9 – Business Needs and IT Alignment

**1 – Importance of Information Technology to an Insurer**

**Objective**: Explain why information technology is important in insurer operations

As the insurance industry’s collection and use of data continue to evolve, so does the power structure that manages those tasks. Chief information officers (CIOs), who manage an insurer’s information technology (IT), and chief data officers (CDOs), who oversee the organization’s data collection, work together to provide a clear path and directive that enables an insurer to better meet the needs of its customers.

Insurers are more likely to meet these challenges if business and IT professionals collaborate to leverage IT capabilities in an effort to meet these goals:

**Gain a Competitive Advantage**

Information is essential to effective underwriting, and IT capabilities improve the speed with which information can be stored, processed, and retrieved. This enables insurers to collect and validate data using outside sources-such as motor vehicle registration and licensing records or an individual’s claims history-to create a data resource that can become a basis for enhanced business decisions.

In the modern insurance environment, insurer differentiation – and therefore competitive advantage – may hinge on intelligence, customer relationships, and speed. Business and IT professionals should collaboratively use predictive analytics to develop intelligence using database information (a collection of information stored in discrete units for ease of retrieval manipulation, combinations, or other computer processing), such as customer behaviors and preferences, the markets the insurer serves or might consider entering, and the risks and opportunities it might encounter. Example, analytics that incorporate medical information, claims history, and fraud incidence might suggest that an insurer should withdraw from writing auto liability insurance in a particular region).

Data from the Internet of Things (loT), such as telematics that create a picture of an insured’s driving habits or information collected from a home heating system that monitors temperature or water pressure can help an insurer provide an insured with the most protection necessary at the lowest price possible. IT intelligence gives insurers better insight for underwriting, product development, and pricing.

IT supports tools such as smartphone applications that offer policy self-service, auto maintenance reminders, and route planning. The intelligence could suggest solutions that improve collaboration and communications with insurer’s stakeholders, such as a web portal for producers that aggregates customer information to suggest endorsements, new policy feature, and other products, all customized for each insured. It could also assist the insurer with governance by embedding building code requirements into a database to help claims representatives accurately estimate reconstruction costs.

Blending of business and IT can combine business intelligence (BI) with web-enabled capabilities, social media, and innovation to craft marketing programs, explore distribution channels, and develop new products and services that entice and boost retention and loyalty by engaging producers and policyholders.

Personnel from both the business and the IT sides of an insurer must work together to manage the quality of its data. Successful insurers identify data that has the greatest impact on their business strategy and focus on defining and validating that data. The data might reveal trends or an emerging niche market.

**Underwriters increasingly use analytical engines with predictive modeling to experiment with pricing changes and predict their effect on key performance indicators. It also enables underwriters to integrate cost and demand to find the optimum premium that is likely to gain regulatory approval, be low enough to attract customers, and be high enough to meet or exceed the organization’s profit and growth objectives**. An underwriter might find parents for young drivers are likely to shop for low-cost auto insurance. To encourage retention and reduce the risk of claim, an underwriter might use predictive model to determine a premium discount that encourages young drivers to take a safe-driver course every 2 years.

Underwriting, claims, and accounting personnel and their IT partners must examine the needs of insurance consumers who use web-enhanced tools and mobile applications to get instant insurance quotes from multiple insurers and price changes on their current policies, as well as submit new applications, change request, and cancelation requests. The capabilities can be enhanced through IT’s collaboration with outside entities such as motor vehicle departments, credit rating agencies, and insurance subscriber services that share information from their own databases. This partnering reduces customer entries and provides accurate quotes through a channel that speeds delivery of insurance products.

Because all these processes rely on accurate, secure, and often personal data, efficiently capturing data from and about consumers is crucial to innovation. This data is often captured by smart products, which can sense their environment, process data, and communicate with other smart products and smart operations through the LoT, generating data to which advanced analytics can be applied. The security and integrity of this data then become paramount, as does accessibility.

Blockchain technology – which offers a virtual distributed ledger that maintains a dynamically updated list of records (blocks) and confirms the data within them through a consensus process – is possible solution for this need. By allowing cooperating entities to share data quickly, it expands the information available to an organization acting on its own.

**Increase Operational Efficiency**

IT capability can increase the operational efficiency of nearly every functional area of in insurer’s business. **When considering whether to develop or purchase new technology, the costs of efficiency enhancements should be weighed against the savings and benefits that the new IT would produce to determine the return on investment (ROI).**

***Apply your knowledge*: Before considering any new technology purchase, business professionals should collaborate with their IT professionals to determine user needs and current system capabilities. Together, they should explore system options, their costs and benefits, and the feasibility of adopting new technology. Even if the new system were compatible with the company’s existing network, the insurer may still be likely to incur costs to integrate the new system with the existing one. If conversions were required to adapt data for the new system, reduced retrieval speeds would create operating inefficiencies. In either case, the time to complete the integration might outdate the proposed claims system, as technology continually evolves.**

**In addition to the cost of purchasing and installing the equipment, as well as any development costs, insurers should consider theses costs when calculating ROI:**

* **Staff’s time for training and any associated fees or materials costs**
* **Time lost until staff become proficient using the new technology**
* **Maintenance of the technology**
* **Required services associated with the technology**
* **Any costs associated with building or structural modifications and equipment needed to house and protect the new IT equipment**

The savings/benefit calculations should consider any salary and benefits costs eliminated through staff reductions; the savings from eliminated expenses incurred for the use, support , and maintenance of the old technology; the realized value of employee’s reduced time once the learning curve has been eliminated; the value of customer’s satisfaction with the improved technology; and new business volume that results from the IT upgrade.

Insurers that align all their objectives with their vision, mission, and goals might decide to use a transformational approach to evaluating IT system and process upgrades rather than a cost/benefit approach. In a transformational approach. I a transformational approach, insurers focus on the future state of the organization based on its vision and strategic goals. If IT initiatives align with the organization’s goals, then they are worthy of pursuit. Example, if a goal is to improve efficiency by reducing costs and risk, an appropriate improvement may be technology that allows the insurer to monitor its operations on line in real time and identify backlogs and workflow bottlenecks.

Improvements in mobile technology and declining costs have made adoption of portable IT enhancement imperative for operational efficiency. The benefit is evident for field claim representatives, who access and verify policy information and transmit claims information while adjusting property losses at loss sites. IT features enable them to settle losses or make partial payments immediately so that displaced families can return to their homes as soon as possible. The customer service and satisfaction benefits of this technology are exponential compared with the costs of the technology.

Insurers can also increase operational efficiencies using enhanced IT models. Example; Insurers might use cloud technology to eliminate the costs of purchasing and owning expensive computer equipment and to enjoy the processing and owing new equipment. However, they must also consider the potential trade-offs, which include losing control over data and the risk that the cloud vendor might not properly protect the data.

**Support Strategy and Decision Making**

Managerial decision making requires analyzing complex business information from multiple sources that often change. Unfortunately, human decision makers have limitations. The volume of information to be analyzed increases the time people need to make informed decisions, but the pace of change makes timely business decisions essential. Further complicating these decisions is the fact that while a manger with considerable education and experience could potentially make superior decision, personal bias, and values may negatively influence those decisions, rendering them less effective.

IT decision support capabilities can help people overcome these limitations. **Decision-support systems analyze large databases of BI to supply managers with suggested fact-based outcomes for the business problem the manager inputs. Each database is logically organized for efficient procession, and the results can include graphics and other tools that support a decision. The number of outputs is limited to a few that are best supported by the data. The manager must still exercise good judgment to select the best solution, but the software improves the speed and quality of decisions and may help the manger recognize flaws in his or her thinking. Another benefit is that the manager can add to or change details of the problem and then rerun the application to produce better-defined or more specific solutions**. In addition to the speed this decision support produces, they incorporate business rules with knowledge that has developed over time, and they easily transfer the knowledge to new managers, resulting in more consistent, rational decision making, whether by one individual or many.

Because decision-support systems include business rules and vast databases of BI, they have become essential tools for developing business strategy. Predictive analytics tools are often paired with decision-support functionality. When manager input data that they deem strategic to the organization, these systems can project the outcomes of various strategies. Managers can examine the results in conjunction with the organization’s vision, mission and objectives to produce optimum strategies that will help set the insurer apart from its competition.

At various point during the year, managers may reassess their strategies by rerunning the analytical decision-support systems – using new and developing data that have periodically been added to the database – to ensure the strategy remains effective.

**Facilitate Governance, Risk, and Compliance Initiatives**

**An insurer’s governance, risk, and compliance programs create rules, processes, and controls that support the insurer’s operating policies and strategic goals. They create transparency that offer the insurer’s management and stakeholders a macro view of all of the organization’s daily activities and helps them identify potential credit, marketing, or operational risk exposures so that they can react quickly and appropriately.**

Modern IT support and decision-making tools enable insurer to proactively analyze various scenarios and conduct test for corporate exposures to risk. The results of these tests and analysis help insurers anticipate and identify risk and react to it promptly and effectively. IT controls help insurers better understand financial market risks and changes in laws and regulations; threats and vulnerabilities to IT systems; and threats caused by environmental issues, political unrest, and terrorism.

Governance, risk and financial reporting features that are embedded in insurer’s IT-enabled end-to-end process and controls on an enterprise-wide basis are, in effect, integrated into that insurer’s daily processing. The integration can reduce the insurer’s administrative burden and provide ongoing compliance and risk monitoring. The holistic view of enterprise risk allows the insurer to respond promptly to changes in its environment and markets, enabling it to use strategic risk and return to sustain a competitive advantage.

The National Association of Insurance Commissioners (NAIC) monitors insurer’s corporate governance practices through annual and quarterly reports that insurers develop and transmit. The NAIC guides insurers on corporate governance, requiring them to have adequate top-level controls, checks, established structures, and communications.

IT capabilities can assist with auditing by preventing unauthorized entries, such as a reserve that exceeds the authority level of the claim representative who set it. Control features might also select files for auditing based on established criteria and provide the list of files to a manager or an internal auditor. Control functions can also provide systems alerts to IT staff concerning systems problems and errors.

Accurate data reporting is crucial to government oversight, the industry, and stakeholders. State insurance regulators require the use of statutory accounting principles (SAP) for insurer’s financial statement, which help regulators monitor insurer solvency. SAP accounting uses a conservative approach to the valuation of assets and liabilities (the insurer’s obligations) and the recording of income to ensure that the insurer has adequate capital to meet solvency requirements. IT tools and capabilities simplify categorizing data according to SAP requirements and developing standardized SAP reports.

Accurate data is equally important for insurer’s generally accepted accounting principles (GAAP) financial reporting. GAAP reporting provides investors, members, or other stakeholders with financial information in a uniform format, enabling them to analyze and compare an insurer’s profitability and earnings with those of other insurers and types of business organizations. Credit rating agencies, such as Moody’s, analyze insurer’s GAAP financial reports to assign ratings that help investors, creditors, and additional stakeholders make sound financial decisions.

**The company should provide training for its IT staff to learn the basic business and insurance principles. Doing so would help them understand the needs of the underwriting and claims personnel so that IT could design appropriate systems. Training should also be provided for the business managers and key underwriting and claims staff to expand their knowledge of technology and the importance of data quality. This training should help the effectively communicate their business needs to the IT staff and would explain the importance of providing the correct information in data entry in supporting the businesses strategic decisions**.

**2 – The Importance Of Data Quality In Meeting Insurer Information Needs**

**Objective:** Explain how data quality practices enable insurer to meet operational, managerial, strategic level information needs

Almost every crucial insurance decision is based on data. So insurance professionals who have a well-rounded understanding of how quality data is collected, stored, and used are in a better position to help insurers best meet their goals and serve customers.

Collecting and managing quality data are critical insurer functions. Such data is needed to set pricing, control risk, evaluate new markets, manage finances, and support compliance efforts. To support insurer’s goals, data managers must ensure that data quality standards are met and that the data is protected, used, and enhanced in the best ways possible. To facilitate this, the data needs of insurers are split into three levels: Operations, Managerial, and Strategic.

**Usage and Characteristics of Quality Data**

In insurance, data serves many purposes, and in many cases the same data serves multiple purposes. Example a policyholders zip code is stored as part of an insured’s address, and insurers use that same zip code to evaluate loss exposures in a region for pricing or for decisions on whether to expand or withdraw from that region.

**Quality data is data that is appropriate, reasonable, and comprehensive enough to accomplish its given use. Certain traits determine whether data is appropriate, such as its timeliness or historic value, the source from which it was collected or derived, its independence from or dependence on other appropriate data, and the suitability of the data to produce a reliable result or assessment.**

**Reasonable data is data that’s been validated using outside sources or audited for consistency and accuracy.**

**Comprehensive data contains the full range of information needed to produce a reliable result or analysis**.

For example, data for evaluating auto rates by insured’s ages must include age groupings that have been used consistently within the organization and in nationwide claims databases. The data must also include claim data the help determine rate for various coverages, such as claims for which losses were paid; their settlement amounts; the territory; the types of claims paid (PD or BI); and causes of loss. A Quality control audit should be performed on the selected data to ensure accuracy, validity (quality as a permitted value in a dataset), and consistency.

**Quality data is free of any factors or limitations that could adversely affect an outcome**. If any such factor exists and reasonable alternatives are available, alternatives should be used. Example, when selecting data for study auto claims, claims that occurred before the year 2015 would be limited because of the growing frequency in the use of driving aids after that year. Viable alternative data to reflect trends would be claims from the two most recent years.

The Casualty Actuarial Society (CAS) and the Insurance Data Management Association (IDMA) are two examples of business associations that have been formed to develop data-quality standards and practices for gathering, organizing, analyzing, and distributing information to support insurer’s decisions. The IDMA Value Proposition states that poor data quality can be costly, so the best approach is to proactively address quality at the moment data is created – by engineering processes to create quality data.

**Data managers achieve data governance (creating rules and processes to protect and enhance data) by creating data definitions and metadata (information describing the data); developing standards, ensuring compliance with standards; and monitoring and assisting with data analysis, data warehousing, predictive modeling, business intelligence, and risk management. Data managers also advocate for standardized data across the industry**.

**Operational-Level Information Needs**

Insurer’s operational-level data needs are triggered by necessary activities such as setting rates, underwriting, producing policies, collecting premiums, reserving and paying claims, defending insureds and claim decisions, supporting producers, developing sales information, financing, auditing, and controlling losses.

* **Customer Information** – both producers and insurers benefit from learning as much as possible about their customers and prospects. This drives product development, sales and customer service. In addition to personal identifying information, insurers need customers’ current and past insurance information – including exposure information and specifics about risk retention and management efforts – to underwrite and rate exposures.
* **Underwriting information** – Underwriters are charged with selecting profitable exposures and developing rates that produce a profit. So **underwriters need specific, detailed data on the coverage requested and claims history. Selection and rating data must be accurate, complete, and granular enough to support decisions. Underwriters need data on the insurer’s rating formulas, reinsurance criteria; loss costs; and, for workers compensation NCCI classifications codes.** Poor data quality results in improper pricing. **Underwriters also need data from outside organizations, such as credit rating; loss experience data; driver records; authorized medical records; wildfire, flood plain, and National Weather Service data; vehicle valuation data; stolen equipment data; and more. This data is structured data because it can be standardized. Underwriters also need access to**.
* **Claims Information** – Claims representatives require extensive information. When a claim is reported, they must gather data from numerous sources. They get policy information from the insurer’s database and the loss notice to verify that coverage existed at the time of loss identify policy limits, and determine whether aggregate limits or reinsurance applies. Claims representatives should also resolve entry or processing errors to ensure data quality.
  + When conducting an investigation, claims representatives develop the claim information using additional loss details, claimant information, investigation details, claim reserves, loss payments, salvage and reinsurance recoveries, notes, digital images, correspondence, and audio and video files. This data is recorded in the insurer’s database along with data from outside sources such as fire and police departments, motor vehicle departments, medical providers, claims history and fraud databases, property damage estimators, valuation services and salvage buyers, stolen property registries, social media, independent adjusters, lawyers and courts, and others. The insurer’s claim file must provide documentation to support its decisions and avoid or defend against bad faith. Claims managers also need information from the insurer’s defense and corporate legal counsel and from state insurance departments. Ideally, all of an insurers’ data is stored and accessed in a central database.
* **Accounting and Financial Information** – Accounting staff need all billing and collection information stored in the insurer’s database, and they need access to premium and claims information. Accounting and financial staff need digital information from banks and other financial institutions. Finance extracts most federal, state, and local tax reporting information from the insurer’s database(s), but is also needs information and systems for tracking depreciation on business property, processing and filing state statistical and rating information, and completing and filing tax returns and reporting payments to employees and vendors. Additionally, financial staff need data from analytic engines and predictive modeling for investment planning and fulfillment of reporting and legal requirements.

**Managerial-Level Information Needs**

Managers need accurate information to control and monitor the performance of the enterprise. This information should indicate the insurer’s progress toward meeting objectives and suggest changes to improve performance and achieve profitability.

* **Financial Reporting and Premium Determination – For financial reporting, accountants need complete, accurate, and detailed current and historical data for tracking the insurer’s assets and liabilities**. Financial reports are required by stat insurance departments to evaluate insurer’s solvency and are submitted to rating bureaus to assist with investor decision making. **Managers also use financial reports to analyze the insurer’s profitability, determine where problems might be occurring, and prepare budgets based on expected premiums, losses, and expense**s. This data aids the organizations’ planning process and ensures that department goals are aligned with strategic goals. Actuaries need premium and loss information for ratemaking to determine the insurer’s premiums. Financial reports enable underwriter to monitor premium and loss data and discover new loss exposures that might merit a premium change.
* **Product Development and Pricing, Producer Relations, and Reinsurance** – Underwriters and actuaries often monitor sales trends and profit margins to identify market in which the insurer can grow its business. Insurers can use predictive modeling to simulate market conditions and change policy terms and coverages to estimate future loss patterns and develop pricing structures for new products. Quality historical data must from the foundation of these new product prices to ensure profitability. Insurers analyze their policy and financial data to determine the volume and profitability of business provided by each producer. They also analyze premium and loss information to determine the type and level of reinsurance protection the insurer should seek. The data can be analyzed on exposures by geographic concentration, industry, and coverage limits to suggest the appropriate mix of reinsurance protection. They use financial data to monitor their books of business for new patterns in risk assumption and to review their reinsurance programs for continued adequacy.

**Strategic-Level Information Needs**

Insurers examine their vision, mission, and goals and align their strategies to achieve them. An insurer needs data and output from analytics and predictive modeling to determine which products to produce, what processes to adapts, which customers to serve, and the optimum size and composition of the organization.

Executive manager needs extensive, high-quality data resources and analytics to determine the insurer’s strategic path. Executive information systems combine the insurer’s financial data with data from external databases containing news feeds, market research, populations trends, trade activity, and economic activity to create powerful decision-support systems.

Strategic use of quality data enables insurers to improve their customer’s experiences and determine which technologies to use. Conversely, and insurer’s use of faulty data for customer-facing tools could alienate customers and become a liability.

**3 – Types of Business Information Systems**

**Objective**: Explain how insurers use these technology systems to optimize decision making, customer service, and daily transactions: TPS, DSS, ES and Customer-focused collection and safety systems

Insurers rely heavily on technology to compete against other insurers and enhance the customer experience. As a result, the more you know about the tools and systems insurers use, the better equipped you’ll be to aid in insurance transactions and organization decision making.

A Business information system (BIS) consist of the technological tools of insurers use to remain competitive and serves customers. A BIS can include one or more databases, decision-support tools, information management controls and applications needed for an insurer to conduct thorough and accurate business analysis.

A BIS consist of four systems that help insurers make sound business decisions an deliver information and products to customers: Transaction processing systems (TPS), decision support systems (DSS), expert system (ES) and Customer-focused collection and safety system.

**Transaction Processing Systems**

**TPS is the generic name for a collection of software, databases, procedures, and devises that can perform a high volume of routine and repetitive business transactions and analyses. A TPS can include database management systems, multipurpose databases, data mining and big data systems, telematics devices could storage, and blockchain technology.**

**Insurers can use a TPS for efficient collection, modification, and retrieval of transaction data. TPS data is useful for policy and claims processing, managing purchasing and inventory, accounting with ledger systems, managing financial investments, and more**.

* **Database Management Systems** – **A database management system (DBMS) stores and organizes data flowing from a TPS in a database. It also provides a user interface for retrieving information using a TPS. A DBMS manages information from each TPS and stores it in a central repository database or in individual database from the beginning of a policy life cycle and makes that data available for reuse in other systems or by other departments. This prevents duplicate entries, errors, and confusion, which can be created when the same or similar information is entered through multiple systems at different touchpoints**. The DBMS works together with the TPS for efficient data collection, access, and modification. So when one department example - underwriting want access, the policy information will automatically prefills. When the insured reports a claim, customer service can key the policy number into the claims and the policy and premium information is automatically fed into the claims TPS for reuse.
* **Multipurpose Databases** – Multipurpose databases, or data warehouses, can be used for structured and unstructured data. Structured data is made up of standardized fields, whereas **unstructured data can include open text fields and objects such as emails, audio and video files, webpages customer intelligence retrieved through social media, and data transmitted from vehicles and smartphones.** With unstructured data, an insurance manager can develop actionable information by selecting and sorting the data by territory, code, policy limits, loss amount, or policy term. Using unstructured date, however can involve searching the data using tags (labels) or terms such as “fraud” or “arson”. Searching for the tag “SIU” for example, could enable the manager to identify suspicious claims that may be related.
* **Data Mining and Big Data** – Database and data warehouse features enable data mining, the analysis of large quantities of data to find patterns, trends, and correlations. Data mining offers users new perspective on information, leading to better decisions, new products, new customer groups, and recognition of emerging exposures, all of which can create a marketing advantage. Data mining has also been used to identify fraud activity, predict customer buying patterns, and increase operating productivity. Example, data mining can generate a report of a city’s suspicious rear-ed collision claims. Large database systems are also used to store and process big data. This term refers to any data that is too vast and/or complex for traditional data processing or analysis techniques. Big data systems take large quantities of information and apply statistical modeling and artificial intelligence to it to produce forecasts of future events, losses and risks. Big data can influence functions, such as underwriting, ratemaking, claims processing, and marketing.
* **Telematics** – The variety, volume, and velocity (speed with which data is transmitted) of data involved in telematics exemplify big data. A telematics device installed in an out or mobile devise senses behaviors -such as hard braking, fast turns, quick acceleration, and speed – and other information – such as miles driven, location, and the time of day driven (variety and volume) – in real time (high velocity), then transmits this large amount of data wirelessly to an insurer, enabling the insurer to offer usage based rating for insurance. A drawback of big data, like the kind continuously generated through telematics is that managing versions and locations of the various files can be time consuming. One solution is sophisticated enterprise-wide index with a user friendly interface that can tag data and store its location and metadata (information about the data and their attributes), and then locate particular data.
* **Cloud Storage** – Cloud storage is another data model that allows insurers to efficiently store, modify, and retrieve data. In this model, data is stored on remote servers that can be accessed using the internet (“the cloud”). An advantage of cloud storage is that insurers and their employees can remotely access valuable data from just about anywhere the internet is available. Insurers can choose what kind of data can be stored in the cloud, what kind of data can be pulled from the cloud, and who can access and alter the data. A disadvantage of cloud storage is that it can be more difficult to secure sensitive data that is stored in the cloud than data that is stored in an insurer’s traditional database. However, a variety of tools can be sued to protect data from hackers and thieves.
* **Blockchain** – Blockchain technology is a giant leap forward in digital record keeping. It is a decentralized data-storage technology and real-time ledger that contains a history of transactions that cannot be hacked. Blockchain is a shared database that does not require an official record keeper or third party to act as an intermediary. An advantage of blockchain for both insurers and insureds is that it enables the data and financial transactions of authorized participants to be approved and recorded (in digital ”blocks”) immediately. It creates and instant, permanent transaction record that can be viewed, in read-only format, by authorized entities, like an insurer. Due to their security, blockchains can eliminate the need to verify the accuracy of insured’s data. In addition, blockchains can store and execute smart contracts – digital contracts that follow a computer protocol and are executed automatically when conditions of the contract are met.

**Decision Support Systems**

A DSS is an organized collection of hardware, software, databases, and procedures used by a BIS to support strategic decision making. It typically examines and manipulates a vast amount of information collected by a TPS.

A DSS provides an interface that allows users to enter details about a problem and obtain suggested solutions. By entering details on new markets an insurer is considering, insurers can use a DSS to more accurately predict return on investment form strategic changes they might make, as well as the time it will take to realize that ROI. A DSS can also help insurers identify declining markets they may want to abandon.

A DSS can perform analysis based on these factors (and the questions insurer might ask related to them):

* Changes to one or more situational details (what-if factor) – what if we reduce the insured’s deductible by $50 for one year of accident-free driving
* Repeated changes to a single detail (sensitivity factor) – how would the insurer react if his premium increased by 10% each year
* Changes to several details aimed at achieving a target result (goal-seeking) at what premium and deductible will insureds we willing to purchase a vanishing deductible
* Experimentation to find the best combination of details subject to certain constraints (optimization factor) how much can we increase the premium and deductible before a ten year policyholder will research policy prices with other insurers

**Experts Systems**

An EX stores knowledge and makes inferences. It is designed to emulate human decision making using AI. An ES contains case-based or hierarchical facts about a specific subject along with rules that explain to the system how it can use expert reasoning. Using AI, and ES can analyze vase amounts of complex information faster than a human and either recommend solutions or actually make decisions.

**The benefits of using an ES to supplement or support human decision making include speed and consistency, its preservation and use of the knowledge of multiple experts, and the fact that it does not suffer human limitations (distraction, stress, or fatigue). An EX is also objective and not prone to bias. Insurers can use an ES to underwrite complex accounts, handle complex claims, offer potential medical diagnoses, and detect fraud**.

**Customer-Focused Collection and Safety Systems**

Insurer are increasingly using information produced by systems that interact with customers. They enable insurers to collaborate with customers to provide individualized pricing or discounts.

**Telematics is one example. Telematics, used in what is called a pay-as-you-drive or pay-how-you-drive (usage based) insurance, enables insurers to rate drivers based on their driving habits rather than assumptions based on segmentation (such as age, gender, marital status, an auto model). Some regulators prohibit insurers from using personal characteristics as the basis of price because doing so can penalized good, law-abiding drivers. Telematics provides a solution: individualized pricing. Because safe drivers are attracted to telematics’ benefits, insurers can gain a competitive advantage by attracting the most profitable customers**.

Cutting-edge safety and security features are being installed in motor carriers, personal autos, homes, and commercial buildings. These technologies may use the Internet of Things (loT) devices, or smart devices, such as cameras, sensors, global positioning systems, and other devices to transmit data to insurers and/or security vendors and local authorities. Information transmitted and/or collected by these devices can be used by insurers to investigate losses, determine causes of loss, and serve as evidence that can potentially bring justice to those who have committed fraud.

loT and smart devices can help prevent losses. If a property in a floodplain has a sump pump to prevent water damage, a smart moisture sensor in the home could detect if moisture in the home rose above a set level, indicating the sump pump failed. The sensor, which is connected to the internet, could then send a signal to the insurer and/or the homeowner, who could call a repair company to replace the pump before a major loss occurs.

**4 – Security and Control in Information Systems**

**Objective**: Evaluate the security risks in information systems and appropriate responses to those risks

Technology has been a boon to the economy in general, but its increased use and our increased dependency on it also creates new forms of risk. These risks must be identified and addressed to minimize potential damages.

Threats to data security can come from any area: internal sources, external sources, or a combination of both. For insurers, security risks can center on the destruction of data programs, espionage, invasion of privacy, social networks, employee fraud, human error, cloud computing, and mobile devices. All employees should be aware of these concerns, trained in best practices, and held accountable for data safety as directed by the security team.

**Sources of Security and Control Risks**

Weaknesses in data security allow for risk sources that can be internal, external, or collusive (a combination of the first two). Employees who could exploit such weaknesses pose and internal risk for organizations. This risk can be mitigated by segregating duties. This separation restricts the ability of employees to steal and asset then conceal the theft by, for example, altering computer records.

Two major sources of external risk are customers and vendors that process transactions: both have indirect access to an organization’s assets and records. Former employees also constitute a risk to computerized data, as they may have intimate knowledge of data systems and their control weaknesses**. Unknown criminals that pose an external risk include hackers, who may be more motivated by the challenge than the theft; competitors attempting to gain an advantage; or members of organized crime, who may want to exploit weaknesses in data security to defraud an organization of its assets**.

Collusive sources of risk exist when two or more individuals conspire to defraud an organization and to conceal the theft by altering records*. Internal collusion occurs when employees cooperate to bypass an organization’s controls, steal an asset, and conceal the theft*. *External collusion exists when an employee acts with a nonemployee to defraud the organization*.

**Security Risks and Responses**

Specific organizational risks may arise from internal, external, and collusive sources.

**Destruction of Data Programs**

Data and files vital to an organization’s operation may be difficult to reconstruct if destroyed. Intentional data or program destruction could arise from disgruntled employees or former employees gaining unauthorized access to various systems to destroy or modify files as a form of revenge, or from hackers, proving they can bypass the security features of the system to introduce a virus or malware. For general network security, it is important to invest in quality antivirus and spyware software on a regular basis.

Sometimes the destruction of data or programs happens accidentally. **This risk can be minimized by hiring capable, trained, and responsible employees; continually retraining and updating the skills of those employees, providing manuals and resources for safeguarding data; and maintaining high standards of data protection and adhering to them***.* Following prescribed backup policies ensures that data can be retrieved in the event of a fire, flood, or other physical damage to storage hardware.

**6 Best Practices for Backup**

* **Determine what data on which computers will be backed up**
* **Select the appropriate program(s) for backing up the data**
* **Determine an offsite location for backup archives**
* **Set up a regular backup schedule**
* **Periodically monitor the backups for occurrence and accuracy**
* **Periodically pursue data restoration in attest environment**

To ensure data integrity during the backup process, an organization can adopt best practices for employees, including these: Save data often and always at the end of the workday; Report any scheduled backups that are missed; Do not alter or change the scheduled backup times; Store data in designated locations (such as certain drives or certain folders) to maximize backup efforts; If overnight backup is scheduled, leave computers in the correct mode.

If data backup will be on the cloud, organizations should ensure that the above best practices align with those of the cloud provider.

**Espionage**

Executives who are concerned about the actions and plans of competing companies can acquire useful information about competitors, such as financial, production, or employee records, by gaining access to proprietary data. Information could be stolen using a Universal Serial Bus (USB) flash drive or a keystroke logger to monitor a company’s emails, passwords, and newly inputted data.

*USB Flash Drives and Security Failures*

*The US Department of Homeland Security conducted a security check by leaving USB flash drives in the parking lots of federal buildings and private contractors. The majority of those that were found were plugged into company computers, particularly the flash drives that had official logos on them. While this was only a test, it did confirm that hackers can leave tempting USB flash drives in the paths of individuals and wreak potentially devastating results. A flash drive can introduce an executable program to collect information or spread a virus. In addition, it can be programmed to accomplish its activities weeks later, convincing the user in the short term that it is safe and can continue to be used. A damaging flash drive may appear on screen to be blank, luring the user into a false sense of security*.

Companies operating internationally may be victims of espionage from competitors in a foreign country, where certain spying techniques might be legal.

To thwart such efforts, companies should secure wireless connections by encrypting all information between wireless devices and their router. Because the router may be set up with a default setting that is commonly available to anyone on the internet, companies should secure a wireless access key and change router settings often.

**Invasion of Privacy**

Computerized data files can contain a large amount of personal information regarding clients, partners, and employees. Disclosure of this information is an invasion of privacy, with implications of possible criminal or civil liability at the local, state, and federal levels. Employees should be able to assume that their information, such as age, address, wages, and pension records, will be kept private, while customers expect confidentiality concerning current balances, credit ratings, and payment histories.

Threats to privacy can come from hackers or employees, but general network security procedures can protect private data that should remain confidential. Internally training regarding company standards and applicable laws addressing privacy issues can be good reminders for employees to keep personal file information secure.

**Because insurers gather personal information from applicants, insureds, and claimants, they must be aware of the relevant legal and regulatory requirements around invasion of privacy. These include the Health Insurance Portability and Accountability Act (HIPPA) and, for insurer that do business in Europe, the General Data Protection Regulation (GDPR), which standardizes controls for the protection of personally identifiable information across all member nations of the European Union**. ***Insurers can limit their exposure by reducing the amount of acquired and stored personal information.***

**Social Networks**

**While social networking sites can encourage communication and connections, ideally creating and atmosphere of sharing and trust, they can also present another loss exposure for employers. An organization’s internal secrets might be obtained indirectly by analyzing employee’s public posting on social networking sites. Employees detailing company plans or projects can leave their employers vulnerable to information leaks, not matter how unintentional**. **Organizations may find an explicit social media policy helpful in educating their employees of the potential threats, providing detailed standards and guidelines before any damage occurs.**

**Employee Fraud**

*Fraud is the risk that most often affects the accuracy of accounting records by misstating assets and expenses in financial statements*. Major fraud endangers the ability of an organization to continue its operations.

Although many controls protect against fraud by lower-level employees, managers may be in a position to override these controls. Additionally, when employees collude internally or externally, controls may fail to prevent or detect fraud.

**Human Error**

*Human error, including unintentional errors from users, programmers, and service providers, can cause information loss. It, rather than technical failure is generally considered the most frequent cause of security lapses.*

Human error takes multiple forms. If someone casually reveals a password and that same password is used for all of his or her business applications, a company’s security could be jeopardized. Or if an employee is uneducated about phishing expeditions (a fraudulent email scheme by which an unauthorized party acquires a victim’s personal or confidential information), that may put his or her business data at risk. These types of risk can be minimized by hiring technicians with appropriate amount and type of experience and by emphasizing security training and certifications for information technology (IT) employees.

**Cloud Computing**

Cloud computing, or the cloud, allows a company to access and run many programs and applications without buying or maintaining them for each employee and without needed to install the best and fastest computer hardware.

Through the cloud, employees can sign on from any location and store data on remote computers. The cloud also provides data backup with digital storage devices and keeps a copy of all company information to ensure retrieval in case of a breakdown. The risk is allowing others to have this access – there is uncertainty in placing a company’s ideas and secrets in someone else’s control.

Other risks to consider are a cloud provider’s security standards and procedures, which can vary by provider. To date, little conclusive research exists on the costs of losses from cloud computing. Insurance for covering these losses, offered as part of a service agreement, is an option to consider when choosing a provider.

If a company’s files are stored on the cloud, that company becomes dependent on the servicing company or network to provide its data. If the service is disrupted, by damage to fiber-optic cable, the network will be down. Although backup data would be available, a company may merely be inconvenienced, but at worst, it could experience devastating results, depending on when the disruption occurred and for how long.

**Security and Control Measures**

Internal security controls consist of methods, policies, and procedures used by an organization to ensure the safeguarding of assets, the accuracy and reliability of financial records, the promotion of administrative efficiency, and compliance with management and regulatory standards. Examples of external controls include a well-maintained network with firewalls and access control lists.

An organization’s security team should understand senior management’s goals for the company and integrate a security plan that helps meet those goals. In this way, the security team should be supported by senior management and enlist the help of the entire organization. A security team that has familiarized itself with all aspects of an organization’s departments can more easily identify and respond to emerging risks.

An education and training program is especially important for organization such as insurers, which value their stakeholders’ trust by safeguarding personal information. Employees must understand the reasons that safety measures are created, the structure and hierarchy of the security system, and the need for periodic audits to measure and improve compliance. An insurer should impress upon employees that they are partners with senior management ad the security team is accomplishing the goal of attracting new customers, retaining existing insureds, and continuing an insurer’s reputation for privacy and confidentiality.

A technology-usage statement is a policy that identifies levels, responsibilities, and roles for all internal employees and external partners. It should be in writing, identifying any practices deemed essential, such as access to the internet, password requirements, and use of mobile devices. This statement, along with corrective actions for noncompliance, should be explained and signed by employees; then revisited, reinforced and re-signed as needed.

To the extent possible a company should be forward-thinking and aware of emerging technology, new risks, and possible solutions, such as the use of blockchain technology. Blockchain provides a cloud like storage system for information, but, disperses the information across a network of servers. For a limited-access blockchain to be compromised a hacker would have to simultaneously alter the records store on more than half of the participating servers, all of which would have their own security measures.

**5 – Aligning Insurer and IT Strategy**

**Objective**: Explain why an insurer’s information technology strategy should align with its overall business strategy

Practically every insurer, whether large or small, must address the challenges of aligning information technology (IT) strategies with business strategies. Despite the difficulty of the task, aligning current and new technologies with business objectives can result in more efficient and expanded operations in all departments.

**Importance of IT and Business Strategy Alignment**

How IT is aligned with core insurer operations and the integral relationships between IT and senior leadership are essential to the success of an insurer. Insurers are continually evolving operationally in response to market and regulatory influences as well as new trends in technology. Technology can create a competitive advantage as an insurer’s dependencies on information and data increase.

As insurers become more transaction-focused, the value of IT investments increases. IT is no longer a stand-alone cost center. For an insurer to grow to its full potential, IT initiatives must be aligned closely with and insurer’s key strategic goals and objectives.

*Example of an IT initiative that is not aligned with an insurer’s business goals:*

*An insurer’s Chief Information Officer (CIO) visited the vendor booths at an underwriting conference, where he found a WC policy processing system he believed could replace the outdated system they were currently using. The new, off-the-shelf application would be easy for the IT staff to master and was designed to interface easily with several external databases and state WC rating bureaus. The CIO conferred briefly with the VP of WC underwriting, and she concurred.*

*Only after purchasing this software and migrating policy processing off the old system did they realize that the new system did not capture and store key data elements necessary for both internal and external regulatory reports.*

*What went wrong? Although the CIO did consult with the Underwriting VP, the new system still did not align with business needs. In this instance, they failed to consult with personnel in the business units who use the system: underwriters, data quality manager, business analysts, and compliance staff.*

**Benefits and Challenges**

Alignment of IT goals with business goals creates both benefits and challenges. Part of the responsibilities of each of an insurer’s department managers is to identify what benefits can be expected from an IT initiative and what challenges may prevent its successful implementation.

**Benefits**

These are among the numerous benefits to all of an insurer’s department of increasing alignment between IT and business objectives:

* Sustainable improvements in service level realized for internal and external customers
* Cost reduced
* Compliance with state’s insurance department regulations attained
* Private or privileged information protected
* Best practices standardized
* Productivity increased
* Communications enhanced
* Production workflows expedited
* Competitive advantage obtained via faster implementation of new technology

These benefits can result from and IT initiative’s helping an insurer reach a business goal, such as operational excellence, that promotes efficient operations. Examples: Sustainable Improvement in service level for internal and external customers is the use of cost-of-repair estimating software that can generate more consistently accurate estimates. Cost Reduction is a program that allows employees to report monthly expenses more quickly than the previous method, which results in more available time for employees to perform productive tasks.

**Properly aligned and successfully implemented IT projects can create a chain reaction of benefits. Elevated performance can lead to improved customer satisfaction, which, in turn, may lead to fewer complaints to the insurer and state department of insurance, a lower loss ratio and lower loss adjustment expenses, and higher revenue and market share**.

**Challenges**

Every insurer has its own set of unique challenges, which can hinder the complete alignment of IT and business strategies. Challenges that can affect IT and the business functions it serves include:

* **Controlling expenses – this is often the primary concern. The benefit delivered must exceed its expense. To determine whether the investment will earn and acceptable return, assess the insurer’s ability to implement the IT project successfully**.
* Changing IT or business metrics – frequently, in IT, when a trend that management may want to act on is detected, a change occurs that causes current metrics to become obsolete. Be ready to make adjustments mid-cycle. Example increasing speed limit on a state highway will change predicted frequency and severity of BI and PD claims.
* Clearly understanding customer’s needs – Understanding their needs will help IT guide customers through the learning curve and encourage acceptance of IT initiatives. When IT is aligned to serve the business, the business can best align with customer needs.
* Management financial support – substantial infrastructure changes can be a significant investment for an insurer. Senior management may not always see the enterprise wide picture and may have varying opinions about spending budget dollars. Showing a positive correlation can help obtain IT funding.
* Lack of prioritization – IT project to-do lists do not get shorter. Projects must be prioritized to ensure adequate resources are available for successful implementation. Projects without a high enough priority may cause the insurer to incur unnecessary costs and consumption of time
* Lack of Trust – because an insurer’s IT professionals may not believe their jobs are secure, they may pursue training to obtain skills that would be desirable to another employer rather than the IT skills the current employer needs. Assurance of job security can help prevent this
* **Overly complex IT infrastructure – A legacy system that is retrofitted onto the business structure can become difficult to modify and can have trouble supporting overlying business functions. In such a case, comparative analysis should be performed to determine the costs and benefits of retaining the old infrastructure as opposed to updating the new one**.
* IT as a separate unit – IT personnel too often see themselves as a separate unit apart from the rest of the organization, rather than as people who can help a customer perform a business function. There is a business need for an IT solution rather than an interesting state-of-the art technology seeking an application.
* Lack of understanding of insurer and its needs – some IT personnel need to better understand the insurance business and the insurer’s operations to be able to more effectively align business needs with an IT solution. The corporate function needs to be on in which IT personnel are considered part of the business. Training, education and job rotation and shadowing can help resolve this concern.
* Lack of understanding of IT and its capabilities – business people need to understand the technology and what it is, and is not, capable of. Training, education, and job rotation and shadowing can help resolve this concern

**Plan for Alignment**

**To substantial increase the chances of success, IT management must be involved in the insurer’s strategic planning. Insurers that make a significant investment in the planning process in the beginning will likely save time and money as the alignment continues. These savings are probable for a variety of reasons, which include the insurer’s being able to more quickly and accurately anticipate challenges to the implementation of an alignment plan. This advance knowledge regarding which challenges will be problematic allows management to allocate resources more economically and to have them available when needed**.

Once the insurer’s strategic goals have been established, a plan should be drafted in which the business objectives are mapped with measurable IT services. Preferable, business and IT management do this jointly. By charting a path that aligns business and IT objectives, they can be prioritized and placed in the order of execution that optimizes allocation of IT resources and the business value of each IT initiative. The charted path should be a map that also shows the key touch points and interdependencies between business processes and technological opportunities.

Key resources, both internal and external, should be identified. These should be aligned so that the entire staff can function efficiently. The vision and strategy created through the planning process should be shared with the entire staff as well, so they can see the direction in which the insurer intends to go.

**Metrics of Successful Alignment**

Some insurers measure the value of a project by selecting an internal baseline with a goal of improving it by a certain percentage. Others may supplement that measurement by using industry benchmarks to compare their performance with competitors’. However, when performing this analysis, management should not lose sight of the key issue of whether an IT project is enabling the associated business goal to be met and business benefits to be realized. Tracking and measuring value from a project’s design throughout its implementation should help avoid such a situation and support the realization of benefits.

**An important way to track and measure the success of an IT project is to evaluate the efficiency and effectiveness of the business process it is intended to improve and to show tangible results.** Although it is recommended that metrics be developed that are tailored to a specific insurer’s objectives, some standard metrics can work well for any organization:

* Percentage of uptime- consider how downtime affects the functionality and value of the system. What costs re incurred, including missed opportunities, because of downtime of the system?
* Functionality – what is the purpose of the project, and which business process is it supporting or improving? Determine whether the project is meeting that purpose
* Problem resolution – are the concerns of internal and external customers being addressed efficiently? Is there one central office or point of contact to which customers can go for the project? How long does it usually take for customer’s problems to be resolved?