## EXHIBIT C EVALUATION OF CONTROLS IN INFORMATION technology (It)

The evaluation of controls in information technology (IT) is a critical element of the examination process. Determining the complexity of a company’s IT environment and the extent of work that must be performed to evaluate the controls in place is not always easy. Guidance on how to conduct an IT review is included within the General Information Technology Review guidance provided within Section 1, Part III of this Handbook. The tools included in this exhibit have been developed to assist the examiner in gaining an understanding of and evaluating the effectiveness of the company’s general IT controls in mitigating common IT risks, as outlined within the General Information Technology Review guidance.

There are two main sections to this exhibit. Part One, the Information Technology Planning Questionnaire (ITPQ), is a tool designed to assist the examiner in planning the extent of IT control work that might be necessary on an examination. The ITPQ provides the insurance department with a high-level overview of the company’s information technology environment. It is used to plan the scope and extent of IT control work to be performed and assist the examiner in determining which sections or risks included in the Evaluation of Controls in Information Technology (IT) Work Program (Part Two of this exhibit) should be prepared for the examination. To achieve maximum benefit, the ITPQ should be completed in advance of even normal examination planning, so that the examiner can begin planning what work the examiner will complete within Part Two.

Part Two of the exhibit is the Evaluation of Controls in Information Technology (IT) Work Program. The IT Work Program has been created to assist the examiner in identifying general IT risks, and to provide example controls and potential test procedures to assist the examiner in evaluating how well the company mitigates its general IT risks. Part Two of the exhibit replaces the Information Systems Questionnaire that has been included in previous editions of this Handbook, and should be used as the primary tool to evaluate a company’s general IT controls. For more information on how the two parts of the exhibit should be used during the examination, please refer to narrative guidance included in the General Information Technology Review caption in Section 1, Part III of this Handbook.

## PART ONE – Information technology Planning Questionnaire (ItPQ)

For the questions below, provide the requested documentation and the name, title, telephone number and e-mail address of the individual who will be most able to discuss and clarify the information presented.

If a particular section does not apply to your company, give a brief explanation of why it does not apply. All responses should be in the form of a separate summary memorandum, headed with the corresponding section label. Where possible, electronic responses are preferred.

### 1. Use of Information Technology

If the company does not process its business electronically, provide a narrative description explaining how the company’s business is processed. The remainder of this section does not need to be completed.

If the company only processes business electronically on a stand-alone personal computer and does not use networking technology, provide a narrative description explaining how business is processed, including the type of application software being used. The remainder of this section does not need to be completed.

### 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 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.

### 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. In addition, complete a separate Systems Summary Grid for each platform (see Attachment 1). A sample Systems Summary Grid is provided with this questionnaire (see Attachment 2).

d. Provide a narrative explanation of the application-level interfaces (manual and automated) among the various programs/platforms (e.g., claims system feeds into the accounting system).

e. 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.

f. 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.

g. 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.

### 4. Information Technology Audits, Reviews and Risk Assessments

a. Provide the name, telephone number and e-mail address for 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 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. 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. The workpapers should be provided no later than the response date identified for the IT Planning Questionnaire.

d. 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 for 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 exists, please provide a detailed description of:

* Data Confidentiality – Discuss how data elements are classified and who determines which individuals/roles have access to data elements.
* Data Encryption – Discuss if confidential data is encrypted both at rest and in transit, including the process and methods of encryption.
* 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.
* 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.
* Anti-virus/Anti-malware – Discuss the anti-virus/anti-malware software, and patch management program in place including the systems used and the strategy for keeping these products current.
* 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.
* 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.
* 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.
* 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.
* 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.
* IT Asset Inventories – Discuss the inventory management program in place for physical devices, software and applications.
* Third–Party Vendor Management – Discuss the program to assess and address security risks posed by third-party service providers including the group(s) responsible risk ranking or tiering.
* Data Loss Prevention – Discuss the program in place to detect and prevent protected information from leaving the company

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

1. 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.)
2. 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 mitigate 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 quantity of information breached and type of information that was breached).

### 7. System Development/Change Management

a. Provide the name, telephone number and e-mail address for the system architect/chief software engineer (or equivalent).

b. Provide an executive overview of the company’s system development life cycle (SDLC) and change-management methodologies and indicate whether the company uses internal personnel and/or external vendors to develop and/or change its systems or programs. Include discussion of the process used when purchasing application solutions.

c. Provide the name, vendor, version number and platform for all change management/system development software, if utilized.

### 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 (if not already provided in response to the above questions), including information on any contracts for alternate sites (i.e., named parties, site location, type of site, effective date and period covered). Also, provide evidence of the last test results for the plans and management’s resolutions of any test discrepancies.

c. Provide a description of your company’s data and systems backup strategy, including your records retention policy.

d. Provide a copy of the most current business impact analysis.

### 9. Financially Significant Systems

* 1. 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 total dollar amount processed during the prior year. Indicate whether the company anticipates any change in processing volumes during the current year.
  2. 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.
  3. Discuss the accessibility and transferability of significant datasets; i.e., policy admin data, claims data, etc. Indicate whether data can be queried and transferred in the event of an audit, new storage service provider, or other event that would require data to be relocated.

**Systems Summary Grid**

*For each primary hardware platform, list the application software products used in each of the insurance business cycles.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Hardware Platform (manufacturer/model)** |  | | | | | | |
| **Operating System\*** |  | | | | | | |
| **Access Control Software\*\*** |  | | | | | | |
| **Program Management Software** |  | | | | | | |
| **Database Management Software** |  | | | | | | |
| **Hardware Location** |  | | | | | | |
| **Business User Location(s)** |  | | | | | | |
| **Individual Responsible** |  | | | | | | |
| **Process/Application** | **Product Name and Version** | **Software Source:** **Developed Internally Purchased – Not Modified Purchased – Customized Outsourced/Service Center** | **Developer/Vendor** | **Application Support:**  **Internal/External (Provider Name)** | **Date of Initial Implementation** | **Date of Last Significant Update** | **Is the data stored in an accessible and readily transferable format? (Y/N/NA)** |
| **Policy Management (including premium-transaction processing and policy record management)** |  |  |  |  |  |  |  |
| **Claim Management (including claim-transaction processing and record management, and reserving)** |  |  |  |  |  |  |  |
| **Financial Reporting (general ledger and accounting)** |  |  |  |  |  |  | N/A |
| **Investment and Fund Management (including investment-transaction processing and record management)** |  |  |  |  |  |  | N/A |
| **Reinsurance Management** |  |  |  |  |  |  |  |
| **Producer Management (including commissions-transaction processing and agent record management)** |  |  |  |  |  |  |  |
| **Data Warehouse / Data Mart** |  |  |  |  |  |  |  |

**NOTE: Make as many copies as necessary to represent every primary hardware platform being used. These might include mainframe, minicomputer and/or network server systems. Additional financially significant applications should be inserted as needed.**

\* e.g., z/OS, z/VM, Clearpath, OS/400, i5/OS, Windows Server 20XX, Open Enterprise Server, Linux, Unix, AIX, Open Solaris, etc.

\*\*e.g., RACF, Top Secret, ACF2, BSafe, Active Directory, eDirectory, Solaris.

**Systems Summary Grid — Sample**

*For each primary hardware platform, list the application software products used in each of the insurance business cycles.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Hardware Platform (manufacturer/model)** | IBM AS/400 Model 840 | | | | | | |
| **Operating System** | OS/400 v4r3 | | | | | | |
| **Access Control Software** | OS/400 and Client Access/400 | | | | | | |
| **Program Management Software** | Job Scheduler for AS/400 | | | | | | |
| **Database Management Software** | DB2 Universal Database for AS/400 | | | | | | |
| **Hardware Location** | Company’s home office | | | | | | |
| **Business User Location(s)** | Company’s home office | | | | | | |
| **Individual Responsible** | John Smith, VP - Underwriting | | | | | | |
| **Process/Application** | **Product Name and Version** | **Software Source:** **Developed Internally Purchased – Not modified Purchased – Customized Outsourced/Service Center** | **Developer/Vendor** | **Application Support:**  **Internal / External (Provider Name)** | **Date of Initial Implementation** | **Date of Last Significant Update** | **Is the data stored in an accessible and readily transferable format? (Y/N/NA)** |
| **Policy Management (including premium-transaction processing and policy record management)** | PMS v6r2 | Developed internally | By company, using Cobol, C++ | Internal | 09/1987 | 10/1999 | Y |
| **Claim Management (including claim-transaction processing and record management, and reserving)** | Not on this platform |  |  |  |  |  | N/A |
| **Financial Reporting (general ledger and accounting)** | Not on this platform |  |  |  |  |  | N/A |
| **Investment and Fund Management (including investment-transaction processing and record management)** | Not on this platform |  |  |  |  |  | N/A |
| **Reinsurance Management** | Not on this platform |  |  |  |  |  | N/A |
| **Producer Management (including commissions-transaction processing and agent record management)** | PMS v6r2 | Developed internally |  | Internal | 09/1987 | 10/1999 | Y |
| **Data Warehouse / Data Mart** | Oracle Database | Developed internally |  | Internal | 09/1987 | 10/1999 | Y |

**NOTE: This page is for informational purposes only — it does not have to be returned.**

## EXHIBIT C IT REVIEW STANDARD PLANNING MEMOrandum

The following is an illustration of an IT Review Standard Planning Memorandum to assist examiners in documenting the results of the IT planning process. This illustration includes some basic elements that IT examiners may want to incorporate into the IT planning memo to adequately document the IT review plan.

**Salutation**

This section should be in any format the state deems appropriate for its purposes. At a minimum, all states that are placing reliance on the IT review should be included in the distribution of this memo.

**Background and Scope**

This section should identify the following: the companies under examination (domiciliary state and type may also be included as relevant), examination “as of” date and period under examination, and the examination team and/or contractors used.

**Meetings with Critical Personnel**

**Examiner-In-Charge and Other Financial Examiners**

This section should summarize the pre-examination meeting with the EIC and other examiners (e.g., examiners from other states participating in the financial examination). It should include the following: the date and time the meeting occurred, a summary of each topic discussed, operations considered significant to the company (e.g. Claims Handling, Premium Billing, etc. if known at this time), prior examination findings, and any other concerns noted.

**Financial Analyst**

This section should summarize the meeting with the financial analyst and include the following: the date and time the meeting occurred, a summary of each topic discussed, relevant items from the Insurer Profile Summary, and any concerns regarding the company’s systems identified as a result of the financial analysis process.

**Company Personnel**

This section should summarize the preliminary meeting with company personnel and include the following: the date and time the meeting occurred, a description of who was in attendance (examiners and company representatives) and a summary of each topic discussed including who provides the IT services to the insurer, what the size of the IT operations are, where IT personnel are located, whether any recent changes have been made to the IT control environment, whether any key operations or functions are outsourced, and who the key company contacts are for the IT review.

**Review Documentation and Issues Identified**

**Work of Others**

This section should identify work performed (including any issues identified) by outside parties who have reviewed the IT function. This section should also identify and provide a preliminary assessment on how the work of others will be relied upon. Examples of the work of others that may be utilized include work done by other states, external CPAs, the company’s internal audit or risk management function and third-party consultants used by the company. This work could include, but is not limited to, Sarbanes-Oxley 404 or Model Audit Rule workpapers.

**ITPQ**

This section should summarize results of the ITPQ and include a reference to the completed document.

At the conclusion of this section, the IT examiner should document any issues identified during the meetings or from reviewing the sources listed above that will be considered while conducting the IT review. They should also develop a preliminary assessment of the general control environment identified in the examination process.

**Budget**

**Detailed Time Estimate, Staffing and Schedule**

This section should include an estimated time budget, staff resources to be used, and a schedule of when the IT work will be performed. This section would also include timelines for deliverables and a representative draft of the work program expected to be performed.

Note: The IT examination budget should include an initial estimate of time, which is subject to change based upon the availability of information, the extent of testing necessary and any other relevant factors.