Cyber Insurance

ICS4ICS Procedure Template

|  |
| --- |
| InstructionsThe following are suggestions about how you can update this template to create a procedure for your company:* Make decision to obtain cyber insurance
* If cyber insurance is obtained, update cyber incident response and ICS4ICS processes to ensure the insurance company is engaged and involved in these processes to ensure the insurance policy remains valid
* Identify the roles on the Decision Team that will manage insurance decisions
* Review and update the Decision Considerations based on your company requirements
* Exercise Cyber Incident Response and ICS4ICS processes with insurance company staff who are required to be involved in these processes
 |
| DisclaimerISA, ISAGCA, and the ICS4ICS Program provide this template to help asset owners create procedures to perform ICS4ICS and/or Cyber Incident Response and/or other related tasks. Each Asset Owners must update this template based on the needs of their company and ensure the procedure is review and approved by the appropriate parties (e.g., legal, senior management, corporate governance, government relations, etc.) from within their company. |

## Purpose

This document is intended to provide information to describe how your company can select, evaluate and manage cyber insurance.

## Evaluating Cyber Insurance

These are some common steps your company can take when considering and selecting cyber insurance:

* Identify company needs for cyber insurance
	+ Some companies are self-insured for some functions of their business and/or types of business units (e.g., wholly owned vs. joint venture subsidiaries) and/or based on other corporate policies
* Obtain information on the cyber insurance options available for your company
* Understand the controls and risk management maturity your company must achieve before obtaining cyber insurance
	+ Some insurance companies require minimum levels of maturity and controls
* Assess your current level of cyber controls and risk management capabilities, and determine the amount of work required to meet the minimum controls expected by the insurance provider

## Selecting Insurance Companies

* Asset owners must determine if it makes more sense to pay for insurance OR if they should invest to improve their controls and risk management instead of obtaining insurance
* Insurance companies are still trying to determine how best to price insurance premiums and assess risks to determine premiums
* Insurance Policy coverage is often not very clear, so due diligence is required to fully define coverage and ensure all processes for working with the insurance company are defined
* Asset owners are often asked to complete a self-assessment or use an independent 3rd party to complete an assessment so the insurance company understands the asset owner capabilities and risks; This may include:
	+ Develop an inventory of asset owner systems and components, and their associated risks
	+ Define asset owner prevention efforts to reduce incidents and their consequences
	+ Some insurance assessments are not risk-based
	+ Each insurance company may have a different approach on how to evaluate the asset owner compliance and risk management efforts
	+ Insurance companies have used a 1-page self-assessment that was sent to asset owners
* Assess what the insurance company will potentially pay for
	+ System recovery may be or not including in a policy
	+ Cyber Incident Response costs may be or not including in a policy
	+ Insurance companies often exclude payment for numerous situations, incidents, and events to limit their liability.
	+ Some specific incident and response costs are excluded; For example:
		- Ransomware coverage claims may have limited or may not exist; If coverage is provided for ransomware the insurance company will likely be involved with decisions to pay ransom which may result in them not reimbursing for ransom if the asset owner makes decisions that disagree with the insurance company guidance

## Integrating work with Insurance Companies

These are some of the work processes that need to be defined in the insurance policy and require continuous efforts to maintain integration with the insurance company staff and processes

* Asset owner likely will have a limited time after an incident is declared before they must inform the insurance company
* Asset owner may have to include insurance company staff in their Cyber Incident Response and ICS4ICS processes
	+ RACI is needed to understand how the insurance company staff plugs into the asset owner teams and how to define communication flows
		- The asset owner must determine which teams the insurance company staff report to
		- Insurance companies may require that they participate in negotiations of ransomware
* Some insurance companies have forensics and other staff that may benefit the asset owner or be duplicative of asset owner existing staff
	+ Insurance companies may require these staff groups to participate in an incident
	+ These services may be duplicative of the asset owner staff so an agreement is needed to understand who will lead each effort
* Exercising ICS4ICS and Cyber Incident Response processes must include insurance company staff because it is critical to ensure their staff can respond in an actual incident and both parties agree about how they will work together and who is the decision authority
	+ The goal is for all staff to complement existing company processes
* Asset owner may be required to take action to prevent on-going and future attacks
	+ Insurance companies may require the asset owner to put in controls to prevent on-going or future attacks as part of the recovery effort
* Chain-of-evidence requirements must be defined in the insurance policy and built into company incident response and ICS4ICS processes
	+ Several insurance companies will ask for evidence before considering any claim

## Decision Team

The following parties will be engaged to assess the situation, make decisions, and determine next steps as it relates to cyber insurance:

* Corporate Risk Management – Company Cyber Insurance Representative
* Corporate Cyber Security
* Corporate Legal and outside council
* ICS4ICS Incident Commander
* ICS4ICS Finance/Admin Section Chief

## Decision Process

The Decision Team will consider the following factors to make decisions about determining if the company should ignore guidance from the insurance company which may invalidate insurance claims:

* Consider possible Insurance company guidance that may conflict with the interests of the asset owner company:
	+ Insurance company guidance may require the asset owner to not pay ransomware even though the asset owner may determine that there are few viable options to restore systems in a reasonable time impacting associated business functions
	+ Insurance company guidance may require the asset owner to collect more evidence and/or engage law enforcement agencies that may significantly delay the company efforts to restore systems impacting associated business functions
	+ Assess insurance company staff participation to help or possibly delay restoration of critical business functions
* Understand terms of the insurance policy so the company can make decisions that maximize the company interests to restore business operations while obtaining the maximizing future insurance claims
* Identify approval processes required to finalize decisions from this decision team; Senior Executives (the Crisis Management Team) may need to approve some decisions

## Decision Factors (Table)

The Decision Team will consider the following factors to make decisions about the cyber insurance:

|  |  |  |
| --- | --- | --- |
| Type | Enforcement | Description |
| Policy | Required | <link to the cyber insurance policy> |
| Corp Policy | Required | <describe each Corp Policy requirement that impacts insurance decisions> |
| Decision Approval | Required | <describe company decision processes required to finalize decisions> |