FLYER

VALUEMATION
IT SERVICE CONTINUITY MANAGER

With IT Service Continuity Management (ITSCM), risks that might have serious impacts on the availability of business and IT services are controlled in the IT infrastructure. It specifically involves planning pinpointed measures to minimize risks and recover services after an unforeseeable, abnormal event. As an IT service provider, you thereby ensure that you can fulfill the minimum requirements under existing service level agreements (SLAs) even after a disaster (exceptional major incident). ITSCM is closely intermeshed with Business Continuity Management and ensures that business activity is impaired as little as possible.
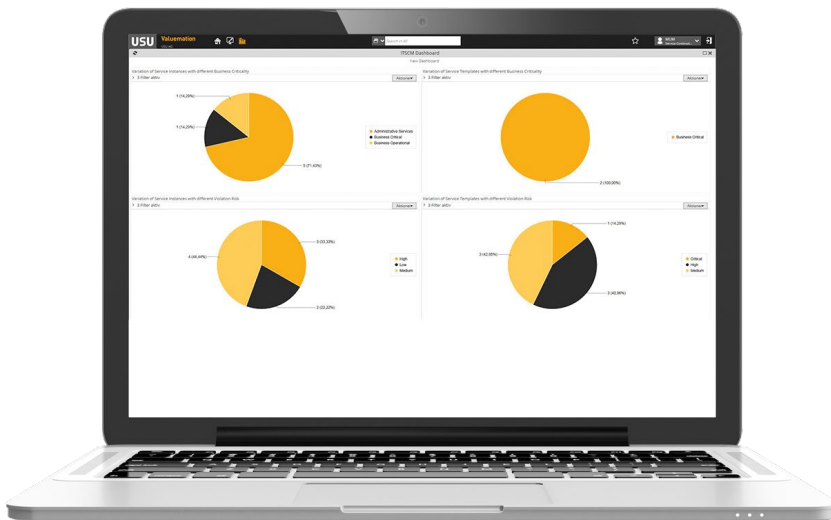
BENEFITS

Valuemation enables you to

Control risks in service operations by means of standardized classification and regular review of elementary threats

Know the potential effects of incidents on business services thanks to a high degree of transparency on dependencies in the service infrastructure

Avoid losing valuable time, since you have access to all relevant data and can initiate documented, largely automated processes

Ensure fulfillment of critical SLAs by means of preplanned and prioritized recovery measures

Prevent economic loss by avoiding or minimizing service outages

Ensure service availability by minimizing risks in IT operation

Objectives

—— The Valuemation IT Service Continuity Manager helps you classify and regularly review potential risks and how business-critical they are. ITSCM managers can use it to define and plan processes and tasks that have to be accomplished after a major incident/emergency change on the basis of their potential business impact and in accordance with existing SLAs. In that way, you ensure that important services are available again as soon as possible after a disaster and avoid economic loss.

Classify Risks on the Basis of Elementary Threats

—— You can use the Valuemation IT Service Continuity Manager (ITSM) to determine the potential threat to service availability from external factors. The "Elementary Threats" catalog of the German Federal Office for Information Security (BSI) is already integrated as the basis for that. It comprises potential causes of incidents, such as damage by fire and water, natural disasters, espionage, theft, failure of systems or the power supply, etc. On the basis of these standardized criteria, you classify the likelihood of threats and their potential effects on defined services and the underlying configuration items (CIs).

Define and Monitor Business-critical Services

—— With help of the service structures from the CMDB the connection between the IT services/CIs at risk and the related business services can be established and visualized. You assign the IT services and CIs on the basis of their business criticality to one of the four categories: mission critical, business critical, business operational or administrative services. The likelihood and impact of an interruption can likewise be classified in four categories (high, medium, low, very low). The above criticality classification supplies a service level violation risk, which is monitored in a pinpointed manner (e.g. using the optional Valuemation Service Monitoring Manager). You can use a business impact analysis to calculate the damage as a result of services not being available, as well as simulate and graphically visualize possible effects.

Plan and Control Service Recovery

—— The Valuemation IT Service Continuity Manager enables you to take immediate action in response to a disruption. Thanks to defined backup/disaster recovery procedures with a detailed description of service recovery and prioritization of it, you can instigate the necessary measures right away in the event of a disaster. With the service type "Business Continuity," you use predefined service parameters, SLAs and various recovery options. The process steps required for service recovery are defined, executed and documented in an audit-compliant manner by means of the integrated process engine (VM Business Process Manager). To enable that, there are predefined workflows that distribute activities with associated instructions on a time-controlled basis. The specified classifications on the threat potential to and business criticality of IT services and CIs must be reviewed regularly and, if necessary, adapted. Depending on the classified criticality, you can automatically initiate the review at defined intervals of time and task the person responsible for the service with it.