UNIT – 15 – „Global Risks“

- **ISP/TSM „own / inherent“ potential cyber resilience capabilities --- 0 ---**

➢ **General Points:** → **it is not a single task to deal with if you want to improve your** “**Cyber Resilience**” capabilities **.**

Besides other aspects it includes “management- / staff awareness”, some kind of strategy, an involvement of all technical SW& HW & organisational levels → *& some kind of “nondogmatic common sense” can / will / should also help*)

→ **so in other words a holistic company approach is needed**.

The following four foils will show as an overview some specific potential ISP /TSM capabilities / possibilities

UNIT – 15 – „Global Risks“

ISP/TSM „own / inherent“ potential cyber resilience capabilities --- 1 ---

Specific ISP/TSM possibilities

- Make use of **enhanced password / lock rules** (available since 8.1.16) .
- Think about using **command approval** feature for restricted administrative commands.
- Use ISP/TSM **DRM** (**Disaster Recovery Management**) feature in combination with “Air Gap” tape robot (or similar - e.g. immutable storage) implementation.
- Establish **immediate E-Mail initiation** / **sending** based on potential **ACTLOG** Message(s).

UNIT – 15 – „Global Risks“

ISP/TSM „own / inherent“ potential cyber resilience capabilities --- 2 ---

Specific ISP/TSM possibilities …

- **Organize backup data & according storage pools for potential fast restores** (& document & test) -- Think about using the **3.2.1 rule** (**three** data copies / **two** different media / **one** copy offsite) for critical data.
- Envisage **different backup techniques** for faster restores.
- If **CVEs** (**Common Vulnerability Exposures**) are addressed in new ISP/TSM versions, **plan for upgrades in a “timely manner**”.
- If **external consultants** are involved, document their ISP / TSM activities with specific **OC** (**Operation Center**) reports.

UNIT – 15 – „Global Risks“

❑ ISP/TSM „own / inherent“ potential cyber resilience capabilities --- 3 ---

➢ Specific ISP/TSM possibilities …

- Use **MFA** (**Multi Factor Authentication**) for interactive ISP/TSM Server sessions.
  - ✓ **Create & exchange “Secret Keys”** and use security app capable of providing an **TOTP** (**Time-based One-Time Passcode / Password**)

- If feasible, use **Data Replication** to <u>one</u> or <u>two other</u> ISP/TSM servers.

UNIT – 15 – „Global Risks“

- **ISP/TSM „own / inherent“ potential cyber resilience capabilities --- 4 ---**

  - **Specific ISP/TSM possibilities …**

    - **Potential encryption possibilities** of “**data at rest**” / “**data in use**” & “**data in transit**” for:

      - ✓ **local Directory Container Storage Pools.**
      - ✓ **DATA transfer** between ISP /TSM servers.
      - ✓ **DATA transfer** between an ISP / TSM server and a BA client.
      - ✓ the **Db2 database.**
      - ✓ BA **client side.**

    - **And more……**