**CHAPTER 2 – INFORMATION SYSTEMS**

[I. INTRODUCTION 129](#_Toc414874800)

[A. Information Systems ─ Requirements and Considerations 129](#_Toc414874801)

[B. Overview 129](#_Toc414874802)

[II. TAKING CONTROL 130](#_Toc414874803)

[A. Assurance of Data Maintenance and Availability 130](#_Toc414874804)

[B. Security and Data Privacy 131](#_Toc414874805)

[C. Systems Processes for Conservation, Rehabilitation and Liquidation 134](#_Toc414874806)

[D. Staff 134](#_Toc414874807)

[E. Hardware 135](#_Toc414874808)

[F. Systems Software and Application Software 136](#_Toc414874809)

[G. Internet/Intranet/Web site 137](#_Toc414874810)

[H. Newer Technologies 137](#_Toc414874811)

[I. New Business Strategies 137](#_Toc414874812)

J. Remote Work

[III. SYSTEM MANAGEMENT AND CONTROL 137](#_Toc414874813)

[A. Systems Operations 138](#_Toc414874814)

[B. Input/Output Controls 138](#_Toc414874815)

[C. Maintenance/Updates 138](#_Toc414874816)

[D. Networks 138](#_Toc414874817)

[E. System Location 138](#_Toc414874818)

[1. Outsourced Operations / Hosted Systems 138](#_Toc414874819)

[2. Shared System 139](#_Toc414874820)

[3. Affiliate Functions 139](#_Toc414874821)

[F. System Ownership 139](#_Toc414874822)

[G. Conversion 139](#_Toc414874823)

[H. Common Systems Applications 140](#_Toc414874824)

[1. General Ledger and Accounting Books 140](#_Toc414874825)

[2. Claims 140](#_Toc414874826)

[3. Accounts Current 140](#_Toc414874827)

[4. Premium Financing 140](#_Toc414874828)

[5. Marketing 141](#_Toc414874829)

[6. Investments 141](#_Toc414874830)

[7. Reinsurance 141](#_Toc414874831)

[8. Email 141](#_Toc414874832)

[9. 141](#_Toc414874833)Large Deductible

10. Other

11. End User Computer (EUC) Applications

[IV. INFORMATION SYSTEMS DELIVERABLES 142](#_Toc414874834)

[A. Considerations Regarding the Insurer’s Historical Business Practices 142](#_Toc414874835)

[B. Volume and Geography of Business 142](#_Toc414874836)

[C. Types of Business Written 143](#_Toc414874837)

[D. Corporate Structure 143](#_Toc414874838)

[E. Sources of Production 143](#_Toc414874839)

[F. Claims Handling 143](#_Toc414874840)

[G. Affiliated Companies 144](#_Toc414874841)

[H. Foreign Exchange Considerations 144](#_Toc414874842)

[I. Existing Systems 144](#_Toc414874843)

[1. Systems Documentation 145](#_Toc414874844)

[2. Process Documentation 145](#_Toc414874845)

[3. User Documentation 145](#_Toc414874846)

[J. Data Validation 145](#_Toc414874847)

[K. Hardware Requirements 145](#_Toc414874848)

[1. 145](#_Toc414874849) Application Servers

[2. 145](#_Toc414874850) Networks

[L. Additional Considerations 146](#_Toc414874851)

[1. PCs, Laptops and Terminals 146](#_Toc414874852)

[2. Environmental Considerations (Climate Control) 146](#_Toc414874853)

[3. Environmental Considerations (Power Consumption) 146](#_Toc414874854)

[M. Liquidation Considerations 146](#_Toc414874855)

1. [Property and Casualty Guaranty Association 146](#_Toc414874856)Funds

A. Compliance with UDS

B. Insolvency Data Transfers

i. Evaluation

ii.Extractions

iii. Processing

iv. UDS Production

C. Priority of UDS Records

2. Life and Health Guaranty Association Funds

A. Specific Data Needs

B. Timing Considerations

C. Secure Data Transfer

[3. Compliance with UDS 147](#_Toc414874857)

[V. IMPLEMENTATION 147](#_Toc414874858)

[A. Retention 147](#_Toc414874859)

[1. Verify Capabilities 148](#_Toc414874860)

[2. Verify Condition of Hardware and Adequacy/Integrity of Software 148](#_Toc414874861)

[3. Assure Adequate Security and Disaster Recovery 148](#_Toc414874862)

[4. Devise Assessment Methodology 148](#_Toc414874863)

[B. Enhancement 148](#_Toc414874864)

[1. 148](#_Toc414874865)

[C. System Replacement 149](#_Toc414874868)

[1. Contract with Vendor 150](#_Toc414874872)

[2. Document and Back Up Old System 151](#_Toc414874875)

[3. Shut Down and Disposal of Old System 151](#_Toc414874876)

D [. General Concerns 151](#_Toc414874877)

[. Implementation of UDS 151](#_Toc414874878)

I. INTRODUCTION

A. Information Systems ─ Requirements and Considerations

The management of an insurance company in receivership is, to a great extent, the management of information. To successfully perform receivership functions and fulfill all obligations and responsibilities, the receiver must effectively utilize system resources.

The nature of the receivership, conservation, rehabilitation or liquidation will affect systems requirements. The type of business written by the insurer, whether Life, Annuity, Accident & Health, Property, Casualty, Liability, Surety, Title, Workers’ Compensation or other lines, will also affect systems requirements for the receiver. Systems needs, and the timing of those needs, will be different in a conservation or rehabilitation process than in a liquidation process.

Because of the importance of securing the data of any company subject to a receivership, immediate attention must be given to obtaining a backup of the data, and consideration given to obtaining a complete backup of the systems.

In all conservation and rehabilitation efforts, the immediate focus is ongoing insurance company operations and the changes necessary to help ensure the viability of the company. A priority focus will be on analysis and management of information to support decision-makers. Realizing potential opportunities such as mergers, divestitures and loss portfolio transfers will require considerable information on all aspects of the business. Throughout the conservation or rehabilitation process, it is necessary to continually consider potential future requirements, such as release of the company to existing management, transferal to new owners (of the insurance business or the entire company) or transition to liquidation. In doing this, the receiver will need to look ahead to what systems requirements may be needed in the future and make arrangements so they are in place when needed.

Liquidation processes will require a focus on timely conclusion of normal operations and an accurate final statement of assets and liabilities. Systems support will be required for estate liquidation processes, including interfaces with guaranty associations, management of claims against the estate, recovery of all receivables, pursuit of causes of action to benefit the estate, and disposition of physical assets. Compliance with all legally required processes and documentation to support compliance are crucial.

B. Overview

The chapter has been divided into the following parts:

* Taking Control
* System Management and Control
* Information System Deliverables
* Implementation

These sections are in the order that anticipated issues may arise during the receivership process. Insurers will vary in size and degree of system sophistication. Each insurer will present varied problems and issues dependent on the situation. In general, companies going into receivership have often neglected internal controls which may have resulted in many control issues related to the company, its systems, and completeness and accuracy of its data. The guidelines, considerations and checklists provided herein are very broad in nature. Management judgment will best determine the appropriate degree of applicability or whether alternate processes are required.

Generally, though, the receiver will first have to gain full control over the systems. Then the receiver can develop a more in-depth knowledge of processes to determine the best manner to meet the needs of the receivership.

This chapter provides suggestions and guidelines as to management of systems, issues resolution and problem avoidance in support of receiverships. While this chapter is intended to be as comprehensive as possible, it is not all-inclusive. Other methodologies may be employed to achieve the same goals in a satisfactory manner, and issues not addressed here may arise. In every receivership, no matter the size or characteristics, the receiver must exercise judgment beyond that which can be given by texts and checklists. Still, the materials provided here should assist in the exercise of that judgment.

This chapter focuses on issues primarily related to automated information systems. When considering the scope of information systems, however, it is important to apply a holistic perspective that considers systems as being made up of processes and procedures—both automated and manual, including human judgment—in performing tasks.

Other chapters of this handbook, specifically the accounting, claims and reinsurance chapters, address many issues related to information and manual processes. Information systems are an integral part of the operations of an insurance company and any receivership. However, not every system need must be met with a fully automated solution. Costs and benefits must be carefully analyzed.

There are detailed information systems checklists in Chapter 1 that should be consulted in advance if possible and then throughout the receivership process.

II. TAKING CONTROL

This section covers the activities necessary for a receiver to take control of an insurer’s information systems in an effective manner. Generally, the checklists provided address a worst-case scenario: an information systems department that lacked control, where many key people have departed, and where documentation is incomplete, inaccurate or non-existent. The checklists should be completed for documentation purposes, noting those areas of the checklist that do not require action.

A. Assurance of Data Maintenance and Availability

The insurer’s data will be in records and files stored within the computing infrastructure. It is important for the receiver to determine location, purpose, structure and content of data files related to all business applications. Given the complex and detailed nature of this information within the context of a contemporary liquidation as well as the security concerns that have increased significantly, it is desirable that the receiver have relevant background information prior to the signing of a liquidation order if possible. Ideally, this information would be shared with the affected guaranty funds in advance of liquidation. These steps will greatly enhance efficiency once liquidation is underway and result in even more dependable and timely protection of policyholders. A good starting point to gather pre-takeover information is the systems summary grid and any IT related workpapers from the company’s most recent financial examination. Reviewing this information in advance of takeover will give the receiver a head-start for what to expect. It is essential that the receiver’s information systems personnel work with the other departments within the insurer to assure that all the available information has been captured and can be retrieved and reviewed at a later date. All system storage devices, including database servers, Web servers, file servers, application servers and related storage media should be reviewed as sources of company information. End-user computing (EUC), such as spreadsheets, databases, etc., that are maintained by business departments should also be considered. EUC applications can easily fall through the cracks if there is no central repository of the EUC applications and there is turnover of personnel who maintain the EUC.

Regardless of system ownership issues, it should be the practice to immediately back up all available data on all systems. Where possible, employee workstations, including laptops, should be backed up as well. At a minimum, key employee workstations and laptops as determined by receivership management should be backed up.

For each major application, the receiver should obtain the following information:

* name of application program;
* Vendor contact information, if applicable;
* Vendor contracts
* sources of data (automated or manual);
* references to and storage of source data;
* complete tables of all codes used (database schema and data dictionary, when available);
* Type and frequency of processing cycles;
* narrative descriptions, in non-technical language, of capabilities and use;
* Administration procedures, including responsibilities of staff;
* Administrative user names and passwords for the application (also, if administration is restricted to a particular workstation or terminal);
* systems error messages and appropriate actions;
* distribution of output reports and samples if possible;
* usage and control of reports;
* links to other system modules; and
* Backup procedures including storage and retention schedules

B. Security and Data Privacy

One of the highest priorities of the takeover phase of systems operation should be the review or initiation of system and data security procedures. The existing data may be the most reliable or only record of the assets and liabilities of an estate, and the need for securing this information is vital. In general, when the receiver takes control of the insurer’s IT systems, access should be restricted until the receiver is confident that data cannot be altered by unauthorized parties. The receiver should identify the levels of access given to employees and any third parties for all applications and limit access as necessary. Remote access should be restricted to authorized users and only to users with encrypted laptops from trusted networks, such as corporate offices, wirtual private networks (VPNs), etc.

In conducting a security review, the receiver is cautioned that relevant and important data records may reside on mainframe computers, servers, PCs, tablets, cellular phones on the systems of contractors or any combination of all of these. Historical information systems records in the form of backup tapes, which may be stored off-site, may be of equal or greater importance and should not be overlooked. The insurer may also maintain a website (see section G—Internet/Intranet/Website), which should also be included in the security review.

One of the primary purposes of the security program is to obtain and safeguard all required data records, which entails the identification and securing of this data. Such a program should include the creation and implementation of a plan to limit access to the systems and data to those with a proven need. The program should enable the receiver to identify changes made to the system and the individual responsible for these changes. The ability to track changes to systems may be limited by the existing company software applications. The information systems checklist in Chapter 1—Takeover will provide the receiver with an overview of the most important aspects of a proper system security program.

In addition to securing the data of the company for conservation, rehabilitation or liquidation information, it is essential to ensure the secure handling of non-public personal information. Insurance companies and other financial institutions are subject to a variety of state and federal statutes and regulations regarding the protection and non-disclosure of non-public personal financial and health information. Some specific requirements are imposed by federal statutes such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, among others. Additional requirements may be found in state statutes, data security breach laws and in state insurance regulations, including those based upon the NAIC Privacy of Financial Information Regulation 2000. Ongoing compliance with applicable data privacy and security laws and regulations is essential to help further the primary goal of all insurance receiverships—the protection of insurance consumers.

Accordingly, the receiver should take steps to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security and integrity of such records; and protect against unauthorized access to or use of such records, any of which could result in substantial harm or inconvenience to insureds or claimants.

The company may have included cyber security self-assessment or audits/ review as an integral part of its enterprise risk management program. If so, the receiver can obtain recent IT audits/ reviews such as: e-commerce areas, self-assessment and IT related reviews of significant third-party vendors. These reports could be in the form of audits/reviews (e.g. internal audit, external audit, SOC type I and II reports, or other contractor affiliate audit reviews. In the absence of a company policy that meets these criteria, it is essential that the receiver implement a data security policy and procedures suitable to the particular receivership. The procedures should be appropriate for the size, complexity and structure of the company and its data. There is guidance contained in the NAIC Receivership Data Privacy and Security Procedures for Property and Casualty Insurers in Liquidation, should address potential security threats in three areas: administrative, technical and physical.

See https://content.naic.org/cmte\_e\_receivership.htm for this document and other helpful receivership tools, such as the NAIC receivership Data Privacy and Security Procedures policy. Since staffing is often not available to write a new data security policy specific to each receivership, the NAIC’s security policy and procedures document referenced above may serve as a guideline which could be edited for purposes of individual receiverships.

Administrative Safeguards

* Designate an individual who is responsible for oversight and compliance with security procedures.
* Publish a written policy statement setting forth the company’s (receiver’s) intention to protect the confidentiality of sensitive customer data from anticipated threats or hazards. The receivers’ policy should include two important components, namely incident handling and communications protocols should an incident occur. Incident handling – General and specific procedures and other requirements to ensure effective handling of incidents, including prioritization, and reported vulnerabilities. Determine if there are procedures related to handling cyber-security incidents. 2) Communications – Requirements detailing the implementation and operation of emergency and routine communications channels amongst key members of management.
* Prepare and distribute written procedures to appropriate personnel and service providers outlining specific steps that must be followed in storage, transmission, retrieval or disposal of sensitive customer information.
* Require all employees and other users to sign an agreement to follow the data privacy and security standards.
* Evaluate potential security threats from existing staff, e.g., disgruntled employees.
* Evaluate service providers regarding the handling of sensitive customer information.
* Train and instruct employees as to their individual responsibilities regarding data privacy and security.
* Train staff to recognize potential security threats, including intentional or inadvertent downloading of malware.
* Check references and criminal backgrounds prior to retaining new staff.
* Periodically test and monitor the effectiveness of the security procedures.
* Evaluate and adjust the security procedures in light of changing circumstances.
* Use appropriate oversight or audit procedures to detect improper disclosure or theft of customer information.
* Implement procedures for notifying appropriate authorities and affected individuals if non-public personal information was subject to unauthorized access.
* Impose disciplinary measures for breaches of privacy and security rules.
* For laptops that are used outside of the office require encryption and the use of a VPN to connect
* Establish a remote work policy for remote workers which includes policies for where work is to be performed with a secured network connection only and safeguards that must be in place associated with their computer and other data (paper files, etc.) used outside of the office.
* Add multi-factor authentication where possible, including email, application servers and company networks.
* Disable USB ports on all company laptops and computers.

Technical Safeguards

* Use password-activated screensavers.
* Use strong passwords unique and independent of any personal passwords.
* Change passwords periodically.
* Prohibit posting of passwords anywhere except for a secure password manager.
* Sensitive information must be encrypted both in transit and at rest.
* Limit or do not allow storage of sensitive information on portable devices such as laptop computers or removable drives or other storage media; if sensitive information is stored on mobile devices, it must be encrypted.
* Limit access to customer information to employees who have a business reason for seeing it.
* Store electronic customer information on a secure server that is accessible only with a password.
* Avoid storage of sensitive information on a machine with an Internet connection.
* Transmit data electronically only through secure, encrypted connections.
* Implement procedures for the prevention, detection and response to attacks, intrusions or other system failures.
* Regularly check with software or systems vendors to update security patches.
* Maintain up-to-date firewalls.
* Back up all customer information regularly.
* Ensure that former employees do not have access to any information systems.
* Ensure that remote access to all information systems is limited to authorized users.

Physical Safeguards

* Lock rooms and cabinets where sensitive data or data storage equipment is kept.
* Ensure the area where data storage equipment is kept is well ventilated, is capable of maintaining an appropriate temperature for the equipment is free from water hazards, and is not visible through a window to the outside the office.
* Allow access to information storage areas only to those individuals with a need for access.
* Require employees to secure sensitive information in their work areas whenever they are not present.
* Dispose of sensitive information in a secure manner.
  + - * Hire or designate a records retention manager to supervise the disposal of records containing non-public personal information.
      * Shred sensitive information recorded on paper.
      * Destroy or effectively erase all data when disposing of computers, diskettes, magnetic tapes, hard drives, copy machines, fax machines, flash drives, or other storage media containing sensitive information.
* Ensure that storage areas are protected against physical hazards such as fire, flood or physical intrusion.
* Maintain a current inventory of all computer equipment.
* Collect keys, computer equipment and other storage devices from employees and disable employee access to company systems prior to termination.
* Develop a computer disposal policy/procedure which includes a strategy for the maintenance and tracking of hard drives.

C. Systems Processes for Conservation, Rehabilitation and Liquidation

Systems emphasis for a conservation or rehabilitation effort typically focuses on timely and accurate processing, resolution of issues and providing information for management. The additional considerations regarding liquidations outlined below may apply in some conservations or rehabilitations.

In a liquidation action, beyond timely processing and termination of operations, there are additional considerations related to accurate identification and valuation of all assets and liabilities of the insurer:

* Liquidation notices and proof of claim processes;
* Policy cancellation and/or non-renewal notices;
* Unearned or return premium calculation;
* Agents’ balances calculation and collection;
* Unearned commission calculation and collection;
* Policyholder contract assessment calculations, where applicable;
* Reinsurance recoverable tracking and collection;
* Transmission of claims data between guaranty associations and receivers See Section IV. M. in this chapter for unique standards such as UDS and others that apply to the different types of insurers.
* Salvage and subrogation accounting and collections;
* Inventory and liquidation of physical assets; and
* Transmission of policyholder records and data to assuming insurer for life and health insurer receiverships.

Some systems will have built-in capabilities for creation of the above items, others may not and an extract from the system may need to be taken and manipulated to achieve desired results. Also, when using Company data to create reports, it is important to discuss the completeness and accuracy of the data with company staff since often companies in receivership may have issues where systems are not working properly or other reasons why it is known that the data on the system may not be complete and accurate.

D. Staff

Assuming control of the insurer’s information systems is critical to a successful receivership. Gaining control of the information systems usually will be most cost-effectively accomplished through use of the existing staff. Since it is important to gain control of these areas at the onset of the takeover process, it is best to assess the staff at the inception of the receivership to determine how they can assist in the receivership process. In some cases, a plan may need to be devised to provide information systems personnel with incentives to continue their employment as the receiver requires. Even so, it is often difficult to retain IT personnel, so it is important to perform as much knowledge transfer as possible at the onset of a receivership.

After assessing the experience, potential contribution, commitment and cost of the staff in the context of the goals of the receivership, the receiver may choose to reduce staff. The allegiance of the systems staff, as with other functional areas, may be questionable, and the possibility of sabotage exists. Sabotage of information systems is hard to detect and may be extremely expensive to repair. Because of the potential exposure to loss of critical data, the systems staffing decisions should be made quickly and decisively. Where possible, restrict full access to any systems, equipment or work areas until staffing decisions have been made and implemented.

E. Hardware

In taking control of systems operations, frequently the first concern of the receiver is to inventory and secure the hardware. The hardware may be owned, leased or shared, and arrangements should be made for continued use to the extent the receiver finds necessary to maintain continuity, especially at the onset of the receivership. The receiver will also want to identify collateral equipment located at branch operations, the homes of employees, related entities, storage facilities, other insurers and agencies. All equipment should be inventoried, including all types of portable computers, tablets, cellular phones, and communication equipment.

Contingency plans may need to be developed in case the receiver must cease use of the systems in order to liquidate components.

Maintenance of the hardware should be done on schedule, and the environment should be maintained to prevent loss of data or system outage.

The configuration of the hardware should be specifically identified and cataloged. The computing hardware environment may be made up of a combination of mainframes, mid-size computers, client servers and PC-networked equipment.

For mainframe or mid-size computers, the most important components of their configuration will be:

* CPUs (central processing units);
* data storage devices;
* printer(s);
* tape drives;
* terminals;
* Data communications equipment; and
* any other peripheral devices.

Similarly, all PC-network configurations should be identified and may include:

* Network servers, firewalls, intrusion detection devices, routers, switches, etc.;
* Mail servers;
* Web servers;
* Imaging servers;
* PCs and laptops;
  + Make and model
  + Internal storage devices
  + RAM
  + Clock speed
* external storage devices;
* printer(s);
* keyboards and other input devices, e.g., scanners, microphones and pointing devices such as a mouse, track ball, touch pad or other sensor;
* monitor(s);
* any LAN-connected devices (high-performance cables, terminals, file servers, printers, modems, etc.);
* Data communication equipment such as cell phones, tablets, and any other internet connected devices. w; and
* UPS (Uninterruptible Power Sources) and generators.

F. Systems Software and Application Software

Systems software includes broad and varied types of software such as operating systems, utility systems, database management, virus protection, e-mail systems, and any other software that is not classified as business application software. These systems will be commercially available systems that are closely related to hardware components.

Application software directly supports business functions and may be licensed, commercially available software or may be custom-developed.

Taking control of the software requires a different approach than that applied to most of the other assets of the insurer. This is especially true for custom-developed software. Control of the software initially means knowledge of the software in place and its intended purpose to the insurer. For licensed software, it is necessary to have an accurate inventory of the software, to have proof of licenses and status of maintenance contracts to ensure authorized legal use, and to obtain updates from the software vendor. In the case of custom-developed software, it is necessary to identify the developer(s), whether contract or in-house, and any relationship with the insurer. It may be necessary to retain an intellectual property attorney to determine the company’s rights to the software. The program source code must be physically located; whether on the company’s servers or elsewhere, and rights to the source code must be determined. Succession planning information should be obtained for software developed by a sole proprietor contractor.

It will be necessary for the receiver to identify the applications that address the following functional requirements:

* Marketing and sales management;
* Agency interface;
* Customer service;
* claims management;
* Policy issuance and endorsement processing;
* premium billing and accounting;
* reinsurance;
* Policy receivables and payables;
* cash receipts and disbursements;
* general financial management and reporting;
* investment management;
* Data warehouse
* word processing and publishing;
* Company Web site; and
* External interfaces and data sources.

G. Internet/Intranet/Website

Increasingly, insurers are utilizing the Web as a tool for their business and have Web-based technologies implemented. The receiver should review the company’s Internet content and application processes. The receiver should also ascertain what Web services are being provided by the insurer and to the insurer by external vendors. Internet service providers should be documented and service contracts obtained and reviewed. The receiver should assume the role of Web-master or make arrangements with a third-party vendor. This may require that external Internet service providers be notified of the change and new passwords issued. Firewalls, Web servers and proxy servers, routers, and other Web- and network-related items should be reviewed for legal, data, ownership, confidentiality and security issues. Integration with the receiver’s own Web usage and applications should be reviewed and considered.

If premiums are being collected over the internet the receiver should ascertain the Company is PCI compliant. PCI compliant organizations will have an annual PCI assessment. If the Company is not PCI compliant it is recommended that areas of non-compliance be mitigated or the ability to take electronic payments removed. The receiver should also understand the process for collecting electronic payments and what if any action needs to be taken by company or receiver personnel to collect and record such payments.

H. Newer Technologies

As emerging technologies become more common in the field of insurance, the receiver should be aware of newer technologies that may have been implemented by the insurer.

Imaging systems and distributed processing of underwriting, claims, collections and other operations all have special requirements that the receiver will need to address. An analysis will be needed to determine system ownership, hardware and network components used to support these implemented technologies, and vendor involvement in the support and maintenance of these systems. These should all be reviewed by the receiver to determine risk, cost benefit of continuation, conversion and receivership issues.

I. New Business Strategies

The receiver should ascertain system ownership and system usage issues such as leased systems, outsourced contractors or vendors performing work or services for the insurer, system availability, and security. The receiver should verify that there will be sufficient access to data and functions necessary to perform the receivership processing. The receiver should identify all the involved parties, what services, hardware and software have previously been provided, what is currently being provided and at what cost.

**J. Remote Work**

In 2020, the COVID-19 pandemic not only created new challenges for the administration of receiverships where activities were carried out remotely from the insurer’s corporate offices, but also brought about changes in how insurance companies operate. Specifically, more insurers have allowed staff to move to remote work or hybrid (partially remote) work environments, as well as to rely more on paperless electronic records and less on (or even eliminate) hardcopy documents. This has led to the need for use of platforms that allow for secure remote access by authorized staff and enhanced data security.

A few IT considerations for the receiver, if the insurer has staff who work remotely, or if the receiver’s access to on-site IT systems is limited due to a disaster, include but not limited to:

* Review the insurer’s Disaster Recovery and Business Continuity Plan for remote access and maintenance of systems
* Identify and understand the critical automated systems that need to continue operating to support business functions, the persons responsible for critical systems, location and back-up systems (i.e., colocation data center).
* Review the insurer’s Work-From-Home Policy to gain an understanding of the roles and responsibilities of staff working remotely
* Understand which employees have remote access to systems and/or may have company owned equipment at home (i.e. laptops, monitor, printers and office furniture)
* Understand what business systems, programs, technology, (e.g., virtual private network (VPN), phone/communication systems) that have been established for employees to work remotely and the internal controls over those systems
* Understand the insurer’s cybersecurity controls and data security protocols that are in place to facilitate secure remote access to the requisite systems and data by off-site staff

III. SYSTEM MANAGEMENT AND CONTROL

The preceding section of this chapter dealt with the first task facing the receiver when taking over a distressed insurer—establishing control. This section will guide the receiver through a more detailed continuation of that process by identifying the areas of management and control.

A. Systems Operations

The hardware, software and personnel who keep systems running make up the systems operations. In many mainframe computer operations, the users of the application software may never have seen the actual data center and its various related equipment. Systems operations are typically supported by an internal or external help desk support and network administration.

B. Input/Output Controls

Many application systems both receive and send data to and from other application systems, which can be internal, external or both. This data may be in the form of removable tapes or disks that are visible, or may be in the form of files/databases that reside on non-removable disks and are created by one application system, then later input or electronically transmitted to another application system or cloud storage The input, output and transmission of all data should be subject to controls, which may range in form from a simple notation indicating the application name/date/time to a more complex procedure (manual or automated) that balances or validates record counts and control totals. Controls may also be part of the application program and be unseen until an error or notification prompt occurs.

The receiver should verify that these internal and external controls are in place and fully documented. After the urgent control matters have been addressed, areas where these controls might be improved will be noted through the operation of the receivership.

C. Maintenance/Updates

Some licensed software is automatically maintained and upgraded by its vendor. In many instances, the end user or owner identifies the availability of, and acquires, updates. The receiver should be aware of the availability of updates to software used by the insurer. For some mainframe and mini-computer configurations, current maintenance costs may exceed the cost of converting to a PC-based system. The inventory made of the software and its licensing is important to ensure proper maintenance and may impact business decisions regarding continued utilization of the existing system.

D. Networks

Network systems in which an on-premises file server, cloud server or central processing unit forms the hub of a network of interrelated PCs are now common. The age and adequacy of the networks should be ascertained and the availability of maintenance and updates determined. Networks may include not only the insurer, but other affiliates or holding company of the insurance company; thus, the ability to separate the network into independent components may be problematic. See also Section III.G. below regarding segregating commingled records and data.

E. System Location

The physical location and management of the computer system is also an important issue. Many computer systems are completely internal to the insurer. That is, all of the hardware and software components of the system are within the insurer’s premises and control. The benefit of this is that the information systems operation is entirely dedicated to, and focused upon, the objectives of the insurer. However, this also requires that all aspects of the systems operation be managed and controlled by the receiver. To maintain and control an entirely in-house operation, it is vital that the receiver have sufficient systems staff in place. In instances where the receiver has determined that the responsibility and expense of an in-house information systems operation are not desirable, he or she may look to alternative arrangements, such as out-sourced operations.

1. Outsourced Operations / Hosted Systems

A service provider may have performed some or all of the data processing functions. The arrangements for this service may vary from hosted systems to a service provider maintaining the company’s internal systems. The receiver’s staff should perform an evaluation of the facilities and competency of the service provider. The receiver should verify that existing contracts will provide sufficient flexibility and accessibility to meet the receiver’s needs; new contracts may need to be executed.

2. Shared System

The insurer may share data processing systems with affiliates or other companies, or have its data is hosted and handled by a third party The receiver should ascertain to what extent the system will be available and whether confidentiality will be compromised. The legal issues arising with shared systems should be carefully considered. In the event that the receiver determines that a shared system is not adequate for the receivership’s needs, a plan will need to be developed to migrate the insurance company data to another system or dedicated cloud under the control of the receiver or a host company that is independently contracted with the receiver. The receiver may wish to retain an independent consultant to assist with the migration. See also Section III.G. below regarding segregating commingled records and data. See Chapter 9, Section VII for discussion of legal issues relating to information systems and data processing.

3. Affiliate Functions

Some information systems functions may be performed internally, while others are performed by affiliates. Again, the receiver should verify that there will be sufficient access to data and functions necessary to the receivership proceeding. The receiver should also review the cost of any services provided by affiliates. See also Section III.G. below regarding segregating commingled records and data.

F. System Ownership

Systems may be owned outright by the insurer, leased from a third party, leased from an affiliate or provided by a vendor on a fee-for-service basis. Further, various combinations of these possessory interests can exist. However, regardless of the ownership of the systems, the records and data of the insurer held by an affiliate are and remain the property of the insurer and are subject to control of the insurer.

In most straightforward ownership situations, the insurer owns the hardware and software, and the insurer’s employees maintain the systems. Possibly the most difficult situations to unravel are where: 1) a related party owns the hardware and leased it to the insurer; 2) another party developed the software and leased it to the insurer; and 3) the staff who operated the systems are on another entity’s payroll.

The insurer may own, lease or have borrowed its software from a third party. The ownership of the software should be determined, as ownership affects the receiver’s rights to use the software. A contractor may be able to provide services using certain software, but the receiver may not directly use the same software. That is, software licenses may not be assignable to the receiver. Where this is the case, the receiver may have to purchase its own license or use an information systems contractor.

The receiver should identify the service providers, the services performed, hardware and software provided, and all of the applicable costs. The receiver should also arrange for temporary continuation of the information systems services that are critical to the continued operation of the insurer (in a conservation or rehabilitation) or to protect the estate. Whatever the system ownership situation, it should be a practice to immediately back up all available data on all systems, including all active PCs.

G. Conversion

It may be desirable or necessary to relocate the insurer’s systems operations or physical servers to a new facility; therefore, the ability to relocate the existing servers or systems should be ascertained. If determined necessary bur are unable to relocate, recreation, cloning or converting data to a new system into the receiver’s environment may be a possibility. The receiver should determine the cost of and ability to create a clone prior to implementing a plan to relocate an office. Sufficient planning and testing by the receiver should be undertaken prior to any decision to move, migrate, clone and/or convert company data.

H. Common Systems Applications

The insurer or estate can put information systems to many uses. The most common are listed below. In each instance, the receiver should ascertain the adequacy of the system and the need to update or enhance it for the tasks that will be unique to the receivership.

1. General Ledger and Accounting Books

The accounting and reporting functions of the insurer or receivership are frequently handled through the information systems. The books of the insurer may not be books at all but rather entries recorded in the information systems. Chapter 3—Accounting and Financial Analysis specifically notes the types of records that may be kept electronically. The subledgers, cash receipts and disbursements records, registers, journals, claims, reinsurance, and Tax records may all be computerized. The related software system may be designed so that all of these records are integrated. Common source documentation for related records may be stored once and linked to each of the related records, cutting down on unnecessary duplication. That is, data is only entered once, and each subsystem can access that data without manual intervention. The receiver should be aware of how the system is integrated and where manual intervention can occur, and be cognizant of linked data if attempting to bifurcate or move only a subset of the existing data.

2. Claims

The claims records will likely be kept in an information system to accommodate reporting, statistics and control of the claims process. (See Chapter 5—Claims.) In a conservation or rehabilitation, control in this area is critical and systems support is vital.

In a liquidation, the claims information system is usually a key component to the notice process and may be critical to the adjudication of claims. Where the insurer has an automated claims system, data will most likely need to be extracted and imported into the receiver’s claims administration system to facilitate the proof of claims process, communication with the guaranty associations and reinsurance recoveries. Where the receiver elects to use the company’s existing system to process estate claims, it will need to be modified to accommodate several new data elements, including, but not limited to, proof of claim numbers, priority classifications, types of claims (third party, guaranty fund, etc.) and Uniform Data Standard (UDS) conversion when transmitting claims data to property and casualty guaranty associations. (See Chapter 2, Section IV. M. -- Liquidation Considerations.)

3. Accounts Current

Some insurers will have systematic tracking of their agents’ accounts. In a conservation or rehabilitation, prompt and efficient accounting to agents can improve cash flow. The receiver may need to evaluate blocks of business for retention or disposal. The information from the accounts current can be used to help make this determination.

Detailed electronic records of agents’ balances for premium, commissions, collections, endorsements, cancellations and remittances can be extremely useful in a liquidation to determine the fixed rights and liabilities of the managing and producing agents. Collecting monies due the estate from agents is dependent on the availability of sound data supporting the amounts due.

4. Premium Financing

The receiver should examine this area for the same reasons as Accounts Current. The receiver should look for affiliate companies that use or share the insurer’s information systems for premium financing For reconciliation and UDS purposes.

5. Marketing

Marketing functions may be important in a conservation or rehabilitation, but in liquidation, there generally is no ongoing marketing function. This is not to say that the marketing database and records should be discarded. These records can be useful in determining what caused the insurer’s financial distress. Further, the files and reports related to the marketing function usually are closely related to the agents’ files and reports and the account current systems.

6. Investments

Information regarding the insurers’ investments most likely will be found on a PC or internal drive in the accounting or executive offices. The receiver’s staff should check to determine if backups or subsidiary systems exist and whether subscriptions to specific services need to be continued.

7. Reinsurance

Usually, reinsurance receivables will be the largest asset of the receivership, and collection is highly dependent on reliable premium and loss information. Use of information systems in recording and tracking this information is fairly common. Depending on the level of integration of the systems, this may be part of, or at least closely connected with, the claims system or accounting system of the insurer.

Increasingly, a third-party hosted web application or system is utilized to track reinsurance receivables. Continued use of the application or system by maintaining or modifying existing contractual relationships with third-party vendors may be utilized. Alternatively, an attempt to clone or recreate the system within the receiver’s environment may be viable options.

8. Email

Virtually every insurer uses an industry standard email system. Emails are important company records that must be preserved. In addition to performing a backup of the email server at the start of the receivership, it is also good practice to extract individual email boxes of key employees at that time as well. Consideration should be given to periodically backing-up these files throughout the receivership to insure preservation of communications. Email backup restoration often requires the use of outsource computer forensic experts. Extracting email boxes in readable format at the outset of a receivership will save costs down the road should email records be required for litigation purposes.

If the insurer is part of an affiliate insurance group or pool which includes employee e-mail correspondence pertaining to other insurance companies that are not entering into receivership, the receiver may need to execute a confidentiality agreement with the surviving entity(s) in order to obtain the troubled insurance company’s electronic correspondence.

9. Large Deductibles

9. Large deductible recoverables can be a large asset of the receivership, and, like reinsurance, collection is highly dependent on reliable policy and loss information. Use of information systems in recording and tracking this information is fairly common. As with reinsurance, this system may be a part of, or at least closely connected with, the accounting or claims systems , or information may be tracked in a separate application or system.10. Other

There may be other information systems, including PC-based calendar and tickler systems, time tracking and personnel systems, salvage and subrogation systems, imaging systems and litigation support systems on either PCs or larger computers. Further, through Web sites and online services, computers now serve as important common communication devices. The company’s Web site can be used to provide and gather useful information about the company in receivership.

The receiver may need to acquire utility programs to perform such functions as restoring deleted data or backing up data in a compressed format. The administration of some receiverships can be litigation-intensive. Case management or other information systems in support of legal activities should be considered for those receiverships.

Another use of information systems that is important to note is project management. Application programs for project management are widely available and understandable to the average user. This software can be put to excellent use in identifying what needs to be done to administer the receivership in the most cost-effective manner.

Finally, the use of electronic data for all documents is becoming more common. Documents may have been scanned and the originals destroyed or kept in a manner that makes them difficult to use. In the event of liquidation, the receiver may be compelled to export these electronic documents to the receiver’s systems or external hard drive for safekeeping, as they serve as the only official company records.

11.End User Computer (EUC) Applications

End user computing (EUCs) “applications” (spreadsheets, databases, etc.) are often used as part of reserving, reinsurance, investments, modeling, forecasting, and other areas. Critical “applications” may get overlooked because they often do not fall under the IT department’s management and/or control structure. Rather they are managed and updated by the business unit. Companies with good internal controls will have a centralized repository of EUC or User Developed Applications, but often troubled companies do not have this information. If an “application” is critical in producing the information needed by the receiver or guaranty association, the receiver should identify the “application,” ensure that change management is in place and guard against loss of institutional knowledge loss if the business unit employees are terminated (i.e., that the receiver has staff able to run the program.) The receiver will need to inquire with personnel in the Company’s various business units to identify these “applications” and should create a list of the various applications. If these applications are password protected, the receiver should also obtain the password. Before using these “applications” to make receivership decisions, the receiver should review the application to determine its accuracy, for example, checking formulas in an Excel spreadsheet.

IV. INFORMATION SYSTEMS DELIVERABLES

The purpose of this section is to assist the receiver in determining what deliverables and services will be needed from the information systems. There will be generic requirements that are applicable to all receiverships. However, to a larger extent, the receiver’s information systems requirements will reflect the characteristics of the subject insurer. The receiver will need to look at the full scope of historical operations, as well as the new requirements that are specific to the receivership proceeding, to determine the data processing tools that are essential to carry out the receiver’s obligations, keeping in mind what the receiver has inherited from the insurer in terms of disposal and acquisition costs.

It may be necessary to perform a detailed study of a receiver’s data processing requirements and compare this to the level of systems functionality and security provided by existing systems. If this level of functionality or security is deemed to be unacceptable, the receiver will need to modify the existing systems or replace them.

This section provides a checklist of the functions associated with insurance, reinsurance and receivership that should be considered when evaluating system requirements, including software, hardware and security considerations. Software considerations will include any accounting, claims, imaging or policy applications, the management of email and/or instant messaging platforms, along with any other tools that provide data capture, processing and reporting capabilities. Hardware requirements will include computing power of application servers and data storage devices, including both on premises and cloud hosted, as well as peripheral equipment and related items, such as network capabilities. Security considerations will include data protection, endpoint protection, user access controls, network security and physical security.

By definition, any list of standard requirements may fail to address requirements unique to an individual estate. This checklist will serve as the basic outline of a systems requirements study that should be supplemented by the receiver and information systems staff.

A. Considerations Regarding the Insurer’s Historical Business Practices

It is important for the receiver to quickly develop an understanding of the business practices of the subject insurer. This understanding will affect decisions regarding the receiver’s ongoing information systems requirements and will provide the parameters for future information systems needs of the receivership.

B. Volume and Geography of Business

A preliminary task is to determine how many policies were written per year and for how many years, and in most cases, the geographic breakdown of the policies. The number of transactions (accounting, claims, reinsurance, etc.) associated with each policy should be considered along with the corresponding costs. This information is commonly requested by the receiver’s staff immediately after the commencement of a receivership. The following items should be considered in determining the volume of the insurer’s business:

* policies;
* claims;
* claim transactions;
* claimants;
* premium volume;
* reinsurance agreements;
* reinsurance participants;
* brokers/intermediaries/agents;
* Face value of the policies (Life);
* Cash surrender value (Life);
* Policy limits (P&C); and
* Geographic distribution:
  + by state, whether one or many;
  + territory, county or zip code breakdowns within a state;
  + by guaranty fund; and
  + worldwide (with foreign exchange requirements).

C. Types of Business Written

Initially, it will be necessary to identify general characteristics of the insurer’s business practices and the insurance/reinsurance. If the insurer wrote only direct or primary insurance, the ability to process assumed reinsurance may not be of immediate concern to the receiver. However, if the insurer ceded reinsurance, the ability to track and control ceded placements may need to be considered in the systems requirements. Also, if brokers or intermediaries processed reinsurance (assumed, ceded and/or retroceded), the receiver may need to determine if these arrangements are to be continued, or if this function needs to be brought under the direct control of the receivership. If it is not brought under direct control of the receiver, the receiver should carefully monitor this function and work closely with the intermediary.

This analysis of insurer’s business practices and the insurance/reinsurance written will provide a general idea of systems sizing and related requirements and should include an analysis of:

* Lines of business – The lines of business underwritten and the characteristics of this business may have a substantial impact on information systems requirements. If it is a business in which claims will develop quickly, the requirement may be quite different from long-tail business in which claims will take a long time to develop. If the business includes large-deductible or loss-sensitive features such a retrospectively rated premiums, there will be additional system demands. This also will impact the amount of historical information that must be maintained in the systems.

– D. Corporate Structure

The type of corporate structure of the insurer (single stand-alone company or one of several affiliates) and how many offices it has are factors to be considered when evaluating the information systems.

E. Sources of Production

The manner in which a company acquired its business (e.g., was it a direct writer, did it use MGAs, brokers or both) will have an impact on the location and source of critical data.

F. Claims Handling

The way a company handled claims will affect information systems requirements as well. Claims can be handled exclusively in or in a combination of the following:

* In-house;
* external adjusters;
* TPAs;
* Agent/MGA; and
* other subsidiaries, related operations.

G. Affiliated Companies

Different companies with a common parent often use a single, centralized system, which can result in data security and privacy concerns. Certain data of the insurer and the affiliate may be comingled within the same systems. The receiver or the affiliate, should segregate the data of the company in receivership from the affiliates’ data.

On Aug. 17, 2021, the NAIC adopted revisions to the *Insurance Holding Company System Model Act* (#440) and *Insurance Holding Company System Model Regulation with Reporting Forms and Instructions* (#450) addressing data and records of the insurer that are held by an affiliate[[1]](#footnote-2). Specifically, the Model Act #440 revisions clarify the following:

* All records and data of the insurer held by an affiliate are and remain the property of the insurer, are subject to control of the insurer, are identifiable, and are segregated or readily capable of segregation, at no additional cost to the insurer, from all other persons’ records and data. The affiliate may charge a fair and reasonable cost associated with transferring the records and data to the insurer; however, the insurer should not pay a cost to segregate commingled records and data. Therefore, if records and data belonging to the insurer is held by an affiliate (e.g., on the affiliate’s systems), upon request, the affiliate shall provide that the receiver can:
  + obtain a complete set of all records of any type that pertain to the insurer’s business
  + obtain access to the operating systems on which the data is maintained
  + obtain the software that runs those systems either through assumption of licensing agreements or otherwise
  + restrict the use of the data by the affiliate if it is not operating the insurer’s business
* The affiliate shall provide a waiver of any landlord lien or other encumbrance to give the insurer access to all records and data in the event of the affiliate’s default under a lease or other agreement.
* The Model #440 and #450 revisions also describes that records and data that are otherwise the property of the insurer, in whatever form maintained, include, but are not limited to, claims and claim files, policyholder lists, application files, litigation files, premium records, rate books, underwriting manuals, personnel records, financial records or similar records within the possession, custody or control of the affiliate.
* Model Regulation #450, Section 19 revisions update and expand on provisions that should be included in agreements for cost sharing services and management services between the insurer and an affiliate.
* Revisions specific to records and data clarify, similarly to that of the revisions to Model Act #440, that records are data of the insurer are the property of the insurer, are subject to the control of the insurer, are identifiable, and are segregated from all other person’s records and data or are readily capable of segregation at no additional cost to the insurer.
* If the insurer is placed into receivership, a complete set of records and data of the insurer will immediately be made available to the receiver or the commissioner, shall be made available in a usable format and shall be turned over to the receiver or commissioner immediately upon the receiver or the commissioner’s request, and the cost to transfer data to the receiver or the commissioner shall be fair and reasonable.

H. Foreign Exchange Considerations

If a significant amount of the subject insurer’s business is international, it may be necessary to include foreign currency exchange considerations in a systems requirements study.

I. Existing Systems

The receiver’s staff (or an independent consultant) needs to determine if the existing systems adequately process the business or if those systems must be supplemented with additional processing. If it is the latter, the receiver should then determine whether the level of supplemental processing required is acceptable, in terms of accuracy and the cost of processing. This will establish whether the existing system(s) are adequate to provide the receiver with the amount and types of information required.

The receiver may require various types of information in the administration of an estate. Especially with systems that do not permit online inquiry, it is imperative that reports which are adequate for the receiver’s purposes be produced. At a minimum, the existing systems should have the capability of generating a wide variety of reports. The receiver’s staff should carefully examine the available reports to determine whether they are adequate or if custom reports need to be developed, assuming the data stored in the systems can support custom reports. Reports are normally required for the following types of information:

* policies and contracts;
* accounting;
* claims;
* accounts receivable/payable;
* cash;
* reinsurance;
* guaranty fund claims counts and reserves by state; and
* Earned and unearned premium.
* Large Deductible Collections and Collateral

The following types of documentation should exist for all of the company’s systems:

1. Systems Documentation

Systems documentation shows how the system operates from a technical perspective. Documentation should include file structures, record layouts, data model and related data dictionary and systems administration information pertinent to running the system and producing reports.

2. Process Documentation

Process documentation consists of narratives and diagrams of the processes involved in the major functions of the systems—imaging, policy administration, claims administration, reinsurance reporting, accounting and billing, etc. Documentation should include the interaction of various systems and feeds to and from outside entities.

3. User Documentation

User documentation shows users how to operate the system to perform their jobs. Documentation should include sections that are specific to particular functions, e.g., claims, accounting, etc. Note that in many off-the-shelf systems, the only user documentation that exists is the online help.

J. Data Validation

The systems should perform basic data verification functions, such as ensuring that the date of loss falls within the coverage period. The system should also provide some form of validation to ensure that data entered conforms to predetermined values and formats (e.g., all dates or dollar values are numeric, etc.). This helps ensure the accuracy of the data and allows the receiver to predetermine acceptable data standards.

K. System Requirements

The performance characteristics of the information systems as they relate to the processing requirements of the receivership need to be analyzed. If the system does not have sufficient resources to process the volume of data required, it may be necessary to enhance or replace the related computer hardware with higher capacity hardware. Conversely, if the computer system exceeds requirements, the receiver may wish to consider the cost benefit of system sharing or, provided company data is appropriately segregated, downsizing.

1. Application Servers

Company systems run on application servers, which must be analyzed to ensure sufficient computing performance. Further, because servers are prime targets for malware, technical staff should analyze company servers to make certain patching is current, malware protection is implemented, the local firewall only permits the minimum necessary services and that all servers are being backed up out-of-band[[2]](#footnote-3). On premises servers should be physically secured with least privilege[[3]](#footnote-4) access applied.

2. Networks

Company switches, routers and firewalls will need to be analyzed to ensure sufficient performance when systems and users access web-related services, such as a cloud-based hosted email service. Network tools are an essential layer of defense for the security of company systems. Technical staff should review network protocols to verify that entries onto the company network is properly authenticated (two-factor authentication strongly preferred) and that data is being backed up out-of-band.

3. Data Storage Requirements and Sizing

Modern storage devices can be managed on premises or in public/private cloud-hosted environments. Technical staff needs to consider the volume of historical, current and anticipated future records that will need to be stored on the computer system. Note that imaged records like PDFs and JPEGs are significantly larger than other document types, which can increase storage requirements as a company reduces its reliance on paper processes. Technical staff must ensure company data repositories are secure, encrypted, and that access is administered on a least privilege basis. Backups of company data should follow similar protocols and should be tested by technical staff to ensure viability in the event of a data loss.L. Additional Considerations

Other systems considerations to address in assessing systems requirements include:

1. PCs, Laptops and Terminals

To operate the system, an adequate number of PCs, laptops or terminals need to be available. The determination of that number will be affected by the type of system as well as the number and functions of staff members required to process the volume of business. Technical staff should determine whether endpoints are encrypted, properly patched, limited by the company firewall and malware protection is applied.

2. Environmental Considerations (Climate Control)

Computers, whether mainframe, mini, or PC-based servers, generally require a stable temperature and humidity-controlled environment in which to operate. Failure to provide adequate air conditioning and/or heating can cause catastrophic systems failure. Incorrect humidity can cause excessive static, which is especially dangerous due to static discharge. It is therefore necessary to balance the computers’ thermal output with a temperature control system capable of maintaining the operating temperatures and humidity specified by the computer manufacturer(s). A water alarm is also a good investment, especially if raised floors are used. Physical access to the computer room should also be restricted and carefully monitored.

3. Environmental Considerations (Power Consumption)

Data processing and networking equipment is sensitive to the quality of the electrical power supplied to it. Surges, spikes and brownouts of any kind can damage equipment, cause systems to crash or, in some cases, corrupt data. Most data centers and their attendant equipment are equipped with power conditioning of some type. (PCs usually have surge suppressors for this reason.) Power conditioning can take various forms, but data centers usually have as a minimum an Uninterruptible Power Source (UPS) that filters the power before distributing it to the equipment. A UPS may also have a backup battery that will power the equipment for a short interval while waiting for power to stabilize or allow a graceful shutdown. Emergency lighting should be provided with enough battery time to allow a safe shutdown and evacuation of the area, if necessary. Emergency shutdown procedures should be available to personnel. Finally, a UPS may be coupled with an auxiliary generator which will supply electricity during a power outage.

In addition to special power and heating, ventilation and air conditioning, many dedicated data centers have fire suppression systems. These systems may be stand alone or tied into a building fire detection panel. The receiver should become familiar with how the fire suppression system operates and how it should be tested. Failure to keep these systems in good working order and to follow procedures could be deadly. It is important that testing and training be carried out regularly and that procedures be posted and read by data center personnel. Additionally, the fire suppression system must, at a minimum, comply with local fire and safety codes.

M. Liquidation Considerations

In liquidation, there are several special considerations as a result of the fixing of rights and liabilities and the involvement of guaranty associations. In nearly all liquidations, guaranty associations are the initial direct handlers and payers of most policyholder claims or other policyholder contractual obligations. In certain instances, guaranty associations are required to provide some level of continuing policyholder coverage. The receiver should consider the ability of the information systems to supply information required by guaranty associations. Most of the data should already be in the company records, but the information systems will need to accommodate the unique needs of the insolvent insurer and the guaranty associations.

* 1. Property and Casualty Guaranty Funds

For property and casualty insolvencies, this information must be in compliance with the Uniform Data Standards (UDS) in order to allow the guaranty associations to meet their statutory obligations. Therefore, UDS expertise is needed to determine whether the systems meet all of the applicable UDS record requirements. The receiver may elect to have an analysis of the system data elements performed by a representative of one or more of the guaranty associations or outside consultants.

ACompliance with UDS

The UDS is a precisely defined series of data file formats and codes used by receivers and property/casualty guaranty associations to exchange loss and unearned/return premium data electronically. These formats were developed by a group of personnel representing both receivers and guaranty associations and submitted to the NAIC. The NAIC originally endorsed the use of UDS effective March 31, 1995. The formats were revised and updated during 2003/2004 with an implementation date of January 1, 2005. Since this time, several additional updates have occurred. UDS and the UDS Manuals are managed by the UDS Technical Support Group (UDS-TSG).

The National Conference of Insurance Guaranty Funds (NCIGF) developed a secure process for transferring UDS data from the property and casualty insurance guaranty associations to insurance receivers. The concept proposed by the California Liquidation Office in 2005 and the process advanced by the NCIGF in 2007 is known as Secure Uniform Data Standards (SUDS) utilizes Secure File Transfer Protocol (SFTP). SUDS provides cost savings by creating greater uniformity and efficiency in how UDS data is transferred from guaranty associations to insurance receivers. SUDS also provides privacy protection through the use of a secure server. In 2012, the NCIGF developed a web-based application that allows receivers to quickly and easily create UDS records for distribution to the guaranty associations through SUDS. The application is known as the UDS Data Mapper[[4]](#footnote-5). The NCIGF, through its subsidiary, Guaranty Support, Inc. (GSI), maintains both SUDS and the Data Mapper and makes them available to insurance receivers or the guaranty associations at no charge.

The NCIGF maintains and provides updated copies of the UDS Manuals. For further details about UDS as it applies to claim records or the implementation of UDS, please refer to the UDS Operations Manual[[5]](#footnote-6). Information and formats relating to UDS financial reports from the guaranty associations are contained in the UDS Financial Manual[[6]](#footnote-7). The site also includes a helpdesk request form, which emails questions to members of the UDS-TSG[[7]](#footnote-8).

BInsolvency Data Transfers

Guaranty associations become statutorily obligated to pay covered claims when the court enters an order of liquidation with a finding of insolvency. The goal of every insolvency is to transmit relevant company claims and policy data to the guaranty associations on the date of liquidation. The guaranty associations and their coordinating body, the NCIGF, have established experts and tools to assist receivers with the transmission of insolvent company data.

(i)Evaluation

Company data will be spread across multiple information systems (claims, policy, accounting, imaging, etc.) oftentimes managed by third party administrators. Each information system is a unique source of data requiring independent attention to extract, process and convert to UDS. On average, each source takes roughly two weeks to process. Getting access to company data managed by third parties can be complicated when it is commingled with noncompany data. Working with information system administrators to segregate company data pre-insolvency can save precious time when an insolvency is imminent. In the event policy and claims data cannot be transmitted to the guaranty associations on the day of liquidation, providing remote access to those systems can help them address hardship claims and other urgent matters.

(ii)Extraction

Beyond the generation of reports, most information systems are not designed to export significant portions of data. This is especially true of imaging applications, which are used in “paperless” offices. Extracting the relevant data from these systems requires specific technical training and oftentimes server access. Data extraction by competent IT professionals can take days or even weeks to complete though various factors can increase the extraction time. If the system is administered by a third party, several factors can add additional delay, such as the administrator not having been paid, company data being commingled with third party data, or the administrator has insufficient staff to extract company data in a timely manner. Obtaining regular backups of all company data from the administrator can help ameliorate some of these concerns. Technical staff should examine the backup data to determine if it is sufficient to create usable UDS records upon liquidation. Further, if company data is segregated pre-insolvency, technical staff or third-party vendors can extract the relevant data without inadvertently accessing or disclosing non-company data.

(iii)Processing

Once extracts of company claims and policy data are obtained, technical staff will need to process the files before they can be loaded into the UDS Data Mapper. Data must be formatted into comma-separated values (CSV). Date and currency values must be normalized to a single format per file. The CSV files must use latin1 encoding and have characters outside the scope of this encoding removed or replaced. The receiver will then create a map that coordinates fields from the source data with their corresponding field in the UDS standard. The UDS Data Mapper will report errors encountered while ingesting data to guide other necessary cleaning steps.

(iv)UDS Production

After the data is ingested by the UDS Data Mapper it may then be reviewed and edited within the application, then sent to the relevant guaranty associations. This process creates the UDS files and notifies the guaranty associations that they may pick up their files, which are provided via SUDS. For the receiver's own purposes, CSV files of the produced UDS records are also provided via SUDS.

CPriority of UDS Records

All UDS records serve a valuable purpose and are important. However, the timing of some of the UDS records is more critical than others because guaranty associations need them to perform their statutory responsibilities of covered claims. Below is a general guide regarding the level of criticality of the various UDS records.

Highest Priority

A Record (Claim File) - confirms the existence of policy with insolvent insurer; necessary to confirm coverage.

F Record (File Notes) - adjuster’s claims notes; needed to quickly grasp essential nature of claim and current issues.

G Record (Transactions) - necessary to understand what has already been paid to timely continue any future payments owed and avoid duplication.

I Record (Images) - contains the contents of the insurer’s claim file including report of incident, claim history, investigation notes, treatment history, photos, medical records, and other essential information.

Very High Priority

C Records (Guaranty Fund Loss Claims) - guaranty association monthly reporting; typically commences within 30 days of the association’s receipt of critical claim information.

High Priority

B Records (Unearned Premium) - the importance of unearned premium reimbursement may vary depending upon the nature of the insolvency; in a liquidation with substandard auto insurer, timely refund of unearned premiums is often critical because many insureds cannot afford to purchase replacement coverage. In such instances, the production of the B Record should be assigned a higher priority.

Medium Priority

D Records (Guaranty Fund Expenses) - important for the reimbursement of the guaranty association’s administrative expense claims but secondary to the records that are essential to the timely payment of covered claims.

Low Priority

E Records (Closed Claims) - important to enable guaranty associations to re-open claims; can be managed on a case-by-case basis until higher priority records are delivered.

M Records (Medicare Secondary Payer Reporting) - allows parties to verify that pre-liquidation MSP reporting was made by company; assists guaranty associations in identifying open or re-opened files where guaranty associations will become responsible for future MSP reporting.

* 1. Life and Health Insurance Guaranty Associations

The life and health insurance guaranty associations do not utilize the UDS reporting system because the data needs of the life and health GAs are much different than those of the property and casualty funds, both in terms of timing and the types of data needed. This is due both to the types of contracts covered and the particular nature of the statutory obligations of the life and health GAs. Because the life and health GAs continue coverage, they need the data and the lead time necessary for putting in place the agreements and infrastructure required to either *transfer* or *continue administration* of the insolvent company’s business. In either event, NOLHGA and its member GAs need data files at the earliest possible opportunity, and well in advance of liquidation, in order to evaluate options and develop a plan for meeting GA statutory obligations while minimizing disruption to policyholders. Policyholders are best served if the GAs can be ready to implement a plan for assumption transfer or for seamless administration of the business immediately upon entry of a liquidation order.

If preliminary data suggests that an assumption transfer may be feasible, a NOLHGA task force will develop a Request for Proposals (“RFP”), which will be sent to prospective carriers, subject to their execution of a Confidentiality Agreement. The RFP will include a description of the business to be assumed, along with summary policy, claims, and financial information. Policy-level detail is not typically required at this stage.

If assumption transfer is not feasible, the GAs must prepare for runoff administration. This typically requires contracting with a TPA and, in the case of health business, retention of the company’s health care provider networks, pharmacy benefits providers, and all related service providers. Policy-level data is essential for policy and claims administration for all lines (life, health, annuity, disability, LTC).

Getting this information can be particularly challenging if the insolvent company has been using one or more outside TPAs. Data may reside on different platforms and systems and can take longer to gather. Other challenges arise when a company has been using one or more legacy systems with outdated software or hardware, making data extraction and transfer more difficult. In those cases, some consideration may need to be given to keeping the legacy systems in place. if short term data conversion is impractical. It may be necessary to contract for access to the existing administration platform, at least on an interim basis, which in many cases will involve the receiver as successor to the insolvent company’s operations, but may also include affiliates of the insolvent company or the company’s outside TPAs.

A. Specific Data Needs

Specific data needs will depend on the facts and circumstances of each case, as well as the types of business involved. Initial, critical data needs typically include all relevant summary policy and reserve information. Typically, if the policy master /eligibility records can be provided, that file may contain sufficient information for preliminary coverage determinations and to consider the potential feasibility of an assumption transfer.

Other data needed for runoff administration, depending on the lines of business involved, typically includes the following:

* + In-force files/counts (by state and by line of business)
  + Policy values (face amounts, cash surrender values, policy loans, interest crediting rates, rate crediting history, etc.)
  + Policy forms
  + Claim files/claims history (including plan of care and related information for LTC lines)
  + Premium files (and status indicators such as Reduced paid up, or Waiver status for LTC)
  + Rate files/history
  + Reserves, by line
  + Provider/vendor agreements

B. Timing Considerations

Initial data files (Policy Master records) are needed at the earliest possible opportunity, but preferably at least 6 months in advance of liquidation, so that the GAs can evaluate the business and any coverage issues, assess the feasibility of one or more assumption deals, initiate an RFP process for assumption of the business, and negotiate and prepare to implement related agreements.

The lead time needed for policy level data will vary depending on the size and complexity of the business, as well as the lines of business involved. Typically 4-6 months minimum lead time is needed in order to evaluate the business, negotiate TPA agreements, and get claims reporting and funding arrangements made for runoff administration. In the case of health lines, additional time is needed to evaluate, retain or replicate healthcare provider networks and related services. If an RFP process is needed to find a replacement TPA, additional lead time may be required for that as well.

C. Secure Data Transfer

To ensure secure data transfer, receivers or insurance department personnel typically establish a secure website portal or FTP site to provide NOLHGA and its member associations secure access to the data needed. Otherwise, NOLHGA (or a designated TPA or consultant) will establish a secure file portal where designated users can securely upload records.

V. IMPLEMENTATION

This section describes various courses of action to meet the receiver’s needs once it has taken control of the insurer’s information systems. The course of action selected will vary according to many factors, including the size and needs of the insurer and whether the insurer has its own information systems staff.

The receiver will be faced with several options as to how to meet the needs of the receivership. These may include: extraction or bifurcation of comingled system data; retaining the present system; enhancing the present system; replacing the system with either a new system or the receiver’s system; or relying on a third-party vendor. The receiver must be prepared to justify a cost-benefit basis expending limited estate assets in pursuing any option other than retaining the present system. The following should be of assistance to the receiver in the formulation of a plan to select and implement the most effective option.

A. Retention

The current system’s ability to meet the receiver’s needs should be carefully evaluated prior to making a decision to retain it. If the system hardware is to be sold, a plan should be developed and executed to move the necessary data to a system that can be accessed by the receiver. The plan to sell existing system hardware should also include safeguards to ensure that any data on the system is erased before the sale. No sale of system hardware should take place without first determining ownership and consulting with the receiver’s legal counsel. The retention policy and decisions should be consistent with the Liquidation Order.

1. Verify Capabilities

Through examination of available reports and interviews with systems staff, management and operational staff or other sources, the current capabilities of the system should be identified, listed and documented. The system’s capabilities, thus identified, should be compared to the previously identified needs of the receiver. Identified needs will be considered from the Information Systems checklist. This will identify information needs that cannot be met by the existing systems and steps that should be taken to satisfy those needs. If system capabilities exceed the receiver’s needs, consideration should be given to whether the configuration and size of the system should be altered to increase efficiency and control costs.

2. Verify Condition of Hardware and Adequacy/Integrity of Software

The condition of the hardware should be carefully examined to determine both its reliability and its capacity to handle anticipated growth. Suspect components should be repaired or replaced. In like manner, the existing software should be carefully reviewed to confirm adequacy, appropriate licensing and integrity. Software that is inadequate, outdated, corrupted or no longer supported by the vendor should undergo review to determine the best strategy for replacement.

3. Assure Adequate Security and Disaster Recovery

Given the likelihood of litigation and other legal proceedings that will depend upon data gathered and processed by the system, as well as the threat of a cyber attack, immediate steps should be taken to ensure its continued security. Access should be limited to those with an absolute need and in whom the receiver has utmost confidence. Consideration should be given to purchasing cyber insurance for the liquidation estate, if the company does not already have an applicable policy. A review should also be made of the current system as it pertains to the documentation and quality of data, and as to a disaster recovery plan. Many data processing centers do not have a disaster recovery plan other than having the system back up information in an off-site location. A true disaster recovery plan provides for installation of system backup information in an off-site location so that, in the event of a disaster, the system can be running within a specified time frame. That time frame may vary from a few hours to a few days.

4. Devise Assessment Methodology

Methodology should be devised for assessing the adequacy of the staff, the system, the software, security procedures and disaster recovery procedures. Weaknesses identified through this assessment should be remedied. If necessary, a third-party contractor may be brought in to make this assessment.

B. Enhancement

If the receiver has control over the system, and it is determined that the existing system can be retained but should be enhanced in order to meet the receiver’s needs, a plan should be devised for the implementation of those enhancements. After careful consideration, a list should be made of the hardware, software and applications that require enhancement. These may consist merely of the addition of hardware components or may require restructuring of the operating system or supplementation of available software. In like manner, available staff may be inadequate for the anticipated needs.

Once the required enhancements are identified, availability should also be ascertained, and the availability of qualified personnel should be similarly confirmed. Once the needed enhancements have been identified and their availability confirmed, a schedule should be prepared for implementation in a manner that will not interfere with other aspects of the receivership proceeding and which will be consistent with the anticipated needs of the receiver. This may require the operation of shadow systems on a parallel track with the implementation of the enhancements. Testing methodology should be implemented to confirm that the enhancements were successful and sufficient

. C. System Replacement

If the receiver determines that the existing system, even if enhanced, is inadequate and decides to replace it, a plan should be devised for system implementation. The first step is to select the replacement system, considering the future needs of the receiver, including how long the estate may have to remain open, and the available assets of the estate. A plan for migration from the existing system to the replacement system should be implemented. In many circumstances, the replacement or enhancement is handled by a third-party vendor.

To make use of a third-party vendor as a replacement for in-house systems, it is essential to prepare a comprehensive list of the receiver’s anticipated needs. Because the receiver will have relatively little control of the actual operation of the system and therefore little flexibility in adjusting the ability of the system to meet its needs, it is essential that the initial list of needs provided to the third-party vendor be as comprehensive as possible.

Once the needs have been identified, a list of potential vendors should be compiled for evaluation. Each eligible vendorshould be carefully evaluated with full consideration being given to at least the following factors:

* Cyber security expertise and data safety requirements;
* short-term and long-term availability;
* expertise and demonstrated ability;
* price and method of charging;
* support and maintenance resources;
* available warranties;
* capability to respond to emergencies;
* ability to preserve confidentiality and comply with security procedures;
* existence of potential conflicts of interest;

ability to respond to changing needs; and

familiarity with the type of business involved.

1. Contract with Vendor

Once the appropriate vendor has been selected, a contract that will meet the anticipated needs of the receiver should be negotiated in accordance with the receiver’s contracting policy. It should be clear that liability under the contract will be limited to estate assets and will not involve personal liability on the part of the receiver or the state. Once an agreement in principle has been reached with the vendor, protocols should be established for the operational relationship. A plan should be devised for assessing whether a third-party vendor satisfies the requirements of the contract.

2. Document and Back Up Old System

As a result of the decision to use a third-party vendor, the existing system will become unnecessary. Before it is shut down and disposed of, however, it should be fully backed up, including both the software and data, and documented for future reference. 3. Shut Down and Disposal of Old System

Once the old system has been completely backed up and documented, it should be taken out of operation and prepared for disposition. Disposal of any system, data or information related to the liquidation must meet the requirements set I the Liquidation Order and be pre-approved by the court before any action is taken. Before the system is shut down, any data must be erased. Once the existing system is shut down, it should be disposed of at maximum gain to the estate. Proprietary software developed solely by the insurer may also be marketable. D. General Concerns

Be careful not to dispose of the system too soon. If the information is to be migrated either to the receiver’s computer system or to a third-party vendor’s system, steps should be taken to ensure that the integrity of the data from the insurer’s old system is preserved and accessible. Controls should be in place to ensure that the same number of records leaving one system is received by the other system. This should be confirmed by the comparison of record counts and the cross-checking of financial data.

If any enhancements have been planned, then consideration should be given to whether the enhancements should be done by in-house staff or an outside consultant. Once again, it is usually best to get competitive bids as required by the receiver’s purchasing policy.

E. Implementation of UDS

A plan to secure the information required for UDS should be developed as early as possible in the receivership proceedings when there is an indication that liquidation is a possibility. Data availability from company to company varies significantly. In some cases, all data for UDS is located on the system; in other situations, manual coding is necessary to capture the required data. The goal is to make the information available to the guaranty associations as soon after entry of the liquidation order as possible.

The guaranty associations must be notified as soon as possible when liquidation preparations have begun. The notice should include a copy of the company’s Schedule T from its annual statement and the receiver’s plans to supply UDS data.Data transfer preparations should begin immediately after the notice, to be put in place immediately following receipt of the Liquidation Order. This step is important, as it places the guaranty associations in a better position to respond to the inquiries that typically occur soon after the company is placed in liquidation.

It is likely that the initial UDS plan will be modified as the receiver completes its review of the company’s systems. (See Section IV. M. above, which expounds on UDS production and record priority.)

.

1. Although in 2021 the NAIC adopted revisions to the *Insurance Holding Company System Regulatory Act* (#440) and *Insurance Holding Company System Model Regulation with Reporting Forms and Instructions* (#450) related to receivership matters including records and data, these revisions may not yet be adopted in every state; therefore, receivers should refer to the applicable state’s law. [↑](#footnote-ref-2)
2. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online). Sources: NIST SP 800-32 under Out-of-Band. [↑](#footnote-ref-3)
3. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. Source: NIST SP 800-12 Rev. 1 under Least Privilege. [↑](#footnote-ref-4)
4. The UDS Data Mapper is available at https://udsdatamapper.com [↑](#footnote-ref-5)
5. https://www.ncigf.org/resources/uds/uds-claims-manual/ [↑](#footnote-ref-6)
6. https://www.ncigf.org/resources/uds/uds-financial-menu/ [↑](#footnote-ref-7)
7. https://www.ncigf.org/resources/uds/ [↑](#footnote-ref-8)