Prompt

Your new role as Chief Data Officer of a medium sized organisation providing specialised data analytics as a cloud provider requires you to create and present a data governance programme that meets the business needs.

Provide a Broad explanation of:

- The necessity of a data governance strategy.
- An overview of the pertinent roles and responsibilities in the organization.
- A data governance operating model that aligns with both business and technical requirements.

Your responses should include projects to remedy data inadequacies, data policies, operational processes or procedures that ensure the effective implementation of the data governance strategy.

Response

For an organisation dealing with large amounts of data, it's imperative that the organisation has a data governance plan. Otherwise, the company is losing significant advantages and creating serious, unnecessary risk. From a generative viewpoint, a data governance plan can help generate increased revenue. However, it can also save the organisation millions of euros that would have been otherwise lost in fines from the Data Protection Commission, following a breach of any of the legislation in place in Ireland.

For example, imagine a scenario whereby an organisation has a large repository of personal, sensitive data, such as health data. Further imagine that the data's security is inadequate, and the organisation has not evaluated the data well, so it cannot be entirely accounted for. This scenario is highly at risk of a cyber-attack, which would have serious repercussions:

- Lots of people would lose very sensitive and personal information, which may lead to individual litigation.
- The loss of trust as a cloud provider would lead to decreased revenue due to a lower uptake in services.
- There would be significant fines imposed by the DPC.

The ramifications of these ethical and financial failings would be significantly mitigated by a data governance plan.

These scenarios are not hypotheticals either. This process is in situ regarding the HSE ransomware attack in 2021. The costs have been massive and still not fully imposed. Furthermore, on a more day to day scenario, consider a financial services company that has concluded, after carrying out risk analysis on data that is 90% certified, that there is risk exposure of €10 million. This still leaves €1 million euro unaccounted for, which could strongly impact the key decisions of the company.

Ultimately, data is a valuable commodity, and it needs to be treated as such. Thus, it's important to ensure that it can't be stolen, it's accounted for, and it's treated with the respect it deserves.

Thus, we can see that a data governance plan is crucial. In the rolling out of this programme, it's imperative that all roles must be clearly defined and ensure that responsibilities are clearly

communicated, so that there is a good balance and good separation between the tactical, operational and executive.

The executive level will include the most senior members in the data department. The CDO will establish an organisation-wide data strategy, establish standards, and provide general oversight. The DG Council will advise the CDO on any decisions to be made and will report up with any issues.

Then, at the tactical level, we have the steering committee, who will look at how the data governance plan is implemented. The job of the steering committee is to provide direction and ensure that any initiatives are put into action effectively.

Finally, on the operational level, there are the data stewards. These are the individuals who manage the property on behalf of the controller. As a result, they represent all stakeholders. They ensure that all data is of high quality and effective and manage any quality issues.

There may also be the data policy officer, who implements new policies following changes to legislation or that help with compliance, a data protection officer, to ensure that data remains confidential and a data architect, engages and plans for the IT aspect. It's important to remember that data is business led with IT input, not IT led.

This is because it's important to ensure that the data governance programme is facing the same way as the business. It's important to ensure that data governance is viewed as a positive thing, and not as something that is pushing back against the company. Hence, the plan must be adaptable with the organisational goals.

Thus, there needs to be a model chosen that most effectively meets the organisation's needs. As is typically in business, the larger an organisation grows, the more complex it's needs are. This is the same for data governance. For a medium sized, cloud computing company, who operate as a data processor, there are three main models that could be appropriate.

Firstly, there's a decentralised execution with multiple business units. This involves data users maintaining their own data. This is generally more agile but allows for a shorter life span. There are also fewer risks stemming from data breaches. However, the data quality is much lower here.

Secondly, there's a centralised governance with business units, where one centralised authority takes control of the master data. This is beneficial if there are multiple plants and there's a need for data to be shared regularly with other business units. There is also a high-quality assurance of the data as there are a limited number of users in the centralised body. However, it raises the exposure risk from data breaches and is significantly more complex to set up, which may cause delays while it's setting up.

Thirdly, there's a centralised data governance with a decentralised execution. This is where there is a centralised body defining directions and each individual business unit creates their own master data. Again, this has benefits in that it has a more controlled creation of the master data. It is also much more agile as there are more people working on it However, since it is a master data, it also creates risks from a data breach, and has complex needs.

There are also the issues to consider regarding cloud providing itself. The company must ensure that an adequate level of protection to the data is offered to the client. There must be sufficient information about security and the safeguards being offered available. Furthermore, the provider

must also be able to adequately support the rights of the data subjects/clients. Incompetence is not a valid defence.

This is because there are many ways cloud computing can be compromised. Data can be accidentally lost, or storage can be misconfigured, or it can be damaged/stolen via: insider threats, Dos attacks, breaches, malware infections, etc.

Thus, it must be ensured that the provider only processes data in accordance with the controller's instructions. The provider must also consider all the risks associated with the personal data that is handled by the provider. The provider must be able to give assurances as to: pseudonymisation and encryption of any personal data, the ability to isolate the personal data of the subject from other's data, the ability to ensure confidentiality, integrity, availability and resilience of all systems and services, and the restorability of the data. The provider should also be able to assure: there is regular testing, assessing, and evaluating security, procedures in a breach and a means to return and terminate all personal data in the termination of a contract.

Regarding the model chosen, I would think that in a cloud computing company, optics on data security would be crucial. I think that there's no room for failure, and consequently, a minor breach could be nearly as consequential as a major breach. The potential consequences of a data breach would be higher in a centralized governance, but there would be a lower risk in that there are fewer devices to keep secure. Thus, I think the correct choice here would be to choose a centralised governance plan and ensure that internal security is kept as strong as can be. This also allows for the assurance of the continued lifespan of the data. Then, I think that quality of data is more important than speed of transfer, as a cloud computing company wants their data to be accurate. Thus, I think the correct choice would be a centralised governance with multiple business units.