Week#5- Q1:

Q1: With this framework in mind that allows for a conceptual look at data governance processes, rules, and people requirements identify and name the 10 levels of the DGI Data Governance framework from the Data Governance Institute?

A)

Data governance (DG) is the overall management of the availability, usability, integrity and security of data used in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures and a plan to execute those procedures. the 10 levels of the DGI Data Governance framework from the Data Governance Institute are the frameworks help us organize how we think and communicate about complicated or ambiguous concepts. The Data Governance Institute wanted to introduce a practical and actionable framework that could help a variety of data stakeholders from across any organization to come together with clarity of thought and purpose as they defined their organization’s Data Governance and Stewardship program and its outputs.

The 10 levels of Data Governance framework components are as follows

Rules and Rules of Engagement:

1. Mission and Vision

2. Goals, Governance Metrics and Success Measures, and Funding Strategies

3. Data Rules and Definitions

4. Decision Rights

5. Accountabilities

6. Controls People and Organizational Bodies

7. Data Stakeholders

8. A Data Governance Office

9. Data Stewards Processes

10. Proactive, Reactive, and Ongoing Data Governance Processes A

Data Governance Components that deal with Rules and Rules of Engagement

1.Mission and Vision

At its highest level, Data Governance typically has a three-part mission:

1) Proactively define/align rules.

2) Provide ongoing, boundary-spanning protection and services to data stakeholders.

3) React to and resolve issues arising from non-compliance with rules.

2. Goals, Governance Metrics and Success Measures, and Funding Strategies:

Some organizations have stand-alone Data Governance budgets to address all these efforts. Others take advantage of other groups’ budgets. Still others are forced to fit all efforts – even ongoing program tasks – into project budgets. Whichever fits your funding model, consider whether you will need to acquire project codes for Data Stewards and other participants with ongoing responsibilities, or for data management, metadata management, and technology resources asked to participate in research and analysis.

3. Data Rules and Definitions:

This component refers to data-related policies, standards, compliance requirements, business rules, and data definitions. Depending on your focus areas, your program may work to

• Create new rules/definitions

• Gather existing rules/definitions

• Address gaps and overlaps

• Align and prioritize conflicting rules/definitions

• Establish or formalize rules for when certain definitions apply.

4. Decision Rights:

Decision rights for compliance-based programs are often simple to define. For example, should the decision about whether to comply with a federal law be left to a vote of those who will have to live with the decision? Of course not – that decision needs to be made by the organization’s Board of Directors, with input from the Legal department. For other types of programs, decision rights may require more negotiation. For example, who should decide the length of a

data field in a new system maybe the decision should be made by Data Architecture. But maybe it requires input from many stakeholders. Maybe one of them has a constraint that needs to drive the decision.

5. Accountabilities:

Once a rule is created or a data-related decision is made, the organization will be ready to act on it. Who should do what, and when? For activities that do not neatly map to departmental responsibilities, the Data Governance program may be expected to define accountabilities that can be baked into everyday processes and the organization’s software development life cycle (SDLC).

6. Controls:

Controls can be automated, manual, or technology-enabled manual processes. You may find it useful to describe some of the work that Data Stewards do in terms of specifying, designing, implementing, or performing data-related controls. You may also be asked to recommend data-related controls that could be applied to user processes, applications, databases, or other parts of the data environment. Examples are Change Control, sign-offs, and data quality checks embedded into applications.

7. Data Stakeholders:

Data Stakeholders come from across the organization. They include groups who create data, those who use data and those who set rules and requirements for data. Because Data Stakeholders affect and are affected by data-related decisions, they will have expectations that must be addressed by the Data Governance program.

8. A Data Governance Office:

DGO will depend upon the scope of work you’re trying to accomplish with your program. It will depend on whether your DGO needs to include data analysts or whether governance staff (and those researching and analyzing data-related issues, defining data, and recommending standards) can count on having consistent access to data management and metadata management resources.

9. Data Stewards:

The Data Stewardship Council consists of a set of Data Stakeholders who come together to make data-related decisions. They may set policy and specify standards, or they may craft recommendations that are acted on by a higher-level Data Governance Board.

10. Proactive, Reactive, and Ongoing Data Governance Processes:

These processes should be standardized, documented, and repeatable. They should be crafted in such a way to support regulatory and compliance requirements for Data Management, Privacy, Security, and Access Management.

Every organization will decide how much structure and formality to bring to the process of governing data.

1. Aligning Policies, Requirements, and Controls

2. Establishing Decision Rights

3. Establishing Accountability

4. Performing Stewardship

5. Managing Change

6. Defining Data

7. Resolving Issues

8. Specifying Data Quality Requirements

9. Building Governance Technology

10. Stakeholder Care

11. Communications

12. Measuring and Reporting Value

References:

Gianni, D., (2015, Jan). Data Policy Definition and Verification for System of Systems Governance, in Modeling and Simulation Support for System of Systems Engineering

Sarsfield, Steve (2009). "The Data Governance Imperative", IT Governance.

Week#5 – Q2:

Q2: From this research revelation in our chapter 11, briefly state and name the countries and organizations identified as the targeted victims?

A) The organizations identified as the targeted victims are the most common threats that businesses experience, including polymorphic malware, man-in-the-middle attacks, cryptominers, DDoS bots, and targeted intruders, and describes security techniques that can mitigate the impact of those threats. The paper goes on to describe five real cyberattacks that Check Point's Incident Response Team encountered on customers' networks and how each was remedied.

So many countries, companies and organizations, ranging from the US government to the UN and the Olympic movement, have had their computers systematically hacked over the past five years by one country, according to a report by a leading US internet security company.

The report, by McAfee, did not openly blame any country but hinted strongly that China was the most likely culprit, a view endorsed by analysts.

China has previously been implicated in a range of alleged incidents of cyberspying – a practice Beijing vehemently denies – including a concerted attack on Google and several attempts to prise secrets from computers at the Foreign Office. But the McAfee report is among the most thorough attempts yet to map the scale and range of such data-theft efforts. "The blueprints are only part of the picture. The technology for, say, how to build a sophisticated jet engine is one thing, but there's a whole set of other processes – the logistics, how to manage the supply chain to build more than one, the long-term management of a really advanced manufacturing process. " McAfee learned of the extent of the hacking campaign in March this year, when its researchers discovered logs of the attacks while reviewing the contents of a “command and control” server that they had discovered in 2009 as part of an investigation into security breaches at defense companies. an integrator or other security professional who is educated in privacy compliance could offer value to the end user and protect the privacy of consumers and passers-by through providing guidance regarding the deployment of cameras and, potentially, other devices.

Reference:

Louis Kriesberg, Constructive Conflicts: From Escalation to Resolution, 3rd ed. (Lanham, MD: Rowman & Littlefield, 2007), 239.

William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” Foreign Affairs, September/October 2010.