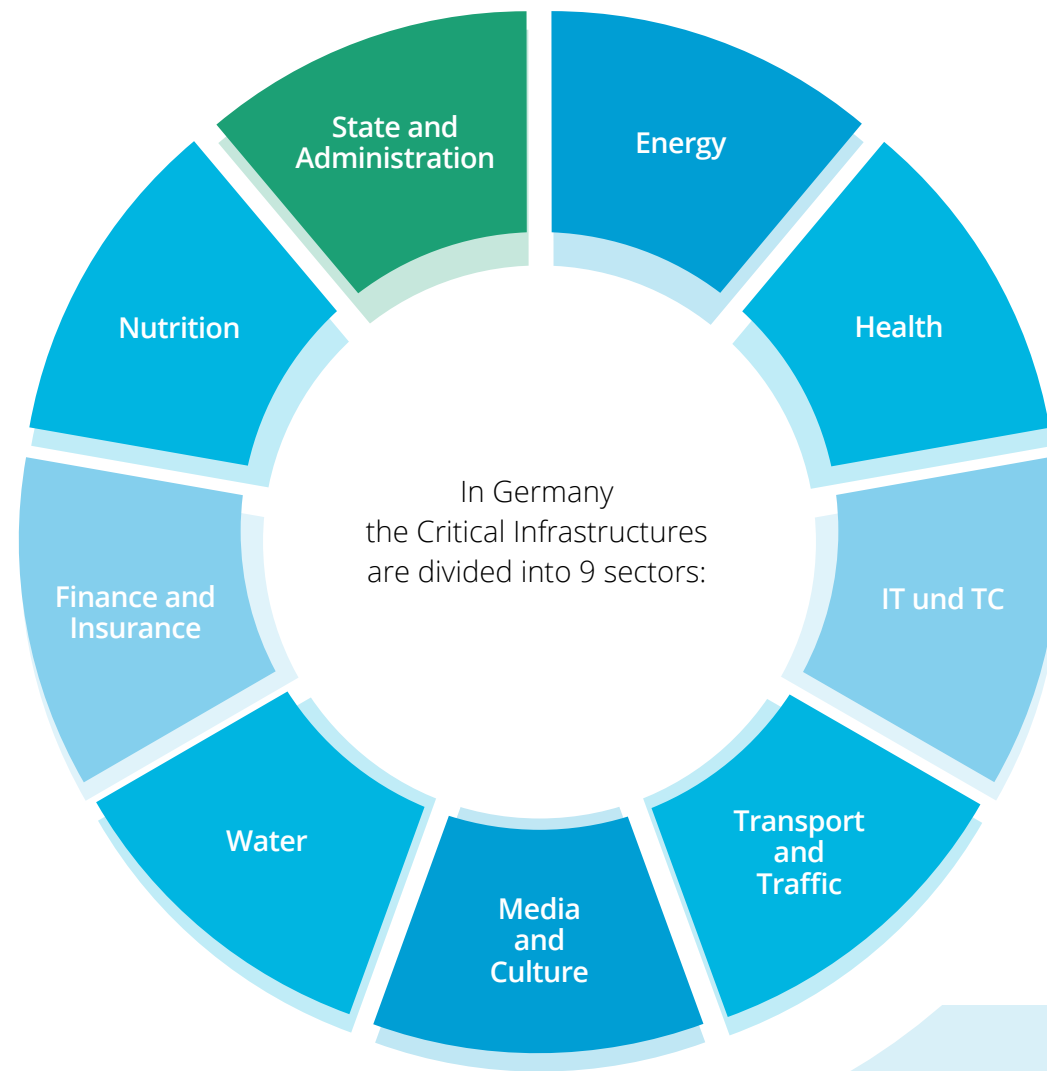## CRITIS

The German government defines critical infrastructures as follows: Critical infrastructures (CRITIS) are organizations or facilities of vital importance to the governmental community, the failure or impairment of which would result in sustained supply shortages, significant disruptions to public safety, or other dramatic consequences.

(Quelle: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html)

PDV CRITIS Services are specially developed for companies and institutions that operate critical infrastructures (CRITIS) and thus have to meet special regulatory requirements for IT security.

PDVSYSTEME

In Germany
the Critical Infrastructures
are divided into 9 sectors:

- State and Administration
- Energy
- Health
- IT und TC
- Transport and Traffic
- Media and Culture
- Water
- Finance and Insurance
- Nutrition

For the protection of KRITIS owners/operators are primarily operators are responsible.

IT Security Act

Since the passing of the IT Security Act in July 2015, operators of critical infrastructures have been obliged to provide appropriate state-of-the-art IT security for the provision of their critical services.

The PDV KRITIS Services combine various IT infrastructure services from PDV-Systeme and manufacturers and enable you to meet the KRITIS requirements for your basic IT infrastructure.

PDVSYSTEME

" IT Services for
Critical
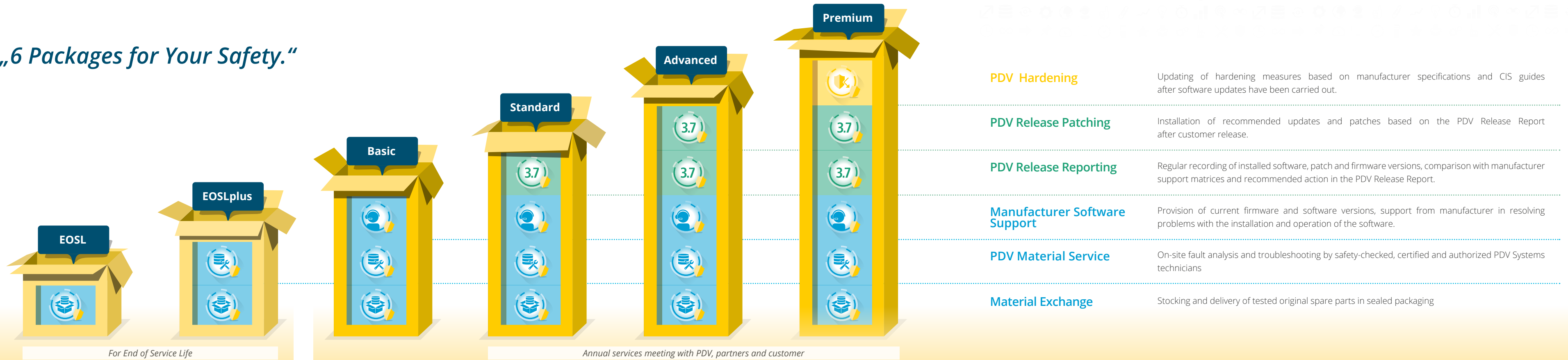Infrastructures "

PDV CRITIS SERVICES

CRITIS Services

Respond quickly. Reduce downtime and reduce costs.

There is no serious guarantee for absolutely trouble-free operation of your IT. But you can take measures that will noticeably reduce the times for troubleshooting, especially in a CRITIS environment.

Our CRITIS services are characterized by the fact that they are provided by us within the framework of an ISO27001-certified ISMS - from call handling to the successful elimination of a fault.

Security features of CRITIS Services

- ISMS/CRITIS compliance
- ISO27001 certified operations
- ISO 9001 certified quality management
- Manufacturer original spare parts
- Security verified employees
- Single Point of Contact (SPOC):
  - In Germany (security-checked personnel - at least Classified - For official use only)
  - With knowledge of your IT infrastructure
  - German speaking support by PDV-Services
- Shipping of spare parts in sealed shipping cartons
- Individually designed delivery notes upon request
- On-site stocking of spare parts possible *(optional)*

„6 Packages for Your Safety."

EOSL · **EOSLplus** · **Basic** · **Standard** · **Advanced** · **Premium**

For End of Service Life | *Annual services meeting with PDV, partners and customer*

Service	Description
PDV Hardening	Updating of hardening measures based on manufacturer specifications and CIS guides after software updates have been carried out.
PDV Release Patching	Installation of recommended updates and patches based on the PDV Release Report after customer release.
PDV Release Reporting	Regular recording of installed software, patch and firmware versions, comparison with manufacturer support matrices and recommended action in the PDV Release Report.
Manufacturer Software Support	Provision of current firmware and software versions, support from manufacturer in resolving problems with the installation and operation of the software.
PDV Material Service	On-site fault analysis and troubleshooting by safety-checked, certified and authorized PDV Systems technicians
Material Exchange	Stocking and delivery of tested original spare parts in sealed packaging

1. Dedicated contact persons with knowledge of the overall infrastructure
2. Support for products that are no longer supported by the manufacturer
3. Multivendor support, for various manufacturers e.g. HPE, VMware, Microsoft, Veeam, Cisco
4. Repair by safety-checked, certified and authorized PDV systems technicians
5. Continuation of work until complete system recovery, even if the contractually agreed service time is exceeded
6. Software service and support by manufacture
7. Provision of current software/firmware versions by manufacture (for multi-vendor support)
8. Access to manufacturer Knowledge Base (for multi-vendor support)
9. Checking the installed software, patch and firmware versions for conformity with support matrices and manufacturer recommendations (release report)
10. Installation of recommended updates, after customer approval and based on the release report
11. System hardening by removing unused functions and software components