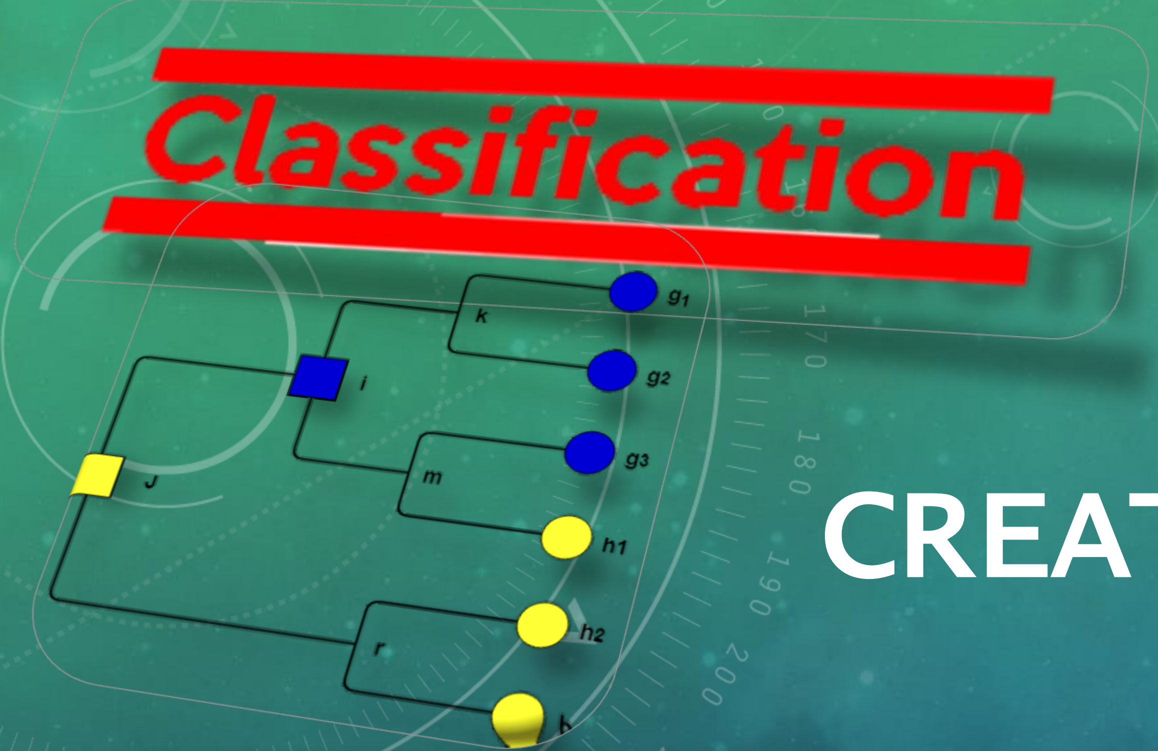


UNIVERSITÉ DE LORRAINE

UFR MATHÉMATIQUES INFORMATIQUE MÉCANIQUE ET AUTOMATIQUE

CIRCL MISP

CREATING A CORPORATE TAXONOMY

MARWIN NIMESKERN

GRÉGORY GUGGENBUHL

JULES CHARRON

SUMMARY

- What is a corporate Taxonomy ?
- State of art : Taxonomy
- GEA – NZ / Bugyo
- Enhancement of GEA-NZ
- Hierarchical Ascending Classification (HAC)
- Example Applicative

WHAT IS A CORPORATE TAXINOMY ?

Classify entities of an

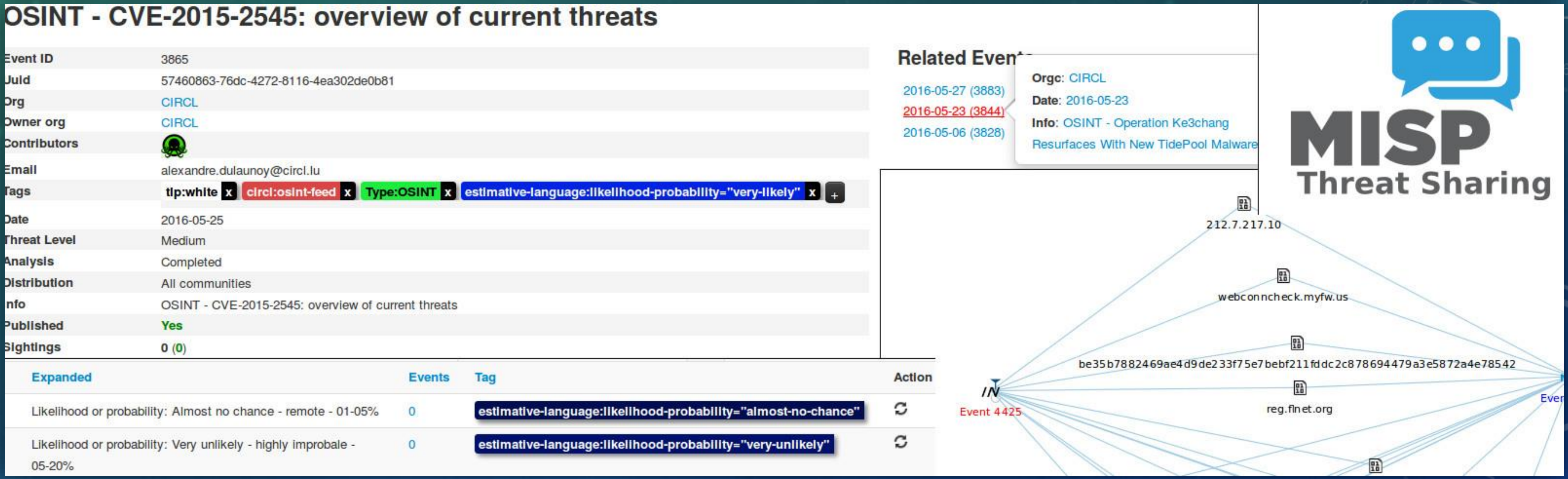
- Enterprise
- Organization
- Administration

used to classify

- Documents
- Digital assets
- Other information

What?
Who?
Taxonomy
Why?
How?

MISP: MALWARE INFORMATION SHARING PLATFORM AND THREAT



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Juid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
nfo	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Even

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

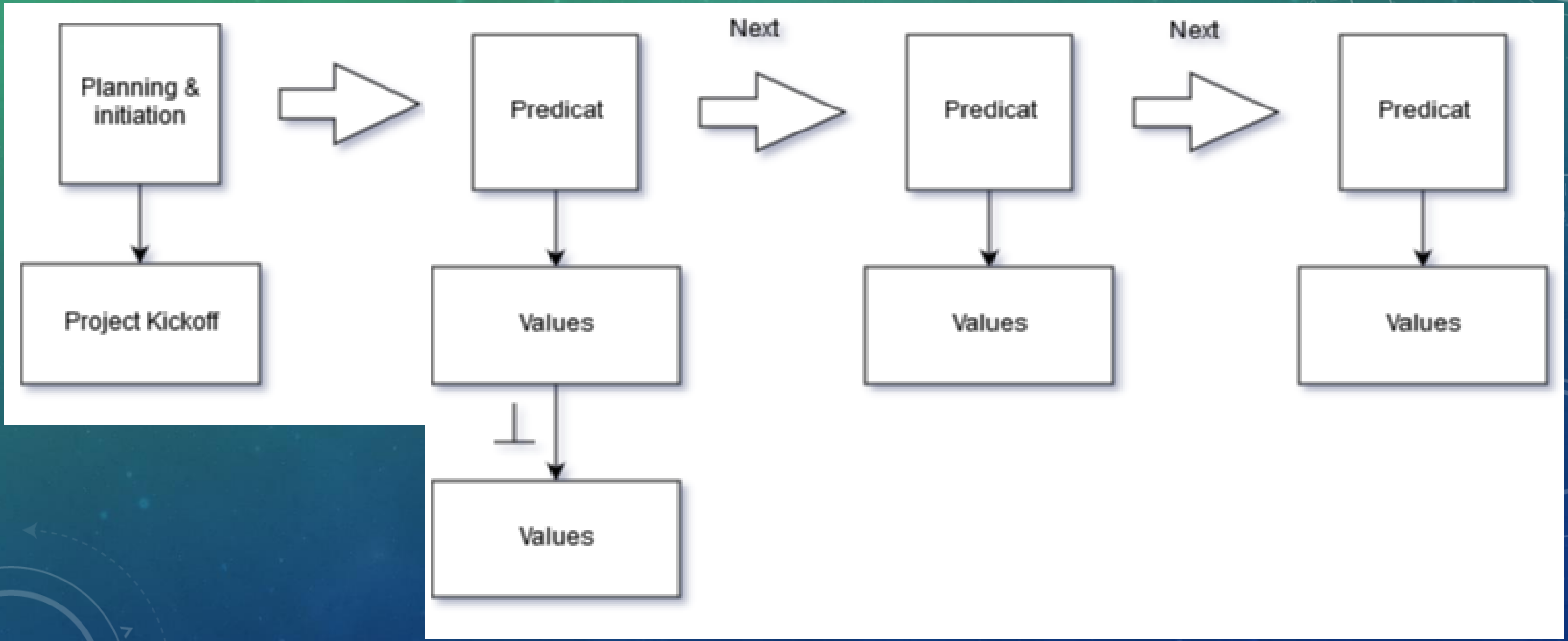
Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	⟳
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	⟳

ERCOT FACETED CLASSIFICATION

Function	Activity	Type	Entity Type	Entity	Rule Type	System Name
Market Participation	Registration and Qualification	Registration Documents	Market Participant		Protocol	
Information Technology	System and Application Development	Revision and Change Request	Market Participant	TDSP		MarkeTrak

ARCHITECTING AN ENTERPRISE CONTENT MANAGEMENT STRATEGY



Planning & initiation

Project Kickoff

Predicat

Values

⊥

Values

Next

Predicat

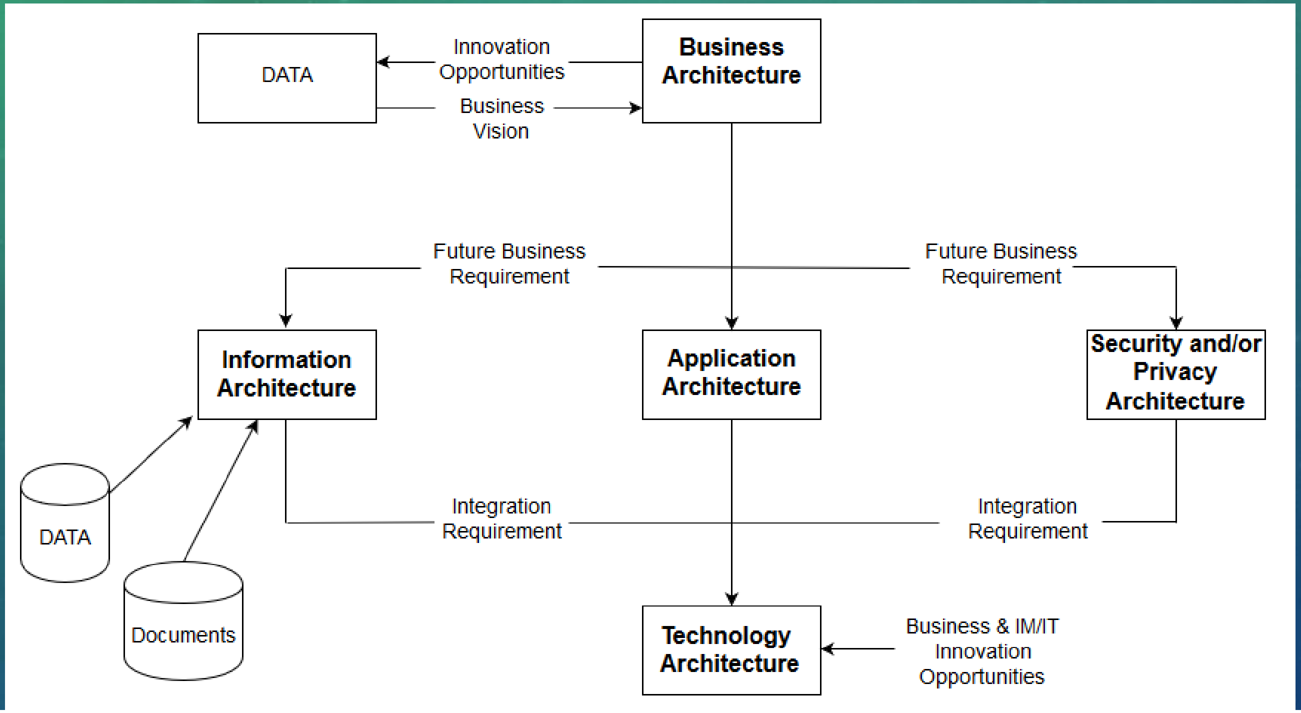
Values

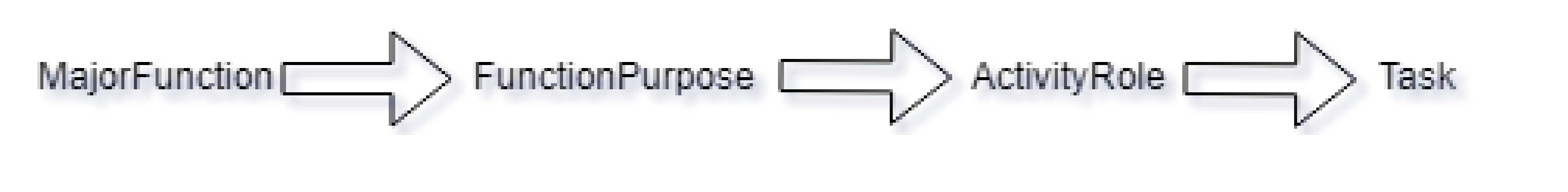
Next

Predicat

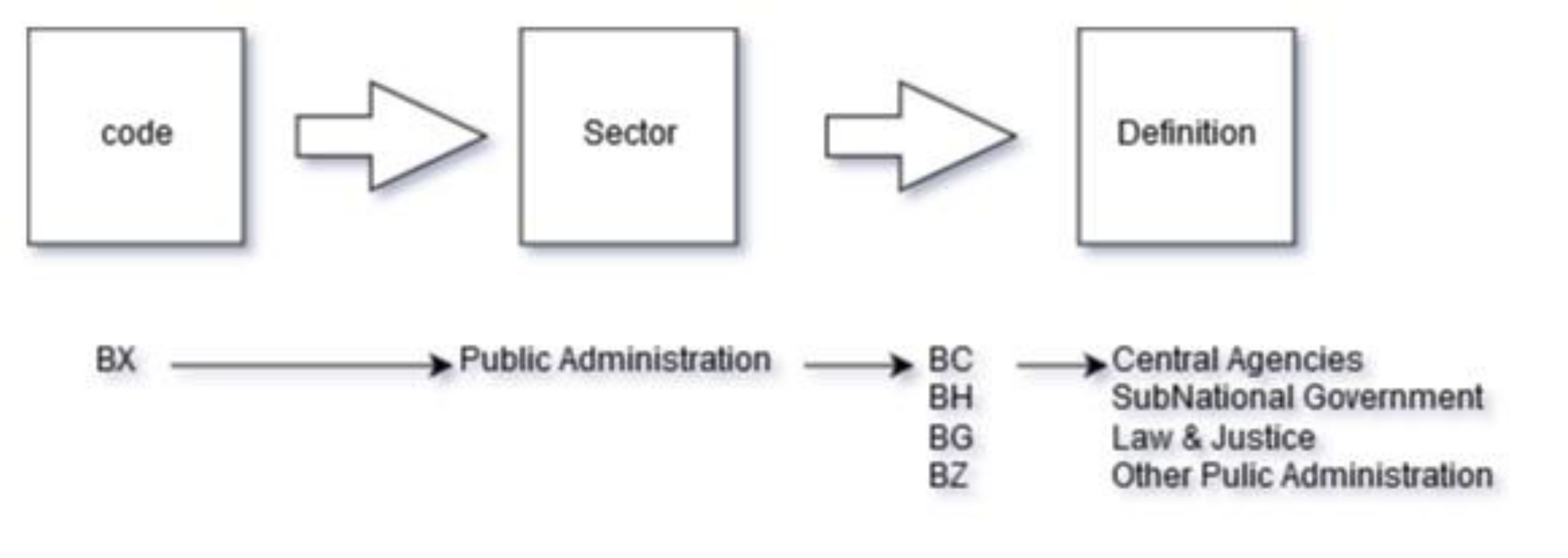
Values

FUNCTIONAL CLASSIFICATION TAXONOMIES





SECTOR TAXONOMY AND DEFINITIONS



code → Sector → Definition

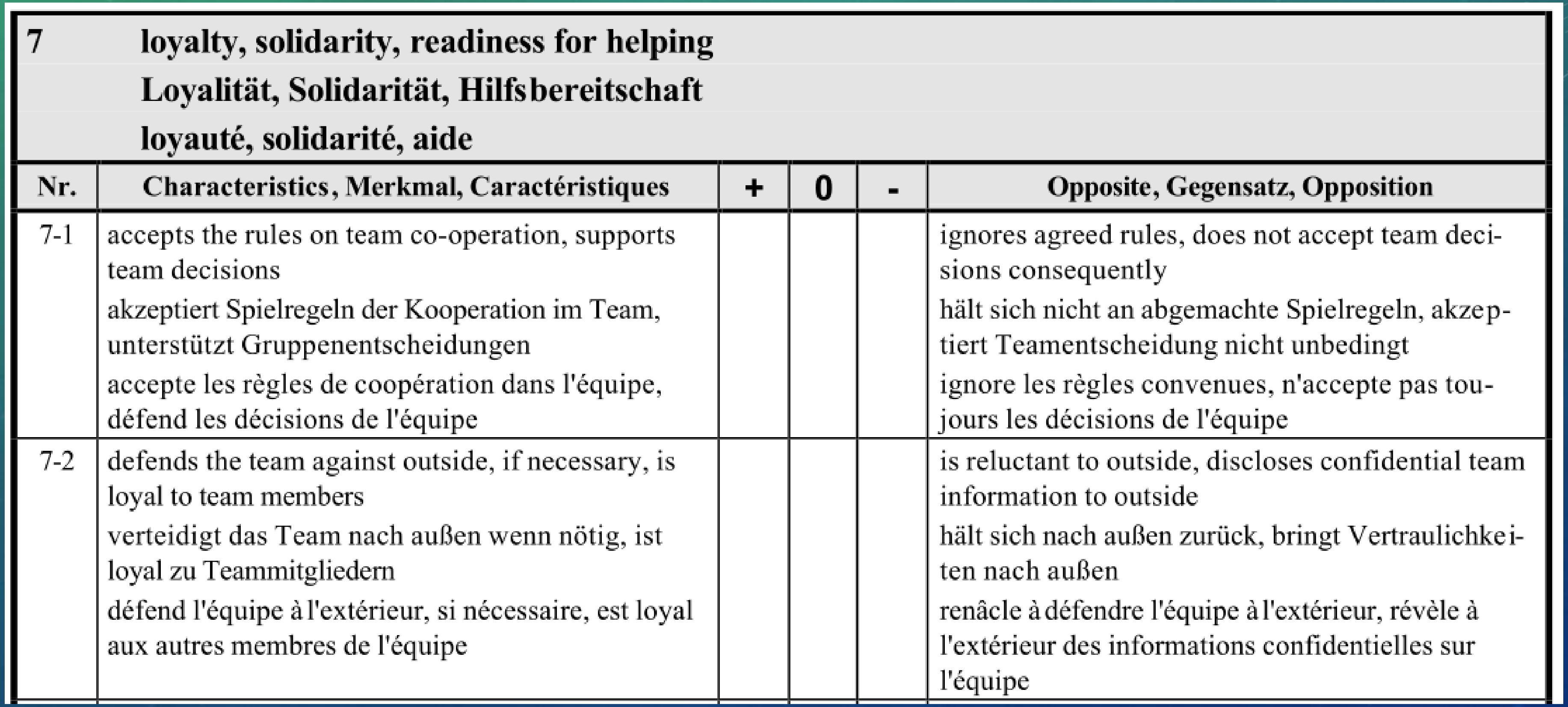
BX → Public Administration → BC → Central Agencies

BH SubNational Government

BG Law & Justice

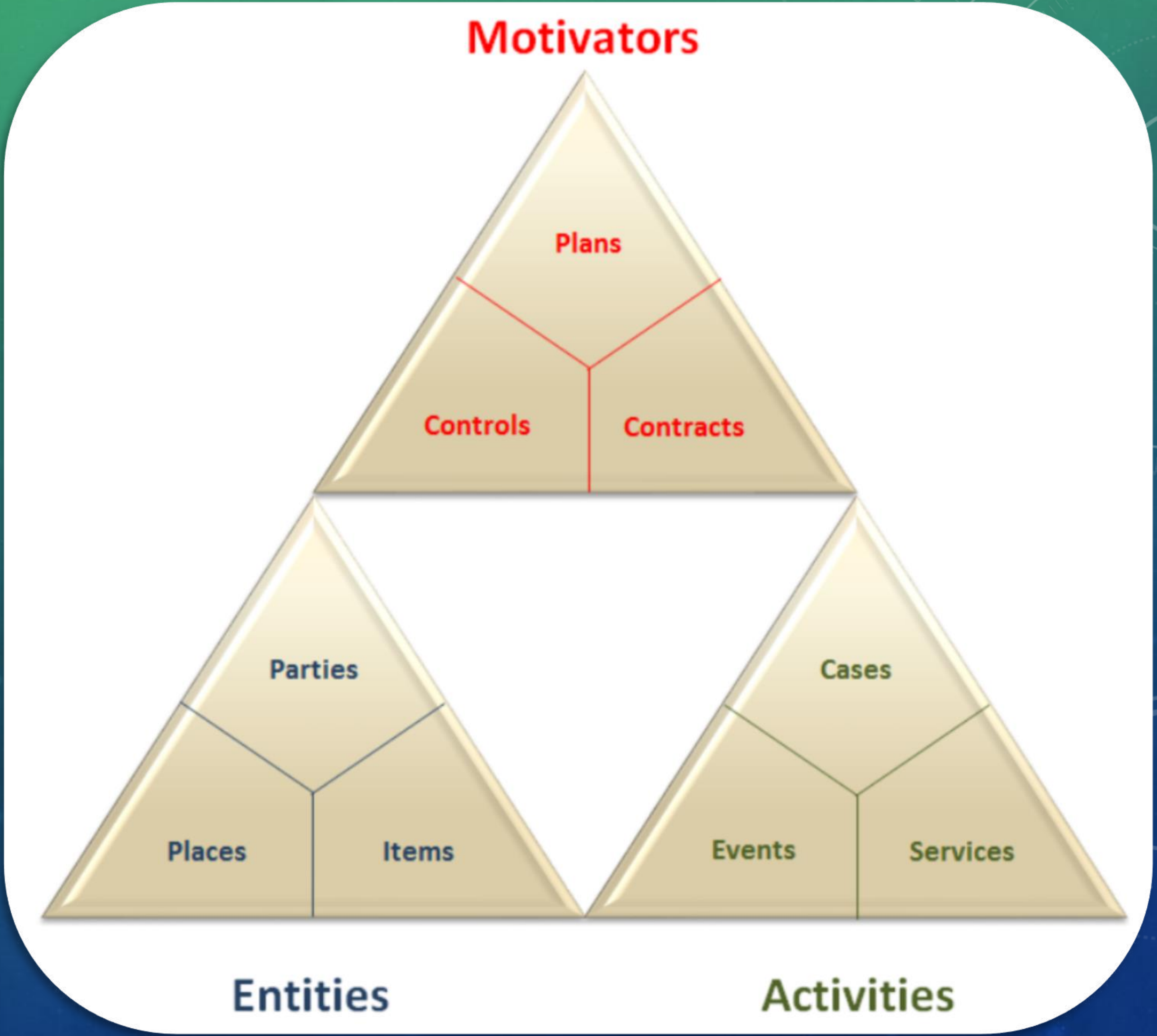
BZ Other Pulic Administration

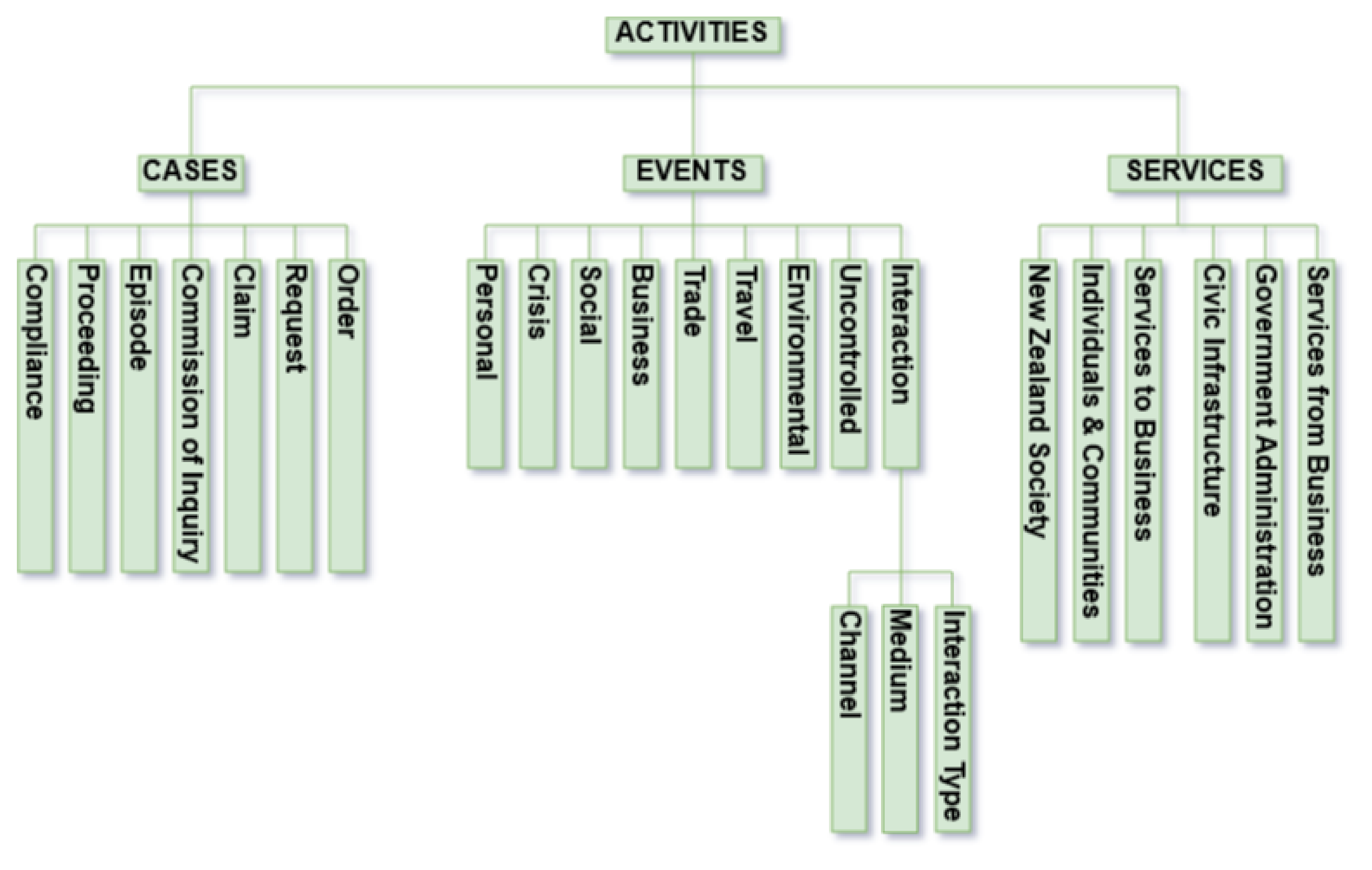
ICB VERSION 2: IPMA COMPETENCE BASELINE



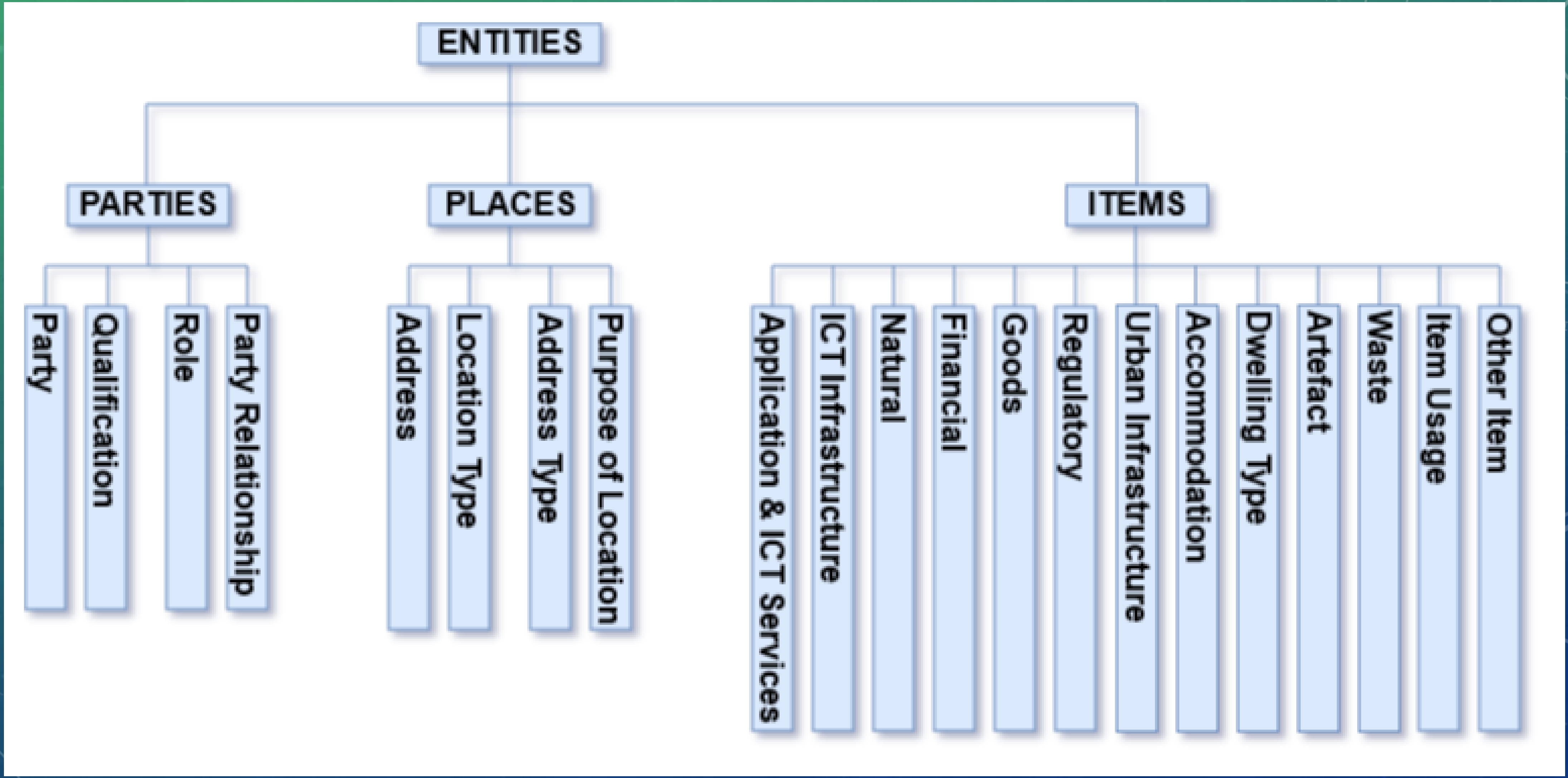
7	loyalty, solidarity, readiness for helping Loyalität, Solidarität, Hilfsbereitschaft loyauté, solidarité, aide				
Nr.	Characteristics, Merkmal, Caractéristiques	+	0	-	Opposite, Gegensatz, Opposition
7-1	accepts the rules on team co-operation, supports team decisions akzeptiert Spielregeln der Kooperation im Team, unterstützt Gruppenentscheidungen accepte les règles de coopération dans l'équipe, défend les décisions de l'équipe				ignores agreed rules, does not accept team decisions consequently hält sich nicht an abgemachte Spielregeln, akzeptiert Teamentscheidung nicht unbedingt ignore les règles convenues, n'accepte pas toujours les décisions de l'équipe
7-2	defends the team against outside, if necessary, is loyal to team members verteidigt das Team nach außen wenn nötig, ist loyal zu Teammitgliedern défend l'équipe à l'extérieur, si nécessaire, est loyal aux autres membres de l'équipe				is reluctant to outside, discloses confidential team information to outside hält sich nach außen zurück, bringt Vertraulichkeiten nach außen renâcle à défendre l'équipe à l'extérieur, révèle à l'extérieur des informations confidentielles sur l'équipe

GEA – NZ

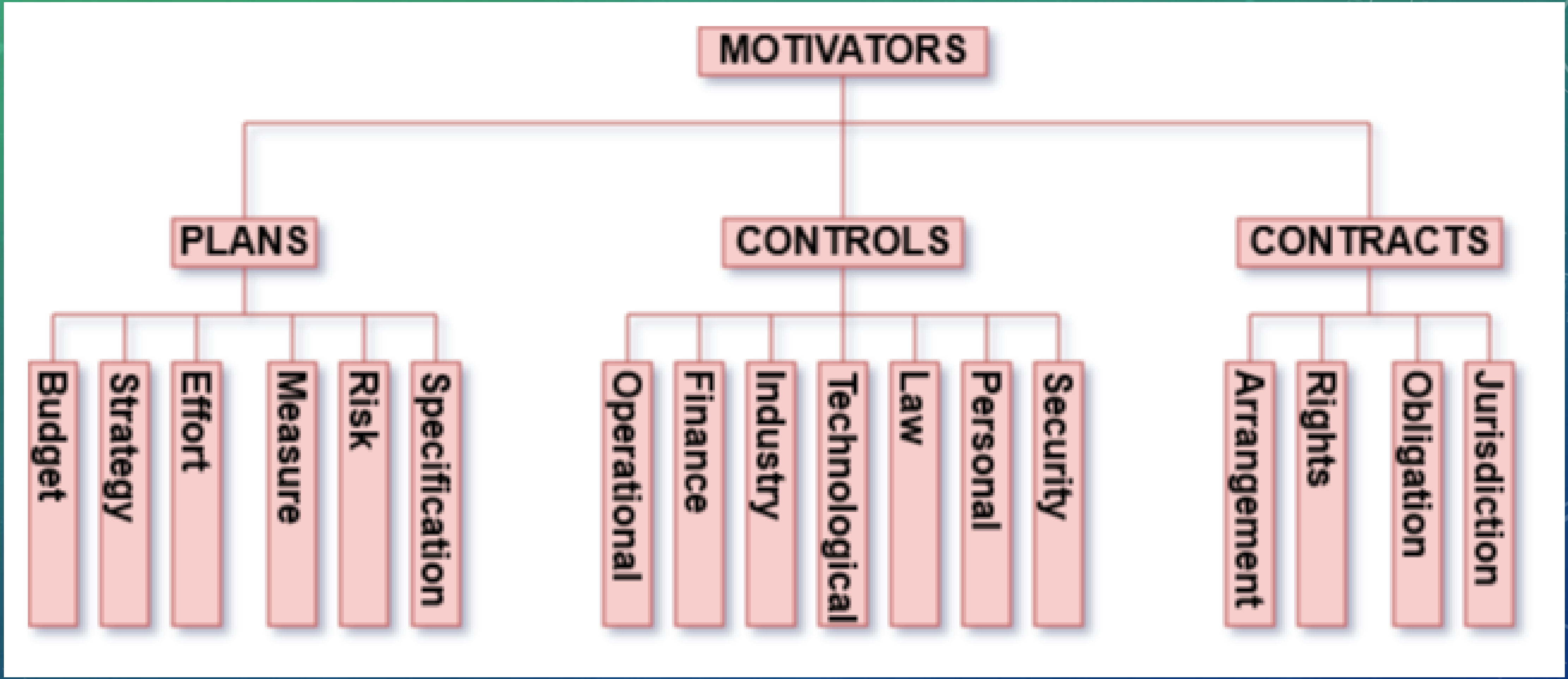

Motivators
Plans
Controls
Contracts
Parties
Places
Items
Cases
Events
Services
Entities
Activities



- ACTIVITIES
  - CASES
    - Compliance
    - Proceeding
    - Episode
    - Commission of Inquiry
    - Claim
    - Request
    - Order
  - EVENTS
    - Personal
    - Crisis
    - Social
    - Business
    - Trade
    - Travel
    - Environmental
    - Uncontrolled
    - Interaction
      - Channel
      - Medium
      - Interaction Type
  - SERVICES
    - New Zealand Society
    - Individuals & Communities
    - Services to Business
    - Civic Infrastructure
    - Government Administration
    - Services from Business

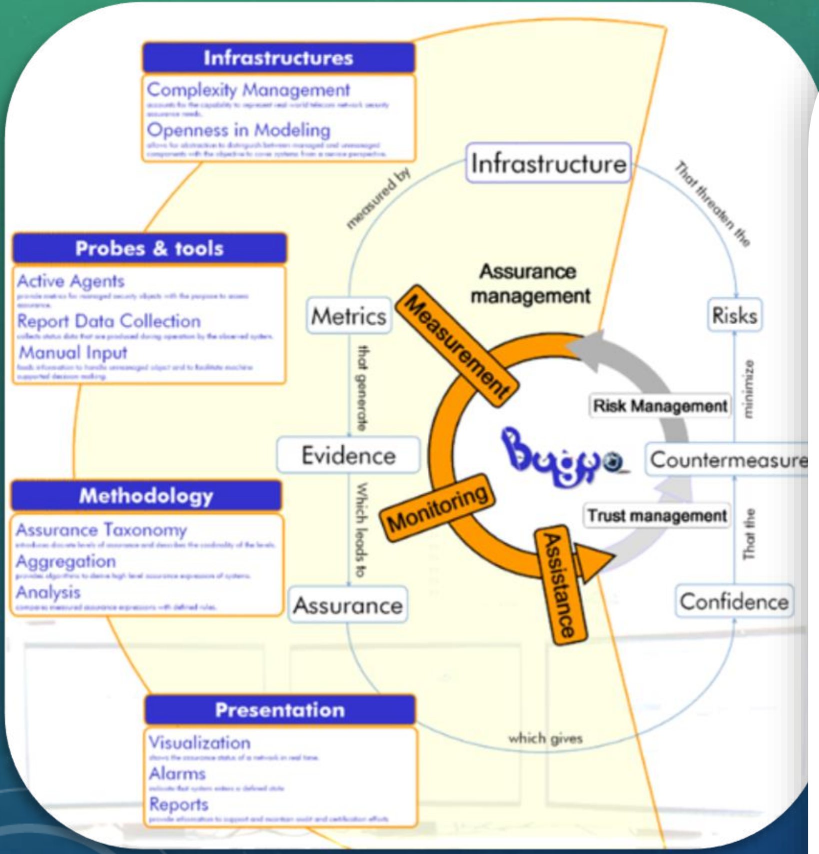


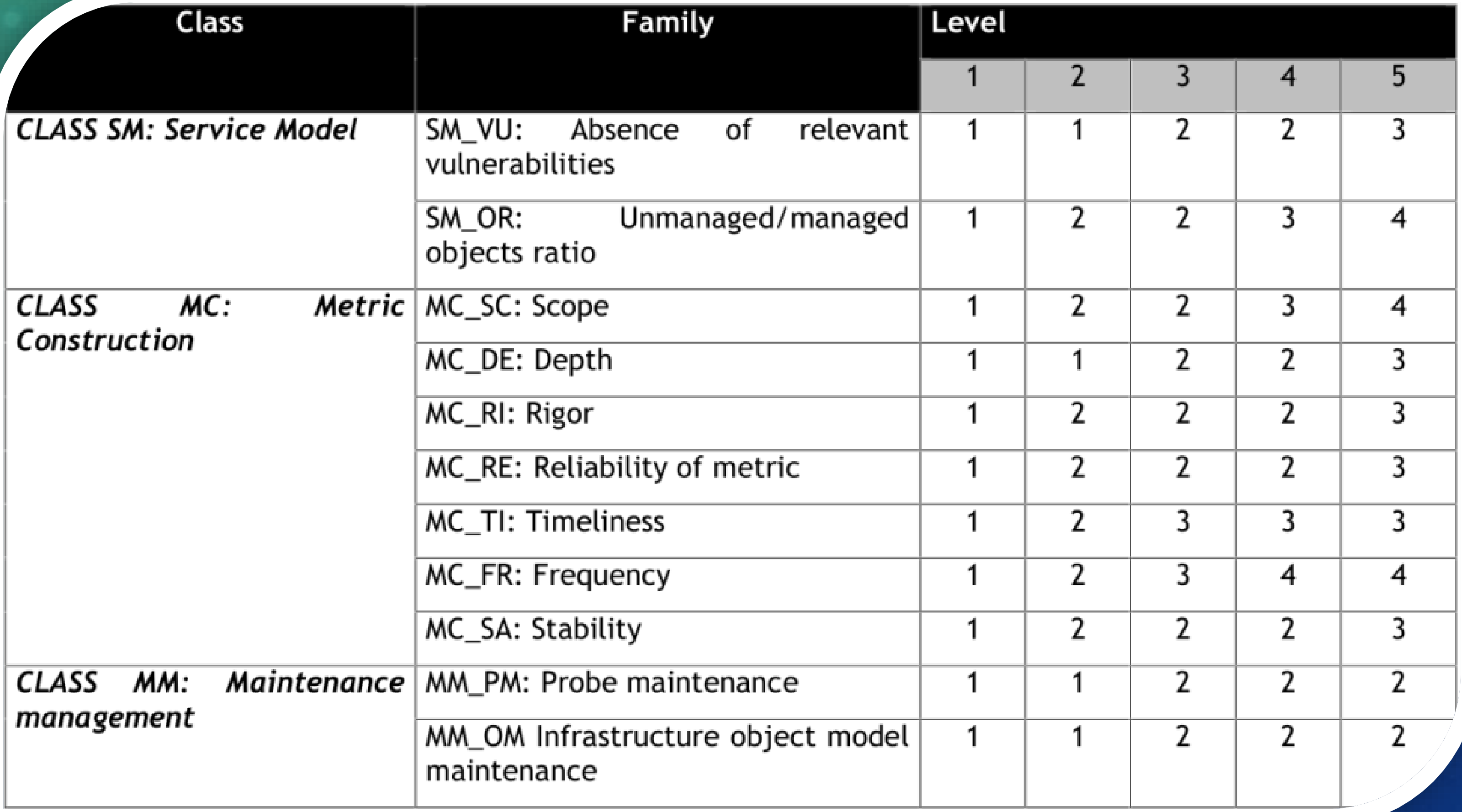
- ENTITIES
  - PARTIES
    - Party
    - Qualification
    - Role
    - Party Relationship
  - PLACES
    - Address
    - Location Type
    - Address Type
    - Purpose of Location
  - ITEMS
    - Application & ICT Services
    - ICT Infrastructure
    - Natural
    - Financial
    - Goods
    - Regulatory
    - Urban Infrastructure
    - Accommodation
    - Dwelling Type
    - Artefact
    - Waste
    - Item Usage
    - Other Item



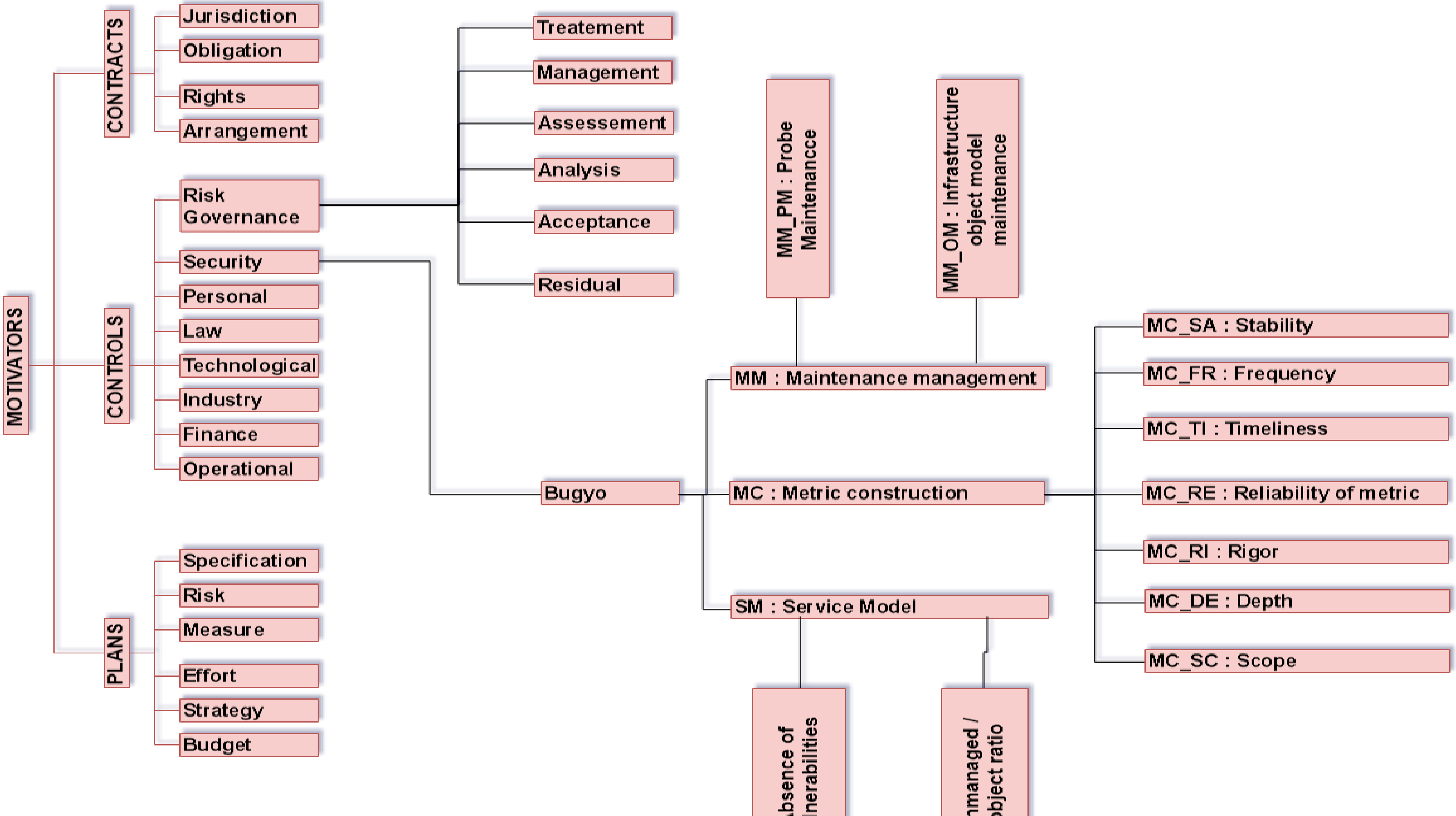
- MOTIVATORS
  - PLANS
    - Budget
    - Strategy
    - Effort
    - Measure
    - Risk
    - Specification
  - CONTROLS
    - Operational
    - Finance
    - Industry
    - Technological
    - Law
    - Personal
    - Security
  - CONTRACTS
    - Arrangement
    - Rights
    - Obligation
    - Jurisdiction

BUGYO





Class	Family	Level				
		1	2	3	4	5
CLASS SM: Service Model	SM_VU: Absence of relevant vulnerabilities	1	1	2	2	3
	SM_OR: Unmanaged/managed objects ratio	1	2	2	3	4
CLASS MC: Metric Construction	MC_SC: Scope	1	2	2	3	4
	MC_DE: Depth	1	1	2	2	3
	MC_RI: Rigor	1	2	2	2	3
	MC_RE: Reliability of metric	1	2	2	2	3
	MC_TI: Timeliness	1	2	3	3	3
	MC_FR: Frequency	1	2	3	4	4
	MC_SA: Stability	1	2	2	2	3
CLASS MM: Maintenance management	MM_PM: Probe maintenance	1	1	2	2	2
	MM_OM Infrastructure object model maintenance	1	1	2	2	2


MOTIVATORS
CONTRACTS
Jurisdiction
Obligation
Rights
Arrangement
CONTROLS
Risk Governance
Security
Personal
Law
Technological
Industry
Finance
Operational
PLANS
Specification
Risk
Measure
Effort
Strategy
Budget
Treatement
Management
Assessement
Analysis
Acceptance
Residual
Bugyo
MM_PM : Probe Maintenancce
MM_OM : Infrastructure object model maintenance
MM : Maintenance management
MC : Metric construction
SM : Service Model
MC_SA : Stability
MC_FR : Frequency
MC_TI : Timeliness
MC_RE : Reliability of metric
MC_RI : Rigor
MC_DE : Depth
MC_SC : Scope
Absence of
lnerabilities
nmanaged /
bject ratio

MISP-JSON

Namespace : predicate = ``value”

- Fichier Json pour Misp
  - **taxonomy_activities**
  - **taxonomy_entities**
  - **taxonomy_motivators**

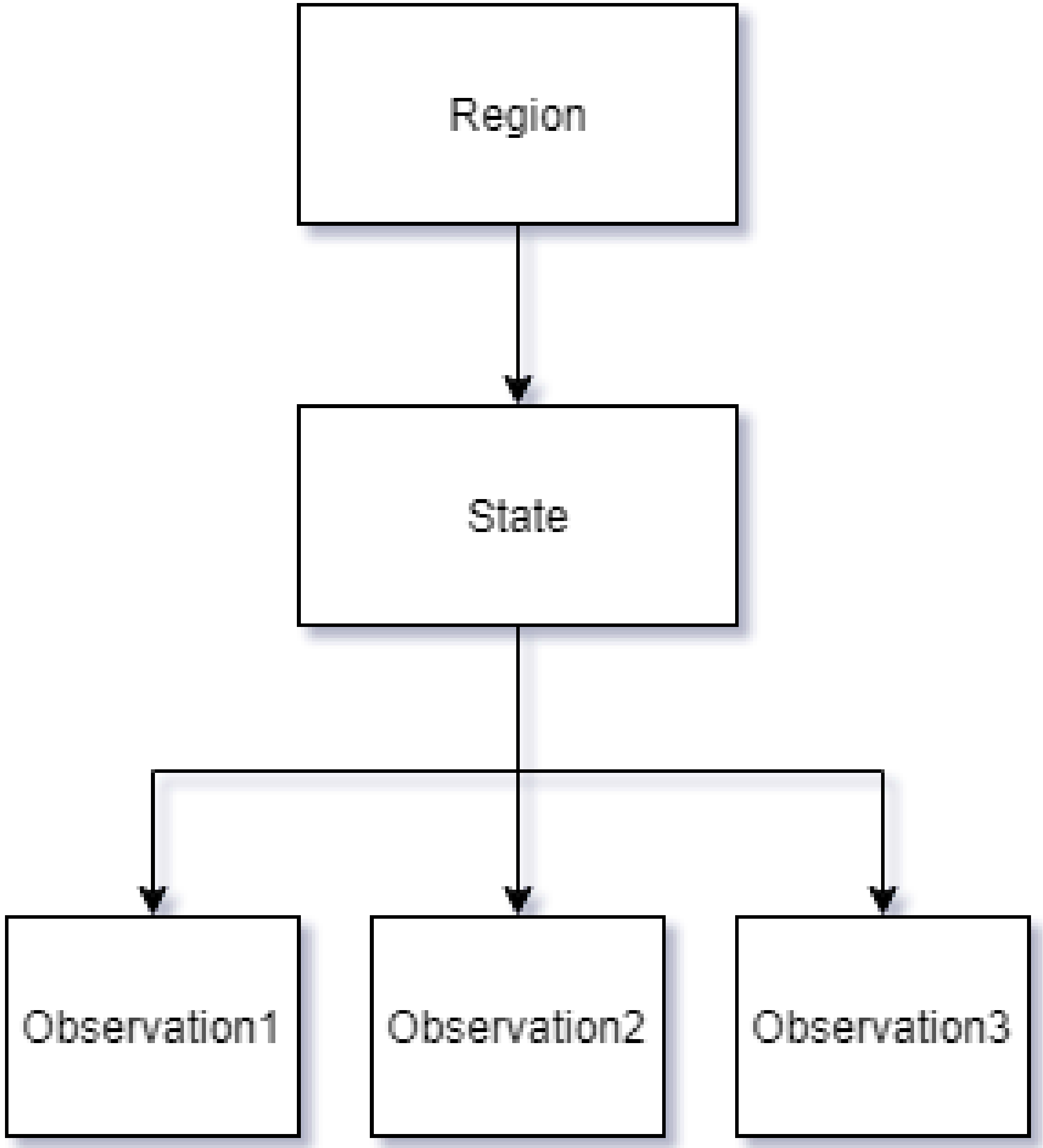
```
{  namespace": "Title
of your Taxonomy",
  "description":
"Taxonomy to classify
the information of ...
.",
  "refs": [
    "url ... "
  ],
  "version": 1,
  "predicates": [
    {
      "value":  "Name1
",
      "expanded":
"Expanded Name 1
",
      "description":
"TDesciption of the
name 1"
    },
    {
      "value":  "Name2
",
      "expanded":
"Expanded Name 2
",
      "description":
"TDesciption of the
name 2"
    }
  ],


  "values": [
    {
      "predicate":
"Name1",
      "entry": [
        {
          "value":        "
value1 ",
          "expanded":
"Def Value1"
        },
        {
          "value":
"value2",
          "expanded":
"Def Value2"
        }
      ]
    },
    {
      "predicate":
"Name2",
      "entry": [
        {
          "value":        "
value1 ",
          "expanded":
"Def Value1"
        },
        {
          "value":
"value2",
          "expanded":
"Def Value2"
        }
      ]
    }
  ]}
```

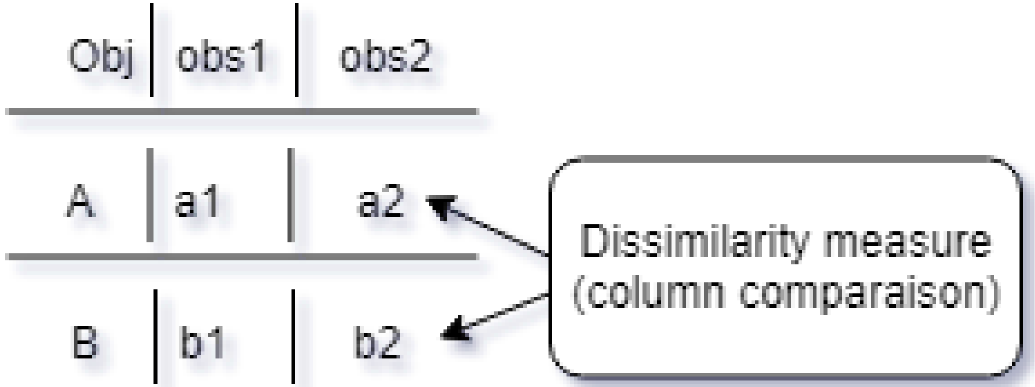
HIERARCHICAL ASCENDING CLASSIFICATION

- WHY Classify?
  - To classify all the instances created
  - To present wiser choices to the client
  - To create some directory for the instances created

- WHAT Classify ?
  - All object created thanks to the GEA-NZ and our structuring tables

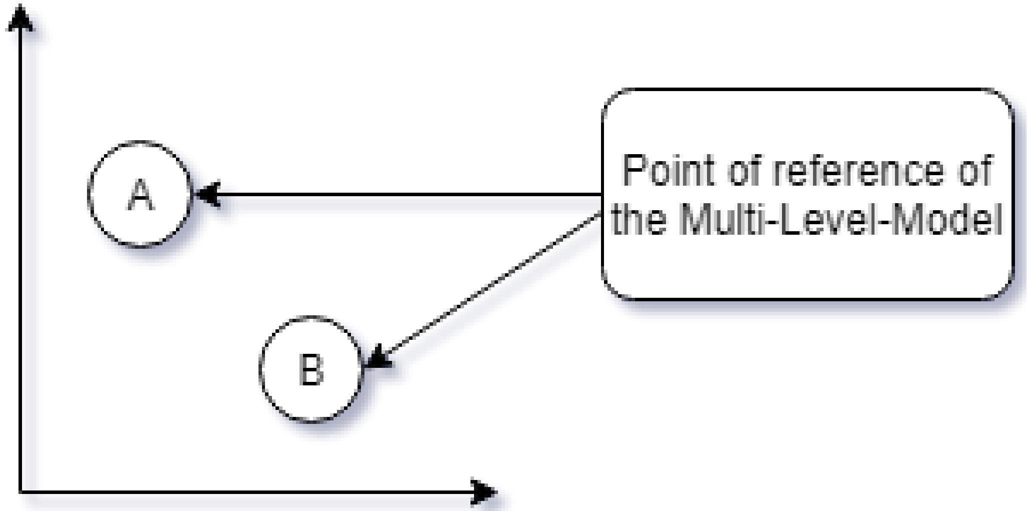
- HOW Classify ? Multi-Level-Model → K-MEANS → UPGMA



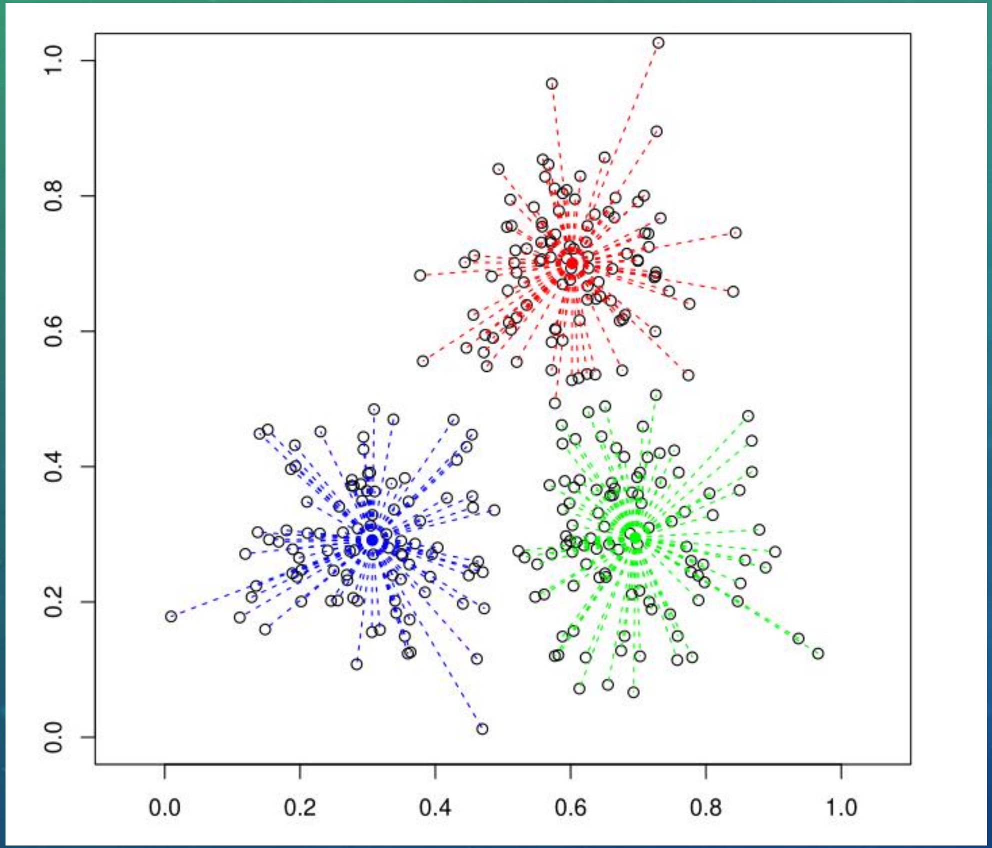


Obj	obs1	obs2
A	a1	a2
B	b1	b2

Analyse of slope & correlation between instances



K-MEANS
DETERMINE BARYCENTER

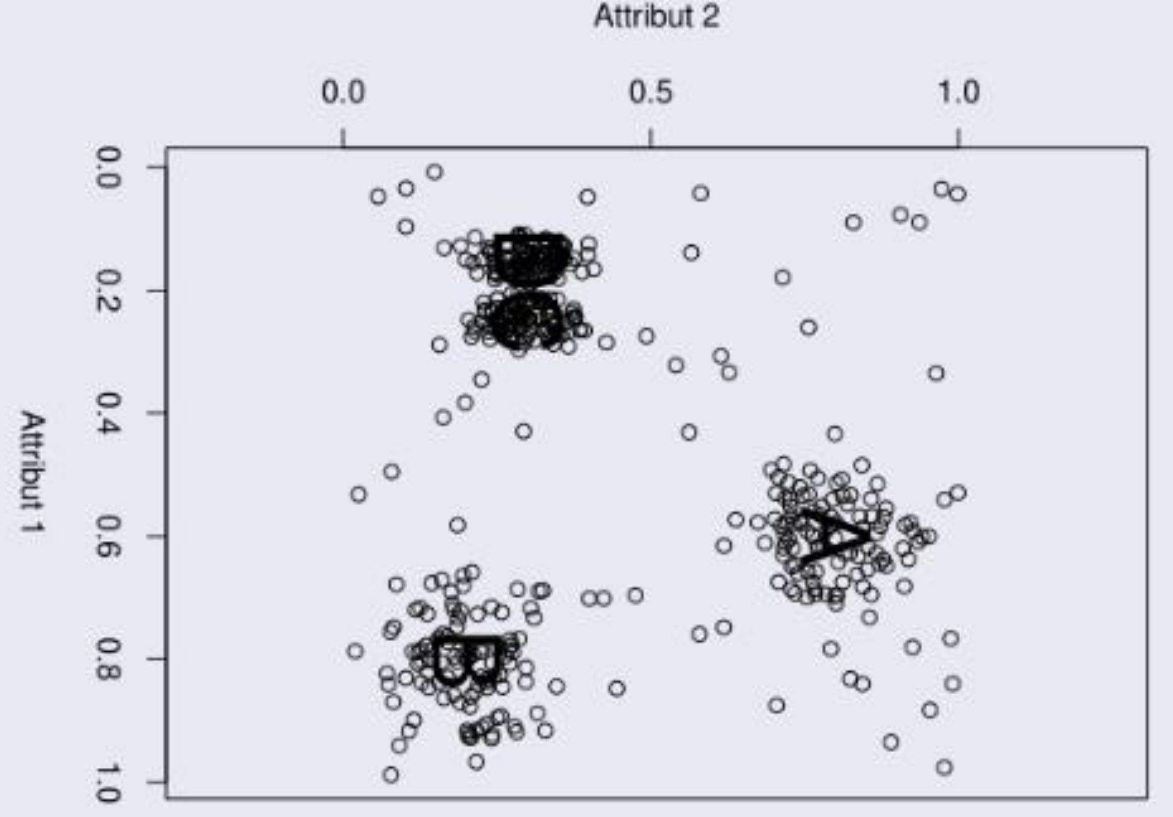


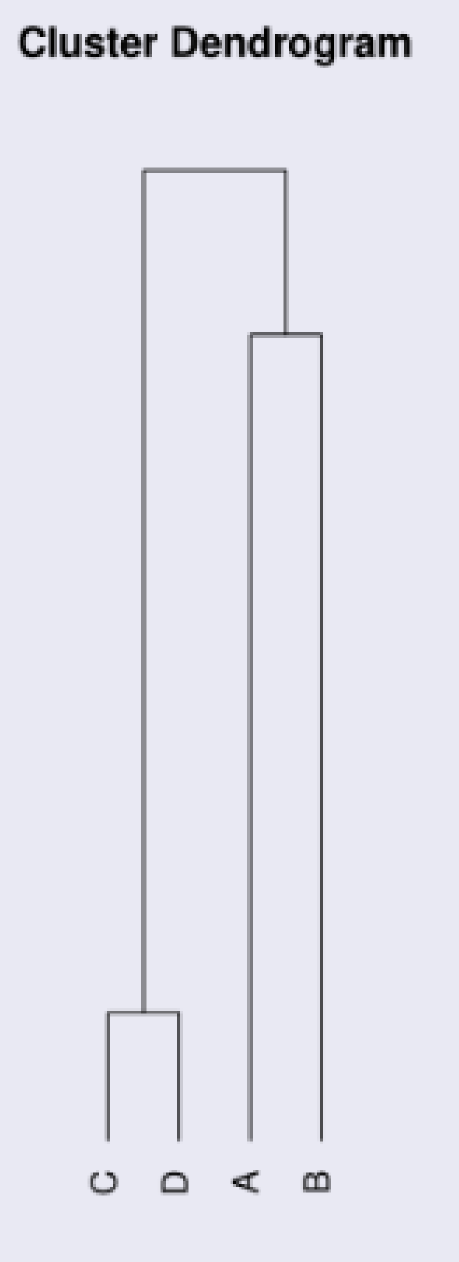
- Random initialization of centers
- As long as the result varies
  - For all objects
    - Calculate the distance to all centers
    - Assign the object to the class most close
  - For all classes
    - Calculate the center of gravity of the objects assigned
    - Assign the center of gravity as new center of the class

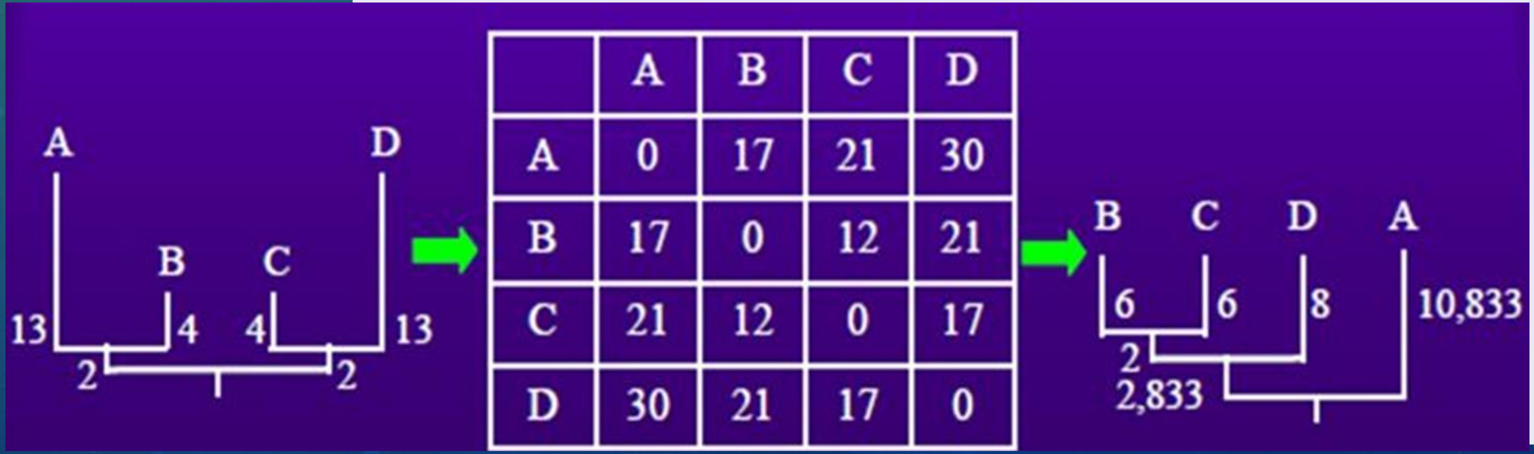
UPGMA

$$\frac{1}{|\mathcal{A}|\cdot|\mathcal{B}|}\sum_{x\in\mathcal{A}}\sum_{y\in\mathcal{B}} d(x,y)$$

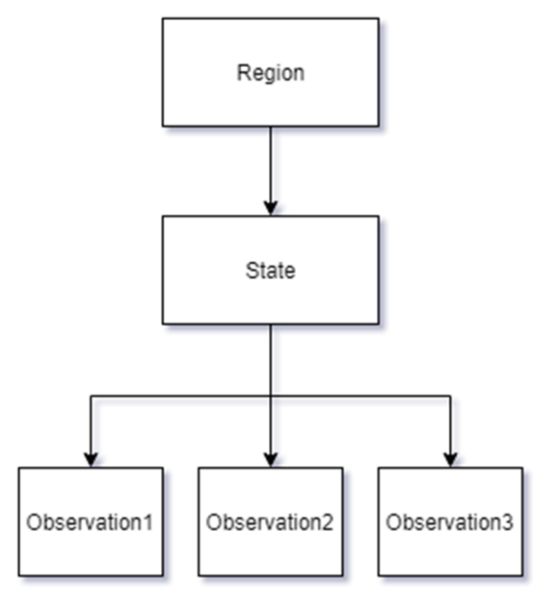
$$d_{(\mathcal{A}\cup\mathcal{B}),X} = \frac{|\mathcal{A}|\cdot d_{\mathcal{A},X} + |\mathcal{B}|\cdot d_{\mathcal{B},X}}{|\mathcal{A}|+|\mathcal{B}|}$$







	A	B	C	D
A	0	17	21	30
B	17	0	12	21
C	21	12	0	17
D	30	21	17	0



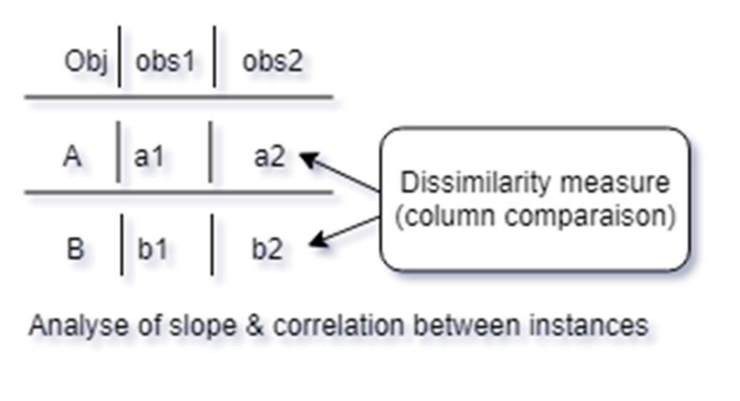
Region

State

Observation1

Observation2

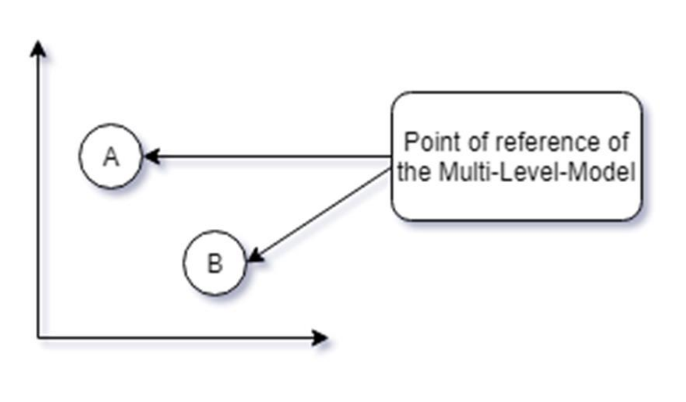
Observation3



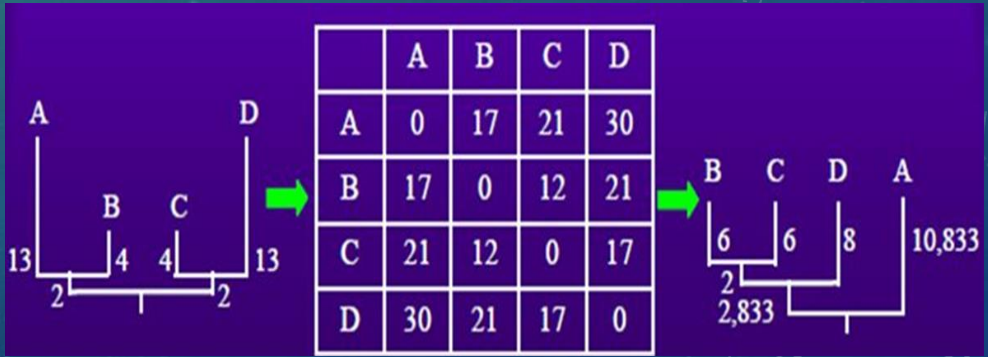
Obj	obs1	obs2
A	a1	a2
B	b1	b2

Dissimilarity measure (column comparaison)

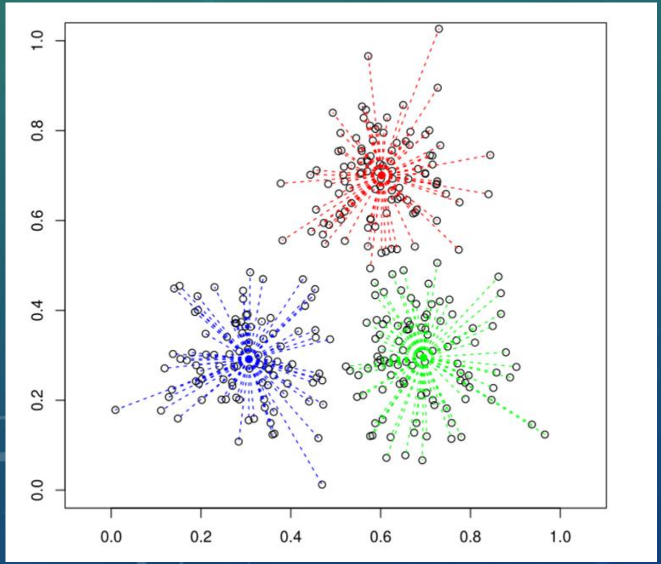
Analyse of slope & correlation between instances

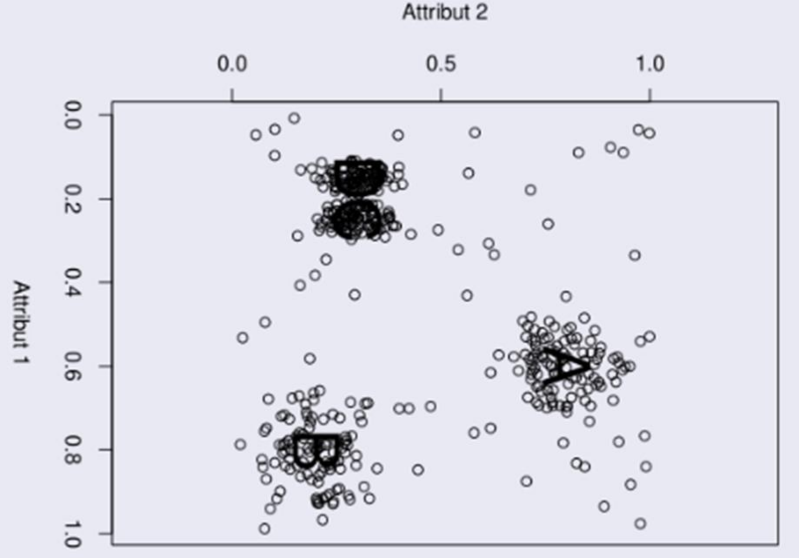


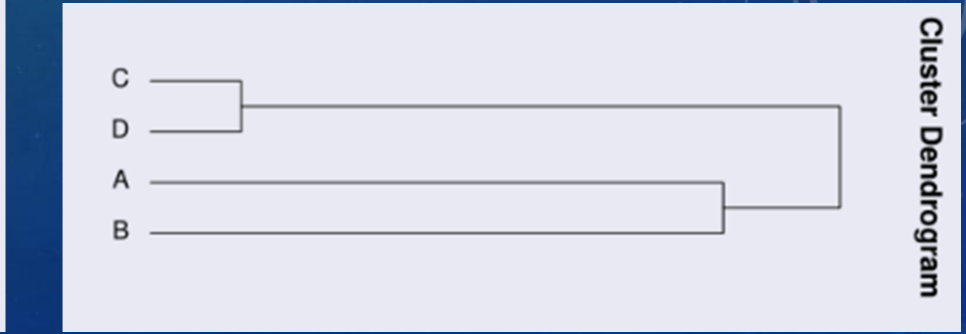
Point of reference of the Multi-Level-Model

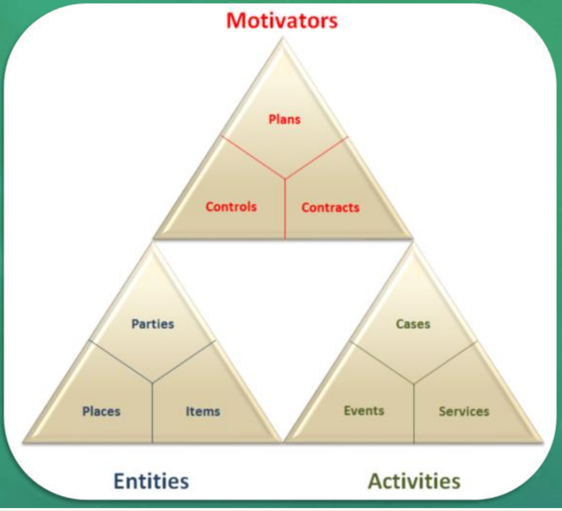


	A	B	C	D
A	0	17	21	30
B	17	0	12	21
C	21	12	0	17
D	30	21	17	0









EXAMPLE : PIZZA DELIVERY MAN

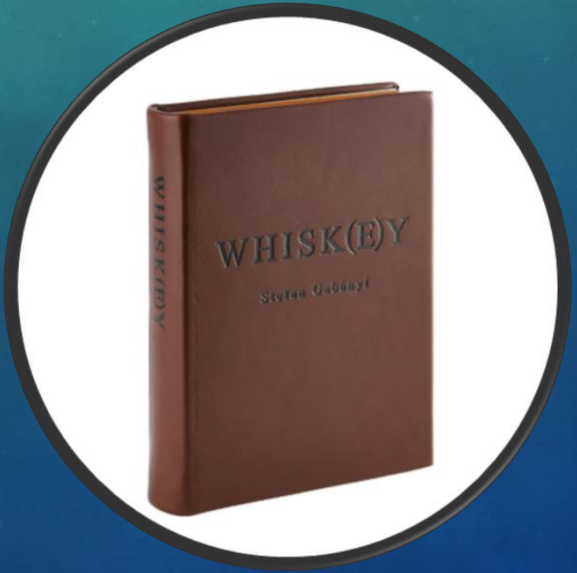
Motivator			Entities							Activities		
Plans Strategy	Control Arrangement	Contracts Arrangement	Parties Qualification	Parties Party	Parties Role	Parties Party Relation ship	Places Purpose of location	Places Address Type	Items Goods	Case	Events Trade	Services Service from business
Directive	Capability	Employement	Occupation	Individual	Commerce	Member ship	Delivery	Rural Delivery Address	Food	Order	Selling	Providing Food, Drink And Accomodation

The yellow : represent the main boxes of GEA-NZ
The blue : Represent the name of the column
The white : Represent the Pizza-Delivery-Man

Example of table template for a job

SOURCE – ANNEXE

http://slideplayer.fr/slide/1153793/3/images/68/Conclusions+sur+l%E2%80%99UPGMA.jpg



THANKS FOR WATCHING