

Information Technology Planning Questionnaire (ITPQ)

The request below is being made pursuant to Wis. Stats. §§ 601.44 (3), 601.43, and 601.956, 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 date of the examination and any significant changes occurring in the current year.
- 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.

1. ITPQ Contact

Insurer Name(s):

Completed By:

Title:

Phone Number:

E-mail Address:

Information Technology Planning Questionnaire (ITPQ)

2. Information Technology Governance

- a. Provide the name, telephone number, and e-mail address of the chief information officer (or equivalent).
- b. Provide specific detailed organizational charts for the company's IT department, and/or any affiliates providing IT services, that show its various functional divisions (i.e., operations, programming, support services, etc.). Show reporting relationships of the IT department within the organization.
- c. Provide an executive overview of your company's IT strategic plans, including plans for e-commerce.
- d. Provide an executive overview of your 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.
- e. Provide an overview of the ERM program, if not already provided, and associated touchpoints in relation to IT risks.
- f. Describe the frequency, type, and content of interaction with the company's board of directors regarding key IT risks, such as cybersecurity.
- g. Provide a narrative on the insurer's adequacy of segregation of duties with respect to internal IT processes as well as concerning IT personnel performing non-IT functions or non-IT personnel performing IT functions.
- h. Provide a summary of the functions performed by the information technology (IT) department. Include and identify outsourced IT functions.
- i. Describe any personnel or systems changes during the period under examination that would significantly affect business and IT operations.

3. Information Technology Infrastructure

- a. Provide the name, telephone number and e-mail address of the chief technology officer (or equivalent).
- b. Provide a listing of the locations of all data-processing centers used by your company, whether owned by the company or by a third-party administrator that processes data for the company.
- c. Provide a system-wide map or topography, showing all hardware platforms and network connections, indicating all internal and external access points.
- d. Complete the system summary grid (Attachment A) for all applications supporting key

Information Technology Planning Questionnaire (ITPQ)

activities, including any applications used by affiliates or third-party service providers to support operations.

- e. Provide a data-flow 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 3.d should be included in this response.
- f. Provide a list of any business or data-processing services provided by the company to any other entities, including affiliates, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, and services covered). Also, indicate if a service level agreement (SLA) exists for each of these services. Provide copies of significant contracts and/or service-level agreements with exhibits and amendments.
- g. Provide a list of any business or data-processing services performed by any other entities on behalf of the company, such as a third-party administrator (TPA, MGA, GA, etc.) or an affiliate, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, location and services covered). Also indicate if an SLA exists for each of these services and if data stored at the TPA is commingled with other data sets or clearly segregated. Provide copies of the significant contracts and/or service-level agreements with exhibits and amendments.
- h. Provide a list of the company's third-party IT service providers. Indicate the type of service provided and summary of the terms and agreements (e.g., named parties, effective date, period, and services covered). Also, indicate if a service level agreement (SLA) exists for each of these services. Provide copies of the signed contracts and/or service-level agreements with exhibits and amendments for the providers considered significant or critical by the company.
- i. 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.
- j. Describe any business the company is conducting through electronic channels, indicating the type and volume of business and the date when it was implemented. Note: E-commerce methods of transmission might include voice recognition units (VRUs), the Internet, third-party extranets, and wireless and broadband communications media.

Information Technology Planning Questionnaire (ITPQ)

4. Information Technology Audits, Reviews, and Risk Assessments

- a. Provide the name, telephone number, and e-mail address of the partner of your company's independent external audit team and the internal audit director (or equivalent), if they exist.
- b. Provide a list of any IT audits/reviews performed within the past two years, including e-commerce areas, cybersecurity assessments and any IT-related reviews of financial significant 3rd party vendors Include the dates, review subjects, and who performed the audits/reviews (e.g., internal audit, external audit, SOC 1 Type II reports, SOC 2 Type II reports, SOC for Cybersecurity reports, cyber self-assessment tools, Sarbanes-Oxley, state insurance departments, governmental agencies, and/or any other contractor or affiliate that might have performed an audit/review).
- c. Provide copies of any IT audits/reviews, results documented in a report, performed within the previous two years such as SOC, HITRUST, and IT penetration testing including the associated remediation plans. Copies of other selected audits may be requested for review during the examination fieldwork.
- d. Provide the insurer's most recent IT control documentation and evidence of testing (as required by SOX or the Model Audit Rule).
- e. Arrange for a copy of the IT work included in the most recent audit workpapers to be provided from the company's external audit firm.
- f. Please provide all current assessments of the company's IT risks, whether internally or externally conducted.

5. Information Technology Security

- a. Provide the name, telephone number, and e-mail address of the chief security officer (or equivalent).
- b. Provide a copy of all IT security-related policies. If not explicitly described in the policies or if formal, written policies do not exist, please provide a detailed description of:
 - b.1 Data Confidentiality – Discuss how data elements are classified and who determines which individuals/roles have access to data elements.
 - b.2 Data Encryption – Discuss if confidential data is encrypted both at rest and in transit, including the process and methods of encryption.
 - b.3 System and Network Access Controls – Discuss how access is controlled (network-level, server-level, application-level, or a combination), which directory services are used for network access, whether authentication servers are used, etc.

Information Technology Planning Questionnaire (ITPQ)

- b.4 Multi-Factor Authentication – Discuss the current use of multi-factor authentication including where it's used, the type being used, and any plans for expanding its usage.
- b.5 Anti-virus/Anti-malware – Discuss the anti-virus/anti-malware software management program in place including the systems used and the strategy for keeping these products current.
- b.6 Security Logging & Monitoring – Discuss the process and tools used for logging and monitoring security events across network devices, servers, endpoints, systems, and applications. Also, discuss how the company aggregates and correlates this information across the breadth of monitoring points.
- b.7 Intrusion Detection & Prevention – Discuss the program in place to detect and prevent intrusion into the company's network and systems including the types of tools and technology being used.
- b.8 Vulnerability Management – Discuss the company's vulnerability management program including the scope of coverage, tools and techniques, frequency of scanning, reporting of known vulnerabilities, remediation, etc.
- b.9 Penetration Testing – Discuss the types and frequency of penetration testing and whether it's conducted by internal employees or external firms. Also, discuss whether the company uses advanced techniques such as red and blue team exercises.
- b.10 Security Awareness Training – Discuss the security awareness training program required for all employees including how often it's required and how participation is tracked. Also, discuss the contents of the training program and whether advanced techniques such as anti-phishing campaigns are conducted to reinforce the program.
- b.11 IT Asset Inventories – Discuss the inventory management program in place for physical devices, software, and applications.
- b.12 Third-Party Vendor Management – Discuss the program to assess and address security risks posed by third-party service providers including the group(s) responsible for risk ranking or tiering. Includes policies that address:
- departments involved in contracting and their responsibilities;
 - the vendor and third-party evaluation in risk assessment and business impact prior to outsourcing;
 - the security of sensitive data or systems that are accessible to, or held by, third-party service providers;
 - the use of encryption to protect sensitive data in transit and at rest;
 - notice to be provided in the event of a cyber security incident; and

Information Technology Planning Questionnaire (ITPQ)

- internal requirements for minimum terms to be included in contracts with third-party service providers.
- b.13 Data Loss Prevention – Discuss the program in place to detect and prevent protected information from leaving the company.
- b.14 Describe the insurer’s method for patch management of hardware, operating systems, database management systems, applications, etc. Include the system used and schedule for ensuring that planned patches are being applied in a timely manner.
- b.15 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.
- b.16 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.
- b.17 If not already provided elsewhere, please provide remaining IT security related policies.
- c. Provide a description of the types of sensitive information that is maintained or accessed by the company (e.g. Social Security numbers, protected health information, personally identifiable information, etc.) and the approximate amount of records containing each type of information. For each type of sensitive information, provide the number of outside vendors who have access to or maintain sensitive information.
- d. If applicable, provide a description of updates to the company’s controls and/or processes to ensure compliance with the General Data Protection Regulation (GDPR) or other applicable data protection requirements.

6. Information Technology (IT) Security – Incident Response

- a. Provide documentation of the response plan in place for cybersecurity incidents. (Note that this may be covered by the disaster recovery plan, but the plan provided should include consideration of IT-specific events.)
- b. Provide a listing of any instances in which confidential company or policyholder information was or was likely to have been breached. Include the following information in the response provided:
- How the event was detected.
 - Correlation of events and evaluation of threat/incident.
 - Resolution of threat, or creation and escalation of an appropriate work order.
 - Post-remediation analysis, including any resulting change in controls/operations to

Information Technology Planning Questionnaire (ITPQ)

mitigate the threat of event reoccurrence.

- Extent of involvement of senior levels of management.
 - Extent of expenses (including legal claims to be incurred) as a result of the incident.
 - Details on the information that was compromised (both in the quantity of information breached and the type of information that was breached).
- c. Have there been any security incidents since the last examination? Has OCI or any other regulatory agency been notified of such incidents? If so, please provide the dates of notifications, to which regulatory agencies they were sent, a summary of each incident, and a description of the remediation effort for each and its status.
- d. Provide the written Information Security Program required under Wis. Stats. § 601.952 (2021 Wisconsin Act 73). If the insurer is exempted or an exception to applicability under Wis. Stats. § 601.951(2), please indicate that this was disclosed in the Cybersecurity Annual Certification filed with this office.

7. System Development/Change Management

- a. Provide the name, telephone number, and e-mail address of the system architect/chief software engineer (or equivalent).
- b. Provide policies and procedures related to the insurer's system (solutions) development life cycle (SDLC). The life cycle would contain the phases from initial requests to post-implementation reviews. Indicate whether the insurer uses internal personnel and/or external vendors to develop and/or maintain its applications.
- c. 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.
- d. Provide the name, vendor, version number, and platform for all change management/system development software, if utilized.
- e. 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.

Information Technology Planning Questionnaire (ITPQ)

8. Business Continuity

- a. Provide the name, telephone number, and e-mail address of the individual responsible for maintaining, updating, and testing the company's business continuity and disaster recovery plans.
- b. Provide a copy of your IT business continuity and disaster recovery plans. Also, provide evidence of the last test results for the plans and management's resolutions of any test discrepancies.
- c. Identify the insurer's alternate sites for their IT systems and employees.
- d. Provide a description of your company's data and systems backup strategy, including your records retention policy.
- e. Provide a copy of the most current business impact analysis.

9. Financially Significant Systems

- a. If the company uses multiple platforms/systems to process financial transactions — including premium, claim, reinsurance, and investment transactions — include a reconciliation of amounts processed on each separate system to the total dollar amount processed during the prior year. Indicate whether the company anticipates any change in processing volumes during the current year.
- b. Identify and discuss other significant critical management reporting/operational systems, such as data warehouses, sales and marketing systems, communication systems, management dashboards, and any other management information systems.
- c. Discuss the accessibility and transferability of significant datasets (i.e., policy admin data, claims data, etc.). Indicate whether data is able to be queried and transferred in the event of an audit, new storage service provider, or other events that would require data to be relocated.