**Information Governance in the Hotel Industry**

Student’s Name

Institutional Affiliation

Course Name and Number

Professor’s Name

Date

**Information Governance in the Hotel Industry**

**Introduction**

A Chief Information Governance Officer is required in the hotel sector to build and preserve an enterprise-wide culture of accountability and correct management of any business-focused information. Leadership, strategy, technical, and engagement would be the four primary categories in which the CIGO's core responsibilities would be split. I would be tasked with developing programs and technology recommendations based on the needs of the Board of Directors, such as creating a metric for measuring information governance success, recommending any relevantprivacy and security compliance policies, and developing a social media strategy.

**Metrics**

The hotel industry, like other modern organizations, understands the value of good information governance processes. As a result, our business has put policies to manage data collected manually but in an electronic format. There is widespread concern about losing essential company information, which has resulted in the development of information governance programs. To ensure that information governance plans are followed, they must be defined and assessed for compliance. It is possible to determine the efficacy of an information governance program in various ways, and it can be as complex as starting it. Although selecting the appropriate, acceptable metric is always the most difficult, the benefits and increasing prevalence of information governance initiatives are undeniable (Sirur, Nurse & Webb, 2018, January). When establishing a measure that will best satisfy our goals, we must consider two major factors: the technology in place and the type of data held therein. The second set of plans is for our information governance program.

In terms of technology and documentation, it's worth emphasizing that our company now keeps data in electronic formats, which complicates governance. As a first-level measure of success, the metric should use previously collected data points (Brooks, 2019). Consider if the total amount of data kept decreases or increases, as well as how frequently archived documents are retrieved. The Enterprise Content Administration solution would be advantageous in gathering more detailed statistics on electronic information access, control, and management.

Although our company creates digital data, we still have a few paper records to keep track of. Understanding what happens with printed papers is a crucial aspect of information governance. I would also recommend that all paper records be managed and retained by third-party providers off-site. In terms of storage by department and location, storage and recovery patterns, and the number of extra boxes added, metric-based reporting for paper records would employ a somewhat different set of criteria. Keeping track of the program's paper and electronic metrics would give a clear picture of its functions. Most importantly, transferring information into readily managed and measurable repositories, such as from paper to digital and eventually into an ECM solution, will benefit the organization.

Another topic to consider for measuring is the goals of information governance, which vary depending on the size of the organization and the regulatory environment. These goals will fall under numerous benefit areas, such as enhancing regulatory compliance, protecting confidential and personal data, lowering IT storage and management costs, and minimizing legal action risks. The CEO would be in charge of creating the program's objectives. The program's efficacy would be measured by gathering and analyzing metrics and determining whether or not they represent the objectives.

Secondary metrics that are entirely connected with the program's objectives will provide a deeper level of comprehension. One of our program's goals is regulatory compliance, and we'll investigate whether information governance has helped reduce supervisory overhead. The program will also be reviewed to check if the ratio of papers recovered and used to those not retrieved and used is manageable. Finally, one of the goals is to lower legal risks. The data volumes will determine this, the number of irrelevant documents recovered and the time required to complete an e-discovery activity.

Other metrics, in addition to these, would help the executive determine whether the information governance program is having the desired impact. The first take measures to manage, and Grays (2019) asserts that one cannot control what one cannot measure. This assumption is valid in information governance, and the organization must determine an appropriate metric for its program. The other alternative is to make the findings public to stimulate everyone in the company. Last but not least, the software must be easily accessible, actionable, and auditable so that the figures' authenticity can be easily checked.

**Data That Matters To the Executive**

One of the most critical pieces of data for a business's management is data integrity, which refers to the quality and validity of the data obtained throughout the business's existence. After all, a corrupted data set is of limited or no use to the business, and the loss of sensitive data poses several risks. As a result of these challenges, it is critical to emphasize the essential nature of data integrity.

According to Zikratov et al. (2017), data integrity can be violated in various ways, and it should always be maintained when information is moved or replicated. To maintain the integrity of stored data, error scrutiny systems and authentication procedures are strongly advised. Maintaining data integrity is critical for a variety of reasons. The first is that it will make a recovery, connectivity, searchability, and traceability significantly easier. The second reason is that it verifies the data's accuracy and legitimacy. Finally, it facilitates reuse and maintenance while also boosting stability and performance. All of these issues should compel the executive to fund information governance programs that improve data integrity.

Even if data must be arranged in a manner that enables informed decision-making, data has a significant impact on the business decision-making process. As a result, data integrity must be a significant priority for our organization. Human errors, whether accidental or intentional, data transmission failures, cyber-attacks, faulty technology, and physical compromise are all systematic ways to compromise data integrity. Because the bulk of these concerns are avoidable by data protection, data backup and duplication are critical for our data security (Gaetani et al., 2017). Additionally, our organization benefits significantly from data integrity techniques such as validation to prevent the insertion of meaningless data, error exposure methods to detect any potential problems during data transmission, and security measures to prevent data loss and unauthorized access.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Employee-ID | Employee Name | Job Name | Salary | Number |
| Post-Academy001 | Levin | Technician | 35,000 |  |
| Post-Academy002 | Philip | IT consultant | 48,000 |  |
| Academy003 | Mercy | Manager | 99,000 |  |

This does not follow the user-defined Integrity, thus not acceptable.

Because client data is stored in databases, database integrity must also be ensured. In the workplace, database management can be done in a variety of ways. The first is through "entity integrity," which protects the accuracy of customer data by leveraging a large number of columns, rows, and tables. A client database, for example, might contain primary vital data such as their names and a unique customer recognition code (Vainshtein & Gudes, 2021, July). The second option is "Referential integrity," which prioritizes the database's primary key table by using foreign keys in the following table. The third component is "Domain integrity," which defines the database's categories and values. Finally, "User-Defined Integrity" lets consumers or individuals outside the company create their own data sets.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Roll no | Customer-name | Age | Recognition number | Foreign number |
| 1 | Noel | 24 | 779 |
| 2 | Ben | 46 | 889 |
| 3 | Annalisa | 28 | 3456 |
| 4 | Mary | 33 |  |

Primary key this value can be null as the customer may not be available anymore

Primary key

**The Roles for Those Executives**

The executive can take on a range of roles in information governance projects, including, but not limited to, developing an integrity culture. Data integrity includes taking safeguards and developing an open, honest, and transparent culture. Such minor efforts will guarantee that the organization stays on pace and that data integrity is preserved. Another duty is to promote collaboration within the organization. Maintaining data integrity necessitates having all employees on the same page regarding who is in charge of creating, modifying, and transferring data. In a data breach, the executive must also maintain an audit trail to track down the source. These audit trails will also ensure that the organization receives breadcrumbs indicating the source of any data errors, allowing them to be remedied as soon as possible. Finally, the executive should establish process maps for any essential data, (Gaetani et al., 2017). This allows you to keep track of how and who is using your data, as well as maintain a close eye on it and keep it from being misused.

**Regulatory, Security, And Privacy Compliance Expectations for the Company**

The organization requires an integrated platform to respond to customer audits and fully comply with legal and regulatory standards. The organization must recognize that "negligence equals accountability" and comply with applicable data privacy laws and regulations. It must establish and adhere to clear policies governing the provision of its services, which include personal data. Additionally, the organization must develop and implement a system capable of properly storing and utilizing personal data, as well as providing an audit report demonstrating that the data is being used properly. This can begin with metadata and folder systems that categorize and organize materials uniformly across content management systems. This will assist users in quickly adopting the content structures (Apthorpe, Varghese & Feamster, 2019). Due to the highly confidential nature of the business, the organization may also utilize "Need-to-Know Security." Only the necessary few will be provided access to the data. Additionally, approved individuals who are actively participating in specific activities will have access to customers' data. While this will improve the organization's security and privacy compliance, it will also demand extra technology and personnel, (Gaetani et al., 2017).

Additionally, the organization can create data mapping capabilities to comply with several confidentiality and cybersecurity regulations. This enables the business to keep track of the many types of data, who has access to it, and where it is stored. Additionally, the corporation must defend its responses to subject admission requests, including giving customers to copy data and any other supporting material (Lansing et al., 2019). There is always a need to answer as fast as possible to such inquiries.

Allowing for trigger-based data minimization is also necessary for data relocation and deletion. This would require content to be moved between and among multiple systems to archive, modifying security settings, and deleting. Additionally, the firm should assure by utilizing analytics to verify that policies are being adhered to precisely. A reporting schedule and automated assurance mechanism would be necessary. There is need of a customized dashboard for tracking all actions and an audit report on compliance and source systems with data reduction criteria. Finally, the corporation is expected to have a business continuity plan for internal procedures and vendor operations.

**Email and Social Media Strategy**

The rapid growth of social media has changed the way individuals connect at home and work. It has influenced communication strategies and policies, as well as organizational learning, employee engagement, corporate intelligence and learning, data security, and collaboration. The usage of personal social media accounts in the office has sparked worries about productivity, data security, and network security (Alimam, Bertin & Crespi, 2017). As a result, HR personnel must take the lead in developing, enforcing, and promoting social media policies throughout the organization.

Collaborative technologies are coveted in any industry to effectively create relationships, increase knowledge, and allow lateral communication. Because social media is such a new area for us at work, many people still have doubts about how and when these tools should be used in the office. The major challenge is how to derive economic benefits from the platforms while simultaneously ensuring that social media does not suffocate productivity and instead becomes harmful to the organization. Any company that does not incorporate social media into its marketing strategy risks becoming irrelevant in the marketplace. As a result, the company's strategic strategy for recruiting, training, and promoting organizational reforms should include various social media outlets. Because the advertisement will reach a much larger audience, using social media in the recruitment process will result in the company taking less time to fill openings and possibly attracting the top candidates. Self-direction can also help the company save money on training and boost employee growth. The company should consider making the most of the benefits that social media provides, such as facilitating open communication, facilitating open deliberation on ideas, reaching a large audience, improving the company's social reputation, promoting diversity and inclusion, and increasing market research and learning.

Despite its many advantages, social media poses a considerable security risk to employees and customers, as well as a legal liability. The use of social media within the organization, whether for professional or personal reasons, is likely to expose the company in various ways, including the potential of fraud and spam and virus attacks from hackers. Several personnel at the company may be falling victim to internet scams that appear to be accurate, resulting in data loss and a violation of the company's data integrity (Jorge et al., 2020). Some employees may use social media to make negative comments about the organization, which may be seen by the broader public. Finally, if firm employees use the sites to access illegal content, legal fees may be incurred. Given the advantages and disadvantages of social media use, it is suggested to be encouraged but utilized carefully.

**Cloud Computing Strategy**

The cloud enables on-demand access to services, resources, and applications over the internet. Without direct supervision from the CEO, the firm can use cloud computing to store data and calculate power. According to Khalil (2019), cloud computing has five essential characteristics: resource consolidation, restricted service, rapid flexibility, extended network interaction, and on-demand self-service. All of this would be necessary to ensure the company's continued relevance.

The Cloud Computing Strategy would enable the firm to save money on capital expenses by eliminating the requirement for frequent equipment replacement. By moving the burden to the cloud, the business may convert capital expenditures to operating expenses, simplifying budgeting. Additionally, the plan assists in right-sizing the business and increasing its agility without incurring substantial costs or inconveniences (Attaran & Woods, 2018). Finally, cloud computing is critical for employee transformation and retention. Allowing people to work in their preferred manner can assist with this. Finally, Cloud Computing is crucial for dealing with large amounts of data by getting real-time data from equipment and processing and analyzing it.

**Conclusion**

Any firm seeking to accelerate innovation, boost revenue, and optimize its business objectives should implement a cloud computing solution. This not only reduces workload but also ensures the security and integrity of data. A CIGO's primary responsibilities in establishing an enterprise-wide culture are to drive information capability and digital innovation, to provide expert and up-to-date guidance on information governance, to lead information governance across the organization, and to deploy best practices for information management.

**References**

Alimam, M., Bertin, E., & Crespi, N. (2017). ITIL perspective on enterprise social media. *International Journal of Information Management*, *37*(4), 317-326.

Apthorpe, N., Varghese, S., & Feamster, N. (2019). Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus {COPPA}. In *28th {USENIX} Security Symposium ({USENIX} Security 19)* (pp. 123-140).

Attaran, M., & Woods, J. (2018). Cloud Computing Technology: A Viable Option for Small and Medium-Sized Businesses. *Journal of Strategic Innovation & Sustainability*, *13*(2).

Brooks, J. (2019). Perspectives on the relationship between records management and information governance. *Records Management Journal*.

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). Blockchain-based database to ensure data integrity in cloud computing environments.

Grays, T. (2019). Information Governance-A Primer. *Int'l. In-House Counsel J.*, *12*, 1.

Jorge, L. F., Mosconi, E., de Santa-Eulalia, L. A., & Marion, G. (2020, October). Conducting an Enterprise Social Media Initiative in the Digital Transformation Context. In *17th International Conference on Intellectual Capital, Knowledge Management & Organisational Learning ICICKM 2020* (p. 187).

Khalil, S. (2019). Adopting the cloud: how it affects firm strategy. *Journal of Business Strategy*.

Lansing, J., Siegfried, N., Sunyaev, A., & Benlian, A. (2019). Strategic signaling through cloud service certifications: Comparing the relative importance of certifications’ assurances to companies and consumers. *The Journal of Strategic Information Systems*, *28*(4), 101579.

Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 88-95).

Vainshtein, Y., & Gudes, E. (2021, July). Use of Blockchain for Ensuring Data Integrity in Cloud Databases. In *International Symposium on Cyber Security Cryptography and Machine Learning* (pp. 325-335). Springer, Cham.

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017, April). It is ensuring data integrity using blockchain technology. In *2017 20th Conference of Open Innovations Association (FRUCT)* (pp. 534-539). IEEE.