



*Manor Group*

# Event Management Best Practices

**Manor Group**



# Overview



- Event Management
- Incident Management and Problem Management
- Principles of Event Management Best Practices
  - Data Acquisition
  - Normalization
  - Enrichment
  - Correlation and Root Cause Analysis
  - Console Consolidation
  - Automation
  - Notification
  - Escalation
  - Reporting
- Benefits
- Customer Examples
- Software Solutions



# Event Management is part of Business Service Management



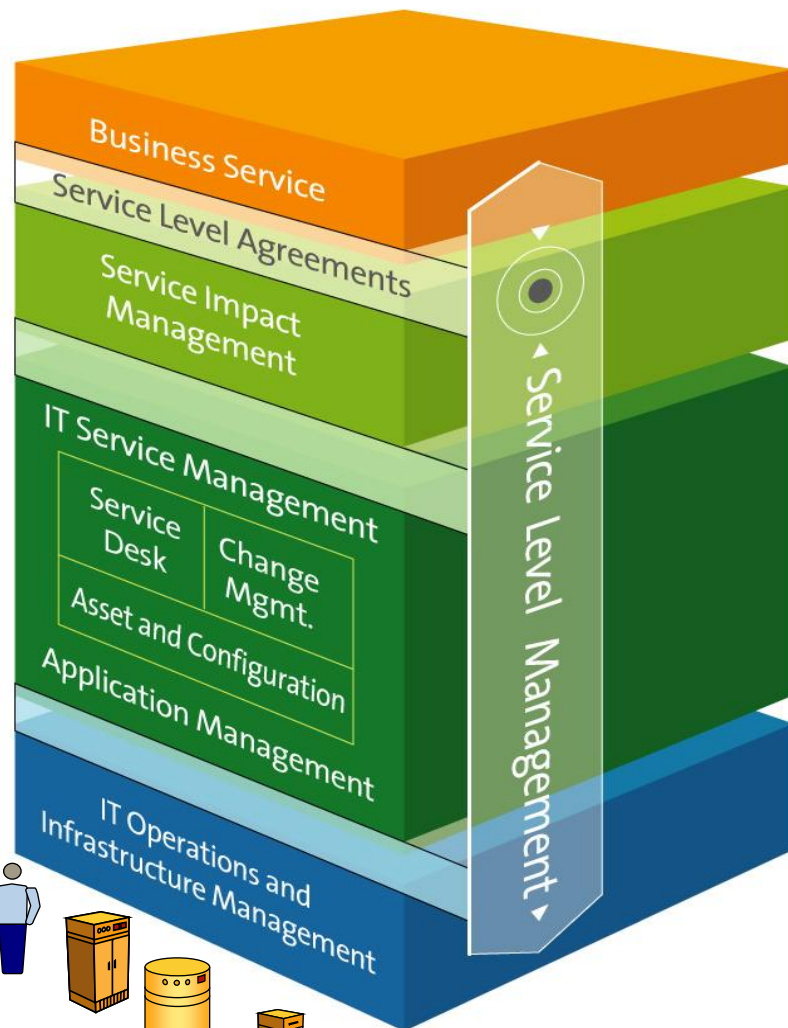
## Service Impact Management

- Deals with the relationships between Services and IT (dependency and impact)
  - Service model definition
  - Service impact
  - Service availability
  - Automate and visualize events
- Requires sophisticated Event Management



## Event Management

- Deals with receiving and manipulating the IT events
  - Collect and process events
  - Define and manipulate events
  - Perform notifications
- Requires well-developed Infrastructure and Application Management



# Incident Management and Problem Management



- Event Management is comprised of
  - Incident management
  - Problem management
- The primary objective of incident management is to restore service as soon as possible to minimize any negative effect on business services.
- The objective of problem management is to take a proactive approach in defining preventative measures so that service disruptions do not occur.



# Best Practices Principles



- Consistent process
- Event management tools that achieve
  - Data Acquisition
  - Normalization
  - Enrichment
  - Correlation and Root Cause Analysis
  - Consolidation
  - Automation
  - Notification
  - Escalation
  - Reporting



# Data Acquisition



**Data acquisition encompasses all the methods by which event management information is collected. These methods can be**

- > Push
- > Pull
- > Publish/Subscribe



# Normalization



**Normalization is the process of homogenizing event data into a common event format.**

- Specific values are always located in a specific field and called a specific name
- Regardless of the source of an event, a standard set of data is associated with all events
- Reporting is made consistent and efficient
- Event data has a common definition



# Enrichment



**Enrichment is the process of adding value to the original event data for the purpose of streamlining incident management and facilitating service management.**

- Provides details that supplement trouble tickets and repair actions
- Extends event data for correlation, automation, notification, and reporting functions
- Associates service data or other data, such as blackout periods, to an event that can be used in incident or problem management





# Correlation and Root Cause Analysis



**Correlation and root cause analysis are processes that determine the source of a problem, identify sympathetic events, and relate associated events.**

- Focuses repair action and speeds service restoration for incidents
- Streamlines the event data presented to operators by suppressing event clutter
- Targets problem management efforts



# Console Consolidation



**Consolidation is the process of delivering all events from across the enterprise to a single pane of glass.**

- Manage more with less
- Reduce complexity
- Leverage existing infrastructure management tools
- Gain a “bird’s eye” view
- Facilitate service management and problem management



# Automation



**Automation is the process of removing or reducing the need for human intervention in event management while promoting service resiliency.**

- Allows problems to be fixed at machine speed
- Supports escalation of events when repair criteria are exceeded
- Streamlines event management workload on staff
- Enforces policies and processes



# Notification



**Notification is the process of presenting incident information to the right person in the right form at the right time, and verifying their receipt of the information.**

- Speeds information about an incident to the trouble ticket system or repair expert
- Contacts a repair expert in a suitable manner
- Frees operators from another rote task
- Supports multiple forms of communication



# Escalation



**Escalation is the process of heightening the severity of or broadening the awareness about an incident if not being addressed in an appropriate and timely manner.**

- Prevents incidents from falling through the cracks
- Ensures attention to the most critical problems
- Elevates the status of an event if the problem persists



# Reporting



**Reporting is the process of disseminating information that reflects the measurement of service level agreements, historical usage, or the performance of service delivery components.**

- Summarizes event management details
- Measures problem resolution effectiveness
- Provides consistent service delivery data



# Best Practices Benefits



- Identifies affected services and prioritizes repair actions through enrichment and correlation
- Pinpoints the exact problem condition through acquisition and correlation
- Presents repair details through enrichment, such as
  - Physical device location or specific application/database
  - Responsible department/staff expert
  - Repair action to be taken
- Reduces incident management workload through automated repair action
- Delivers consistent service reporting through acquisition and normalization



# Best Practices Benefits



- Speeds notification to the right person at the right time in the right form through notification and escalation
- Reduces mean time to repair through escalation, notification and automation
- Reflects problem areas that can be addressed through problem management through reporting







*Manor Group*

# Contacts

**Manor Group**

[info@themanorgroup.net](mailto:info@themanorgroup.net)

[www.themanorgroup.net](http://www.themanorgroup.net)

