Information Technology Planning Questionnaire (ITPQ)

The request below is being made pursuant to ss. 601.44 (3) and 601.43, Wis. Stat., and is intended to provide information to the Information Technology (IT) Examiner to gain an understanding of your IT operations. Responses will be an input into the planning process for the risk-focused IT examination to be performed.

- The scope of the IT examination includes All IT operations of the insurer, including those IT services performed by an affiliate or a third party, wherever located. If a non-insurance affiliate or an insurance affiliate performs IT functions for the insurer, you need to include those affiliates in your ITPQ responses and identify the applicable affiliate in your response. The IT examination will focus on the controls extending from 12-18 months prior to the as of date of the examination and any significant changes occurring in the current year.

- When providing information concerning third-party IT services insurer should show that it evaluated the business impact and did a risk assessment of each third party provider and continues to monitor these services. If any answers to the ITPQ are provided by a third party, they should be identified as such and integrated into the ITPQ.

- Since this request is being used for planning the fieldwork, a response of “Available at the company” is not considered acceptable.

- All questions are expected to be responded to either in a narrative response or the actual documentation. Responses should contain adequate detail to provide an understanding of the insurer’s control environment. If the request is not relevant, the insurer should provide a narrative of why the request is not relevant to its operations. Blank responses or “Not Applicable” responses without explanation are not considered acceptable.

- The response should be provided in an electronic format compatible with Microsoft Office or as a .pdf if necessary. Most text responses can be included in this document. Other documents should be provided in a separate file and referred to in the answers below rather than embedded in this document.

After reviewing the IT Planning Questionnaire and other documentation, the IT Examiner will create an IT risk matrix. The IT risk matrix will identify various IT risks of the insurer that the IT Examiner is interested in evaluating the adequacy and effectiveness of the insurer’s mitigating controls. The insurer will be asked to complete the matrix by identifying its controls that mitigate the risks listed in the matrix. The IT Examiner will then evaluate the adequacy of those controls to mitigate the IT risk and request evidence to test the effectiveness of those controls in mitigating the IT risk. Testing will then be performed during the IT examination fieldwork.

For insurers without adequate documentation of their IT controls, a more substantive approach may be applied.

The findings of the IT examination will be used by the financial examination as an input to determine the residual risk for the insurer’s key activities.

Information Technology Planning Questionnaire (ITPQ)

Please note: If a non-insurance affiliate or an insurance affiliate or a third party contractor performs IT functions for the insurer, you need to include those activities in your ITPQ responses and identify the applicable affiliate in your response.

1) Insurer Name(s):

   Completed By:

   Title:

   Phone Number:

   E-mail Address:

2) Provide a list of the data centers used by the insurer. The list should include all data centers where applications and/or data are located whether owned by the insurer, by a third-party service provider, or for disaster recovery purposes. The listing should differentiate the purposes of multiple data centers.

3) Provide a list of the locations where the insurer's data is entered or output is generated. This would include the insurer's home office, regional offices, and outside service providers.

4) Provide a summary of the functions performed by the information technology (IT) department. Include and identify outsourced IT functions.

5) Provide copies of any affiliated management, cost allocation, or service agreements that address IT services provided to/from the insurer. Also, provide a summary of the services provided under the agreements.

6) Provide a list of business or data processing services ***performed by*** any other entities on behalf of the insurer which support key activities, such as a third-party administrator, managing general agent, pharmacy benefit manager, application hosting, etc., indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, location of services, and services covered). Copies of the significant contracts and/or service-level agreements with exhibits and amendments should be provided.

7) Provide a list of IT services of the insurer ***provided to*** any other entities, including affiliates, indicating the type of services provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, and services covered). Copies of the significant contracts and/or service-level agreement with exhibits and amendments may be requested.

8) Provide a list all other agreements where IT services are ***provided to*** the insurer. Identify the parties and the service provided. For example, offsite storage agreements, consulting agreements, disaster recovery agreements, and internet service provider agreements.

9) Provide specific detailed organizational charts for the insurer's information technology department and its various functional areas (e.g., operations, programming, security, infrastructure, etc.). Include the reporting relationship of the IT department within the organization.

10) Provide a narrative on the insurer's adequacy of segregation of duties with respect to internal IT processes and IT personnel performing non-IT functions or non-IT personnel performing IT functions.

11) Provide the name and contact information (telephone number and e-mail address) of the individuals holding the following positions, or functional responsibility, in the insurer: Chief Information Officer, Chief Technology Officer, Chief Security Officer, and System Architect.

12) Provide an executive overview of the IT Steering Committee or other group that establishes and directs IT policies and strategies, indicating the membership of the group and the frequency of their meetings.

13) Provide an executive overview of your IT strategic plans, including plans for e-commerce. If the IT strategic plan is at a group level, identify insurer management's input into the strategic plan.

14) Complete the system summary grid (Attachment A) for all applications supporting key activities, including any applications used by affiliates or third-party service providers to support operations. Also, provide a list of the company's data warehouse(s) and the key activities they support.

15) Provide a diagram or narrative description of the application-level interfaces among the various applications supporting the insurer's operations (e.g., claims system feed into the accounting system). The diagram should include initial inputs of data into applications and outputs provided to users. Automatic and manual interfaces should be differentiated. At least all applications listed in response to question 14 should be included in this response.

16) If multiple platforms/systems to process cash, premium, claims, or reinsurance transactions are used for an individual type or line of business, include a reconciliation of amounts processed on each separate system to total dollar amount processed during the prior year. This summary should also include and identify processing which is outsourced. Indicate whether there is any significant anticipated change in processing volumes during the current year.

17) Provide a high-level network diagram. If the insurer's internal operations include a wide area network, the WAN should be included in the diagram.

18) Provide policies and procedures related to the insurer's system (solutions) development life cycle (SDLC). The life cycle would contain the phases from initial request to post-implementation reviews. Indicate whether the insurer uses internal personnel and/or external vendors to develop and/or maintain its applications. Identify any differences in the SDLC based on the size or significance of the project or change request.

19) Provide policies and procedures specific to the change management (moving items into the production environment) process. This should include both application and infrastructure changes. Documentation should address the phases from initial request to post implementation review.

20) Provide a list of projects and change requests, including infrastructure changes, made during the period extending two years prior to the examination "as of" date and including significant projects and change requests up to the date your response is provided. The listing should include the project/change number, a description of the project/change, the hours for the project/change, and the implementation date. A sample to review documentation may be requested as part of the IT examination fieldwork.

21) Describe the physical security features over access to the insurer's data center and network closets. Include controls over building access. The description should include the authorization and monitoring of access to your data center(s) and network closets.

22) Describe the environmental controls over the insurer's data center(s). Environmental controls should include fire, water, temperature, humidity, and power. The description should include how these controls are monitored.

23) Describe the insurer's controls over identity access management for each system that supports key activities of the insurer. The controls should include authorization of access rights, access rights monitoring, and password controls.

24) Please provide the name, version, and purpose of software or hardware used by the insurer to monitor the network infrastructure. Examples would include spam filters, anti-virus, anti-malware, intrusion detection/prevention, and vulnerability software.

25) Describe the insurer's method for patch management of hardware, operating systems, database management systems, applications, etc. Include the schedule and process for ensuring that planned patches have been applied.

26) Describe the insurer's incident response plan or other policies or procedures to address security incidents. Security incidents are considered to be events where the company's network, applications, or data, particularly non-public information, is compromised.

    Identify whether the company has an incident response plan that addresses the following:
    - the internal process for responding to a cybersecurity event;
    - the goals of the incident response;
    - the definition of clear roles, responsibilities and levels of decision-making authority;
    - external and internal communications and information sharing;
    - identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
    - documentation and reporting regarding cybersecurity events and related incident response activities; and
    - the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

        a. Have there been any security incidents since the last examination? Has OCI been notified of such incidents prior to this questionnaire? If so, please provide the dates of notifications and to whom they were sent.

27) Provide copies of cyber security related policies and procedures, including those that address the following areas:

        a. information security;
        b. data governance, classification and inventory
        c. data life cycle – retention of nonpublic information and a mechanism for its destruction when no longer needed.
        d. access controls and identity management;
        e. systems and network security;
        f. systems and application development and quality assurance;
        g. customer data privacy; and
        h. all other cyber security policies that have not been discussed elsewhere.
        i. provide the data loss prevention plan and data flow monitoring methodology used by the insurer

28) Provide copies of any cyber security insurance policies that cover the insurer itself.

29) Provide copies of policies developed by the company for vendor and third-party service provider management, including any policies that address:

        a. the vendor and third party evaluation in risk assessment and business impact prior to outsourcing

b. the security of sensitive data or systems that are accessible to, or held by, third party service providers
c. the use of encryption to protect sensitive data in transit and at rest
d. notice to be provided in the event of a cyber security incident
e. internal requirements for minimum preferred terms to be included in contracts with third-party service providers

30) Provide copies of all other information systems policies.

31) Identify the URL(s) for the insurer's e-business home page. Describe the insurer's current use of e-business, indicating the type of transactions allowed, where the web site is hosted, and the volume of business processed.

32) Provide a high-level summary or a copy of your Information Systems Disaster Recovery Plan and a listing of the functional unit's Business Continuity Plans. See Appendix page for Business Continuity Plan guidelines.

33) Identify the insurer's alternate sites for their IT systems and employees.

34) Provide summary evidence of the last exercise/test results for the disaster recovery and business continuity plans, including functional units.

35) Describe the strategy for data and systems back-up.

36) Provide an overview of the insurer's data record retention and deletion strategy.

37) Provide a list of any IT audits/reviews performed within two years prior to the examination as of date, including e-commerce areas and network vulnerabilities. The list should include the dates, review subjects, e.g., SSAE 16/18, PCI-DSS, Sarbanes-Oxley, and who performed the audits/reviews, e.g. internal audit, CPA, another state departments of insurance, other governmental agencies and any other contractor or affiliate who may have performed the audit/review. Provide copies of any SSAE 16/18, Hitrust, IT penetration testing, audits/reviews performed within the previous two years including the associated remediation plans. Copies of other selected audits will be requested to be provided prior to the examination fieldwork.

38) Provide the insurer's most recent IT control documentation and evidence of testing (as required by SOX or the Model Audit Rule).

39) Please inform your company's independent auditor that OCI will be contacting them to review the most current available CPA work papers related to the testing of the IT control environment.

Appendix – Guidance for Business Continuity Plan

Business continuity planning has expanded beyond its initial information systems focus of disaster recovery plans to encompass issues such as natural and man-made disasters like terrorism, fraud, fire, loss of utility services, personnel losses and new laws and regulations. Therefore, it is important that an insurer's business continuity plan be considered throughout all aspects of the examination and not just in the context of a review of the insurer's information systems.

For all insurers, the business continuity process consists of identifying potential threats to an organization and developing plans to provide an effective response to ensure continuation of the company's operations. **The objectives of the business continuity process are to minimize financial losses; continue to serve policyholders and financial market participants; and to mitigate the negative effects disruptions can have on an insurer's strategic plans, reputation, operations, liquidity, credit ratings, market position and ability to remain in compliance with laws and regulations.**

Business Continuity Key Elements

Basic steps that OCI expects all insurers should have in their business continuity processes consist of:

Step 1 - Understanding the Organization

a) Understand its organization and the urgency with which activities and processes will need to be resumed in the event of a disruption.
b) This step includes performing an annual business impact analysis and a risk assessment.
c) The business impact analysis identifies, quantifies and qualifies the business impacts of a disruption to determine at what point in time the disruption exceeds the maximum allowable recovery time.
d) This point in time is usually determined separately for each key function of the insurer.
e) The risk assessment reviews the probability and impact of various threats to the insurer's operations.
f) This involves stress testing the insurer's business processes and business impact analysis assumptions with various threat scenarios.
g) The results of the risk assessment should assist the insurer in refining its business impact analysis and in developing a business continuity strategy.

Step 2 - Determining Business Continuity Strategies

a) The insurer determines and selects business continuity management strategies to be used to continue the organization's business activities and processes after an interruption.
b) Use the outputs of Step 1 to determine what business continuity strategies the insurer will pursue.
c) This includes determining how to manage the risk identified in the risk analysis process.
d) The strategies should be determined at both the corporate and key functional level of the insurer.

Step 3 - Developing and Implementing a Business Continuity Plan

a) The *purpose* of the business continuity plan is to identify in advance the actions necessary and resources required to enable the insurer to manage an interruption regardless of its cause.
b) The plan should be a formal documentation of the insurer's business continuity strategy and should be considered a "living document."
c) Some basic elements that should be included in a business continuity plan include:
    - Crisis management and incident response
    - Roles and responsibilities within the organization
    - Recovery of all critical business functions and supporting systems
    - Alternate recovery sites
    - Communication with policyholders, employees, primary regulators and other stakeholders

d) The business continuity plan should be written and should include a step-by-step framework that is easily accessible and able to be read in an emergency situation.

Step 4 - Testing and Maintenance

a) The insurer's business continuity plan should be reviewed, tested, and maintained.
b) The testing should be based on a methodology that determines what should be tested, how often the tests should be performed, how the tests should be run, and how the tests will be scored.
c) It is recommended that key aspects of the plan be tested annually and that the test be based on clear objectives that will allow the results of the test to be scored to determine the effectiveness of the business continuity plan.
d) In addition, the plan should be maintained and updated regularly to ensure that the organization remains ready to handle incidents despite internal and external changes that may affect the plan.