**Measuring Cyber Maturity with the 100 Point Cyber Check**

The 100 Point Cyber Check is a comprehensive cybersecurity assessment tool designed to evaluate an organisation's security posture across key domains. It consists of 100 individual checkpoints, each representing a critical aspect of cybersecurity, including governance, risk management, data protection, and incident response. The assessment aims to identify strengths and weaknesses in the organisation's security framework, providing a detailed view of where improvements are needed. The ideal maturity state of 80% overall (or 20/25 in each section) in the 100 Point Cyber Check can be theoretically justified using three theoretical concepts – the **Pareto Principle,** the **Law of** **Diminishing Returns**, and the **Balanced Approach**:

1. **Pareto Principle (aka 80/20 Rule)**:
   * The Pareto Principle suggests that roughly 80% of effects come from 20% of causes. In the context of cybersecurity maturity, achieving 80% of the total possible maturity (80/100) may represent reaching a level where the organisation has addressed the most critical and impactful 20% of cybersecurity controls and practices. This ensures that the most significant risks are mitigated and the organisation has a robust cybersecurity posture. Beyond this point, further investments in maturity might result in marginal improvements but with significantly increasing costs, time, and effort.
2. **Law of Diminishing Returns**:
   * As an organisation progresses in its cybersecurity maturity, the effort and resources required to achieve additional improvements typically increase, while the incremental benefits tend to decrease. Thus, achieving a maturity level of 80/100 could be seen as reaching the point where the balance between cost, effort, and benefit is optimised. Going beyond this level may result in a higher cost with less proportional benefit, aligning with the economic concept of diminishing returns.
3. **Balanced Approach**:
   * The choice of 80/100 or 20/25 in each section indicates that the organisation is not only addressing the most critical areas but is also maintaining a balanced approach across different domains of cybersecurity. This prevents an overemphasis on one area at the expense of others, ensuring a comprehensive and holistic cybersecurity strategy.

**Proposed Maturity Levels and Rubric with Qualitative Descriptors**

To provide a more granular assessment of cybersecurity maturity, the following maturity levels and a corresponding rubric with qualitative descriptors are proposed:

**1. Maturity Levels**

* **0-20 (Initial/Ad-Hoc)**
* **21-40 (Managed)**
* **41-60 (Defined)**
* **61-80 (Optimising)**
* **81-100 (Exemplary)**

**2. Rubric with Qualitative Descriptors**

1. **0-20: Initial/Ad-Hoc**
   * **Description**: At this level, cybersecurity practices are largely reactive and uncoordinated. There may be some basic controls in place, but they are implemented in an inconsistent and ad-hoc manner. The organisation lacks formal policies and procedures, and there is little to no strategic direction for cybersecurity. This stage represents significant vulnerabilities and a high level of risk exposure.
   * **Key Characteristics**:
     + No formal cybersecurity framework.
     + Inconsistent or no documentation of policies.
     + Cybersecurity incidents are managed on an as-needed basis with minimal planning.
     + Significant gaps in risk management and control implementation.
2. **21-40: Managed**
   * **Description**: The organisation has begun to recognise the importance of cybersecurity and has implemented some key controls. There are formal policies and procedures in place, but they may not be fully comprehensive or consistently applied. Cybersecurity efforts are more structured, and some degree of risk management is evident, though gaps still exist.
   * **Key Characteristics**:
     + Basic policies and procedures established.
     + Some level of staff awareness and training.
     + Incident response processes are in place but may be underdeveloped.
     + Initial steps toward risk assessment and management.
3. **41-60: Defined**
   * **Description**: Cybersecurity practices are well-defined and documented, with a clear framework guiding the organisation’s efforts. Controls are implemented more consistently, and the organisation is proactive in identifying and addressing cybersecurity risks. There is a moderate level of integration across various departments, and regular training and awareness programs are in place.
   * **Key Characteristics**:
     + Formal cybersecurity framework in place and actively managed.
     + Regularly updated policies and procedures.
     + Proactive risk management and incident response.
     + Cross-departmental collaboration in cybersecurity efforts.
4. **61-80: Optimising**
   * **Description**: The organisation has a mature cybersecurity program with optimising processes and controls. Cybersecurity is embedded in the organisation's culture, and there is a high level of awareness among all employees. Continuous improvement processes are in place, and the organisation actively seeks to stay ahead of emerging threats. There is a strong emphasis on automation and efficiency in managing cybersecurity tasks.
   * **Key Characteristics**:
     + Cybersecurity is a strategic priority.
     + High levels of automation in monitoring and response.
     + Continuous improvement and regular review of controls.
     + Strong alignment of cybersecurity with business objectives.
5. **81-100: Exemplary**
   * **Description**: Cybersecurity practices are exemplary, serving as a benchmark for others in the industry. The organisation is highly resilient to cyber threats, with advanced controls and processes that are continuously refined. There is a strong emphasis on innovation and leadership in cybersecurity, with the organisation often participating in industry-wide initiatives and sharing best practices.
   * **Key Characteristics**:
     + Leadership in cybersecurity innovation and practices.
     + Advanced and highly automated cybersecurity solutions.
     + Regular contributions to industry standards and best practices.
     + High level of agility in responding to new and emerging threats.

**Summary**

By establishing these maturity levels and descriptors, organisations can better understand their current cybersecurity posture, identify areas for improvement, and set realistic goals for enhancing their cybersecurity maturity. The 80/100 maturity state represents a well-rounded and optimised approach, balancing the need for strong cybersecurity controls with the resources required to implement them effectively.