MONITORING (EVENT) MANAGEMENT

www.i-mokymas.com

info@i-mokymas.com

PROCESS GOALS AND OBJECTIVES

Goals

- Manage events lifecycle
- Serve as a base for operational monitoring and control
- Serve as a base for automating operational support

Objectives

- Define changes in CI status, which influence on IT service or CI control
- Establish activities for event control, and ensure that they are managed by a certain function.
- Define a trigger for an appropriate process/procedure.
- Deliver measuring tools for Design phase (SLA, OLA, etc.)
- Ensure basic (raw) data for reporting, quality management, and CSI

DEFINITIONS

Event

- Any change in a CI status or connection which influences a service

Types of monitoring

- Active monitoring
  - Monitoring tools send requests to controlled CIs
- Passive monitoring
  - CIs send information to monitoring themselves

PROCESS AREA

CI

- Control stability of status
- Automate detecting status change

Environment

- For example climate control or fire alert systems

Control licenses

Information security

Define “normal work”

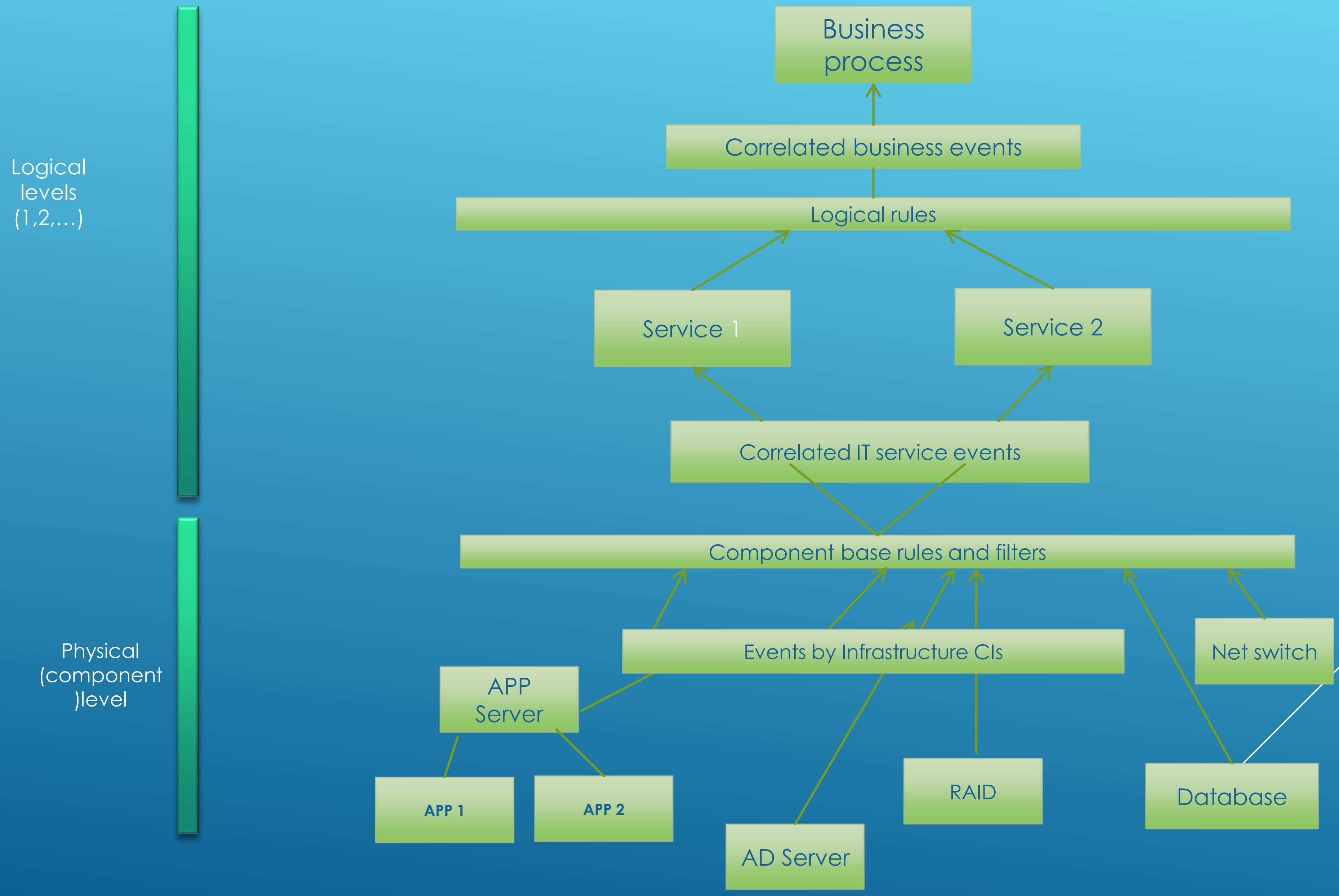
- Identify set of parameters and ranges of their values, which indicate normal work of a service

BUSINESS VALUE

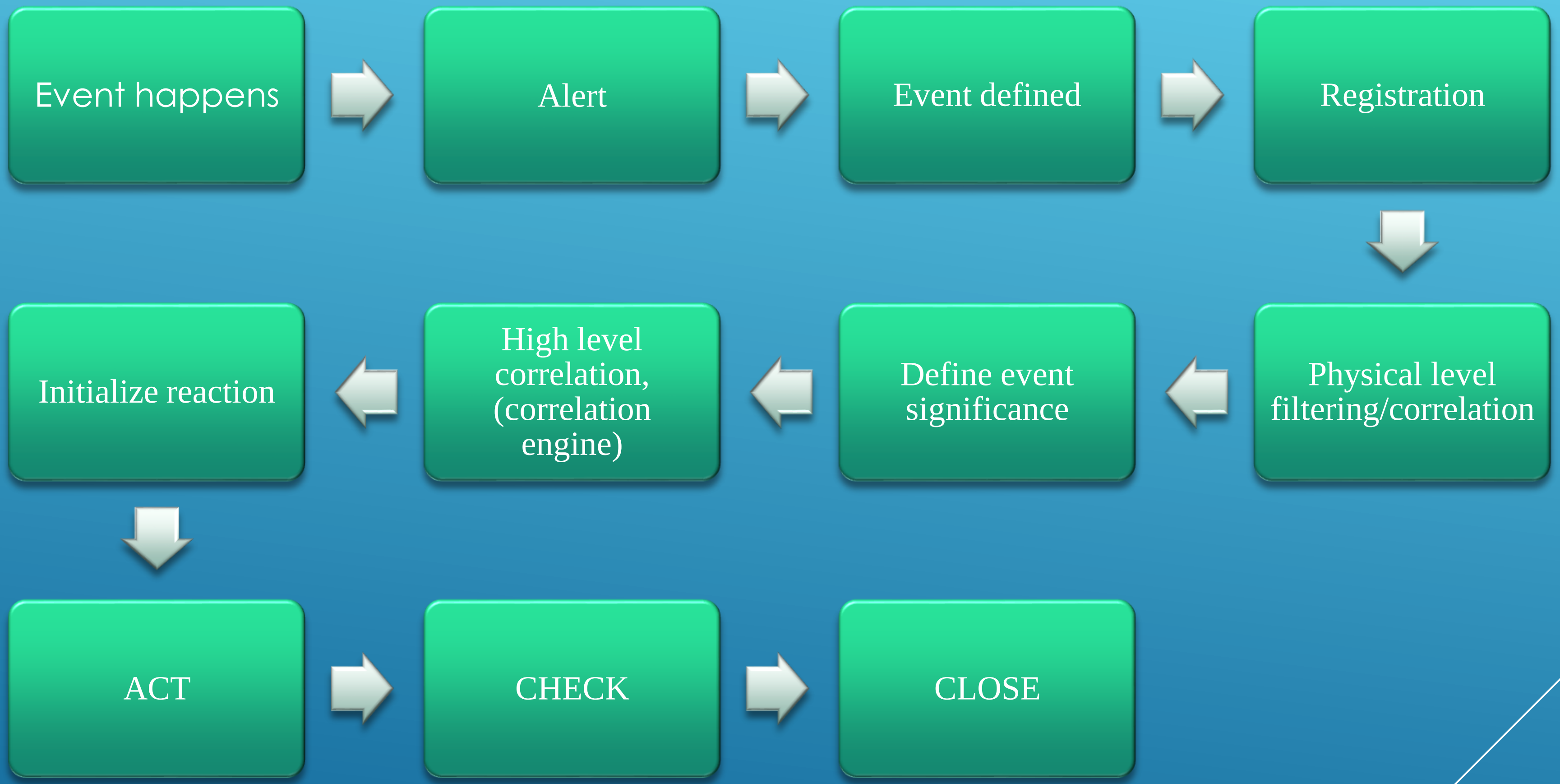
EVT Business Impact is Usually indirect:

- Early and proactive INC discovery
- Improve monitoring efficiency
- A foundation for automation of operation procedures.
- Business operations monitoring
- Proactive customer/user quality assurance

CORRELATION LEVELS


Logical levels (1,2,…)
Physical (component)level
Business process
Correlated business events
Logical rules
Service 1
Service 2
Correlated IT service events
Component base rules and filters
Events by Infrastructure CIs
Net switch
APP Server
APP 1
APP 2
RAID
Database
AD Server

PROCESS WORKFLOW



Event happens

Alert

Event defined

Registration

Physical level filtering/correlation

Define event significance

High level correlation, (correlation engine)

Initialize reaction

ACT

CHECK

CLOSE

EVENT OCCURS

Events occurs regularly, but it is important to define, which of them can impact service level, and fix only them.

The best practice is to involve SD, ST and SO groups into defining EVT policies

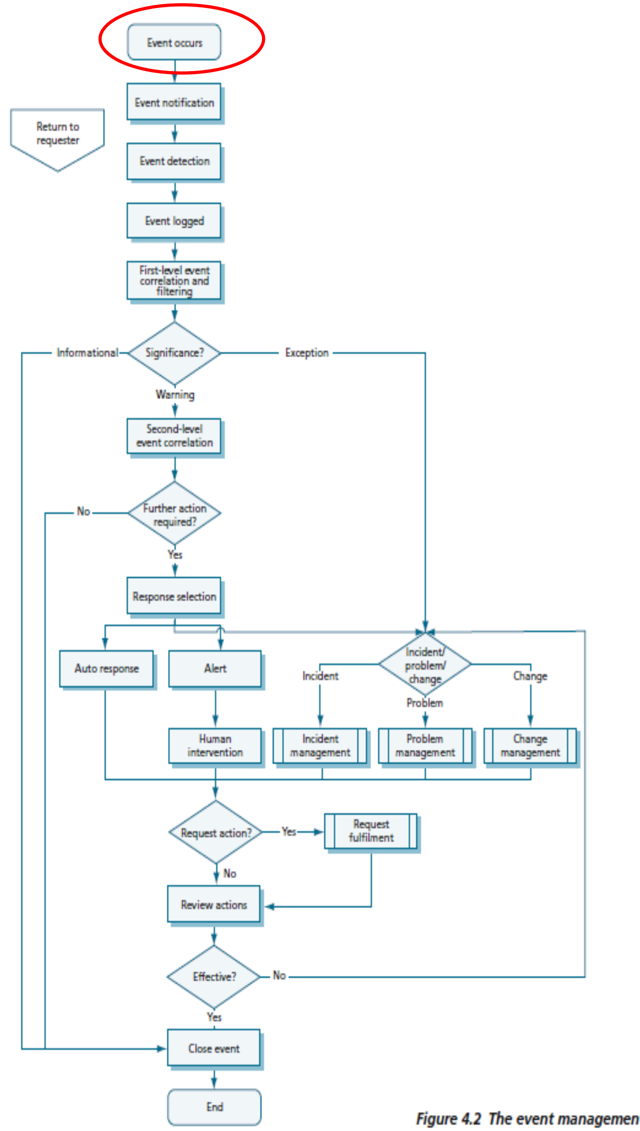


Figure 4.2 The event management process

DETECTION

Two main ways to detect events:

- Active requests by monitoring tools
- CI generates events itself based on a certain triggers or hooks

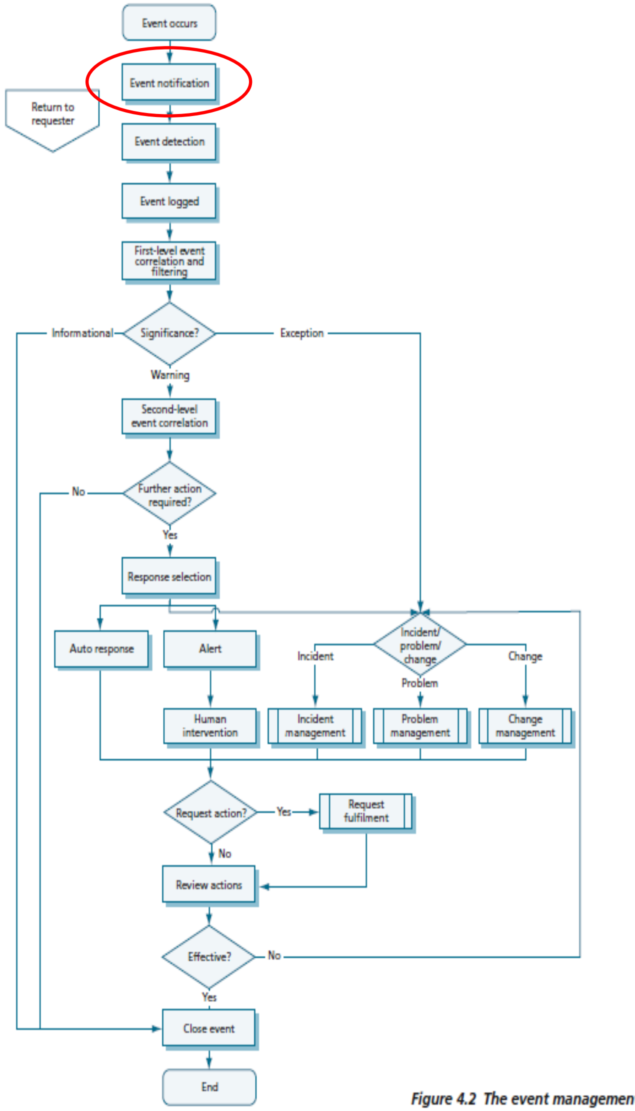


Figure 4.2 The event management process

PHYSICAL LEVEL FILTERING & CORRELATION

Filtering

- Should an event be analyzed?

Fix an event

- Log ignored events

Activities

- Primary even alert
- Switch off alerts from a certain CI
- Define event type

Escalation

- Escalate alerts from certain Cis as they are always important

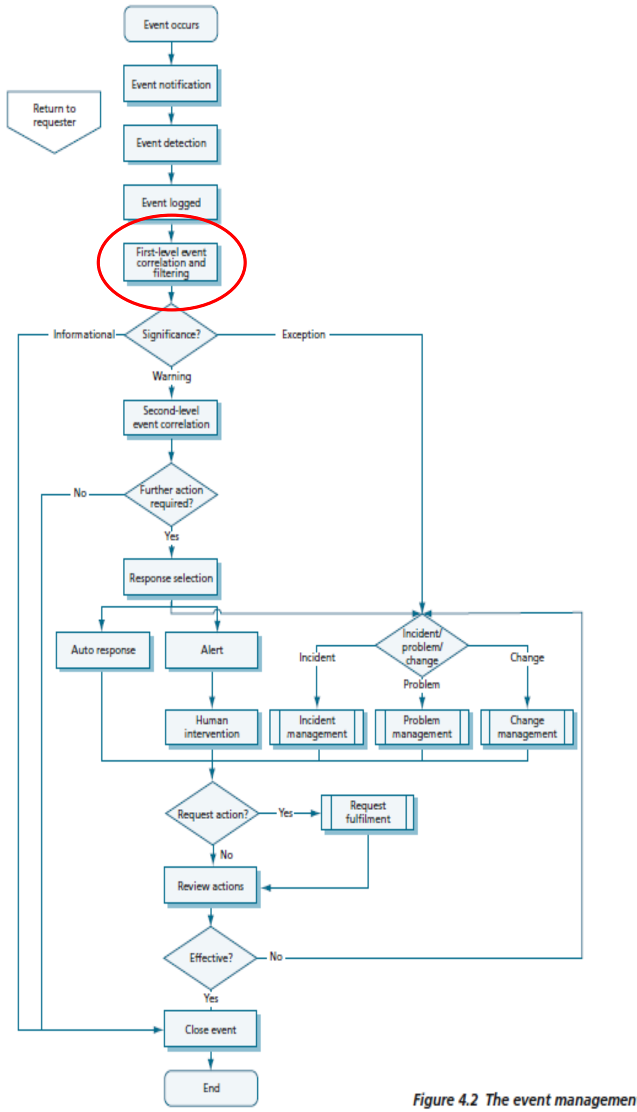


Figure 4.2 The event management process

DEFINE EVENT IMPACT

Informational

- Fix a normal operation (i.e. successful transaction.
- Fix in a log. No alerts

Warning

- Threshold events
- Inform an operator

Exception

- Invalid operation
- Raise INC, PRB, or RFC

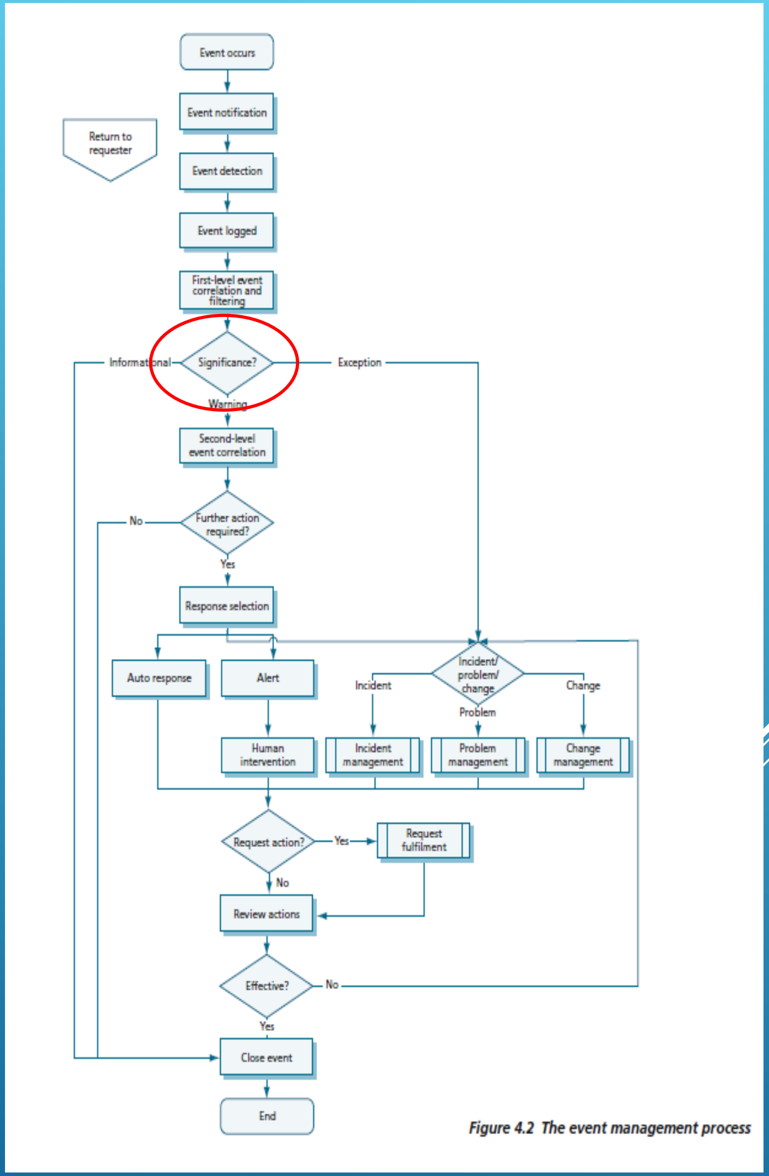


Figure 4.2 The event management process

LOGICAL CORRELATION LEVELS

(Server ping)<20ms AND (Test sql)<50ms AND…

Server ping

DB (test sql)

Application Server

DB Auth OK

DB Sql OK

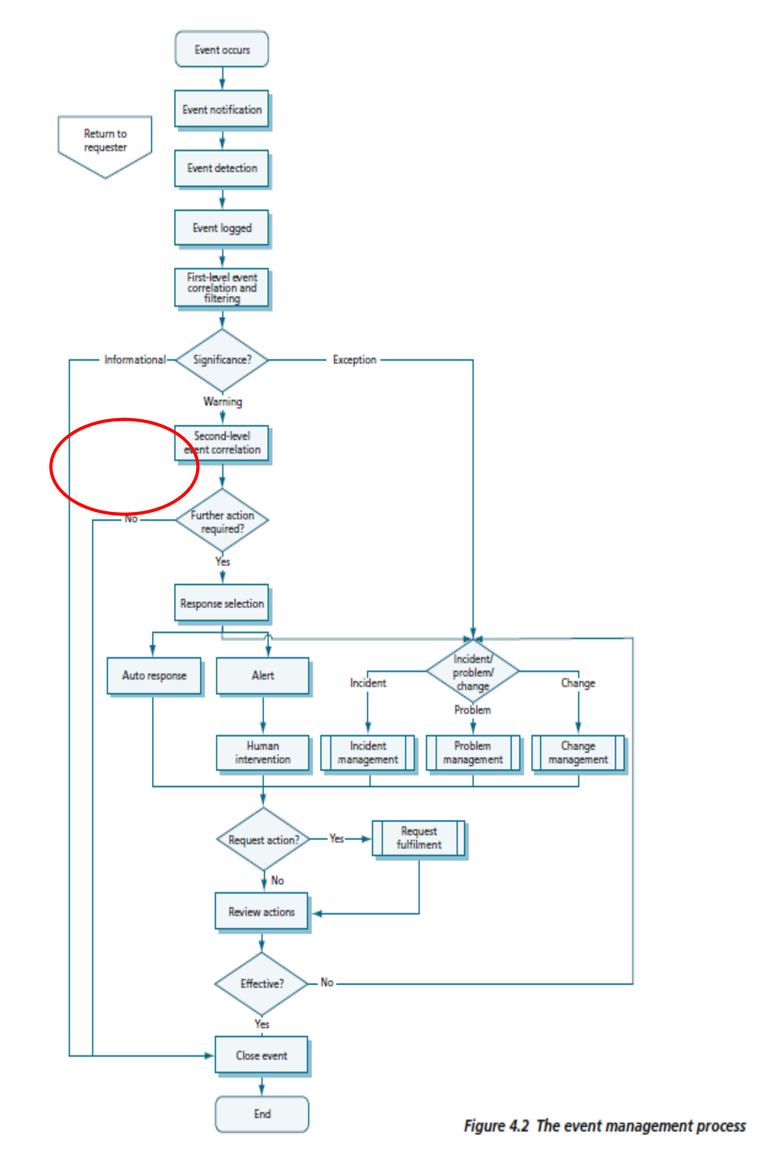


Figure 4.2 The event management process

TRIGGER & RESPONSE

Initiate reaction to an event

Probable actions:

- Raise an INC
- Raise an RFC
- Escalate to a certain operations team
- Run a script
- Other

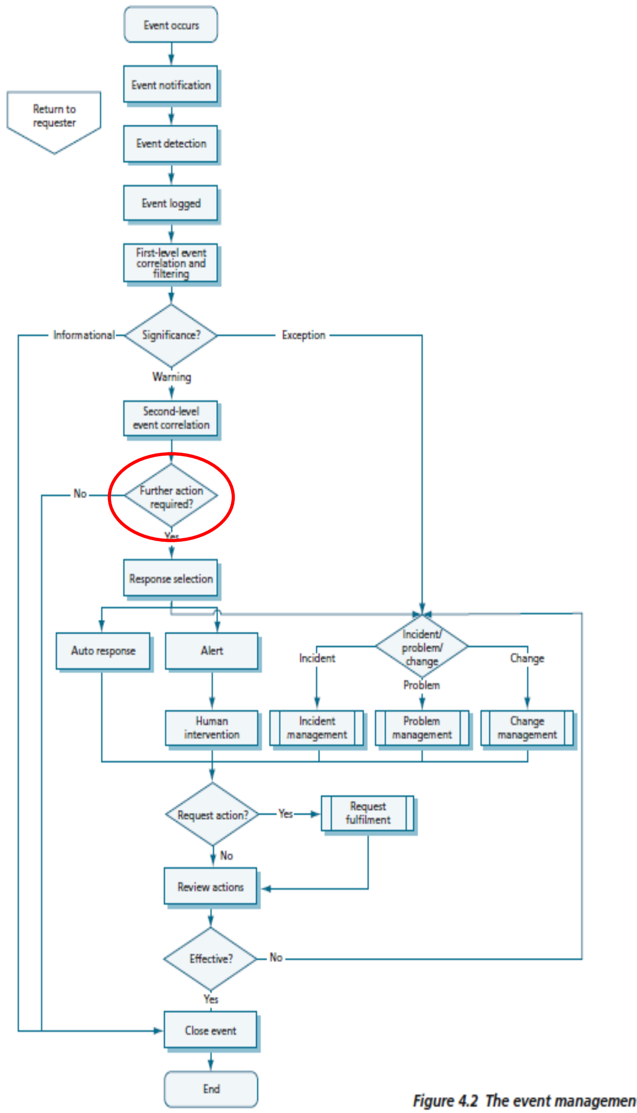


Figure 4.2 The event management process

REVIEW

Review the most important events

Automate review (i.e. Zabbix, MS SCOM)

Establish connection to other processes

Use review for CSI

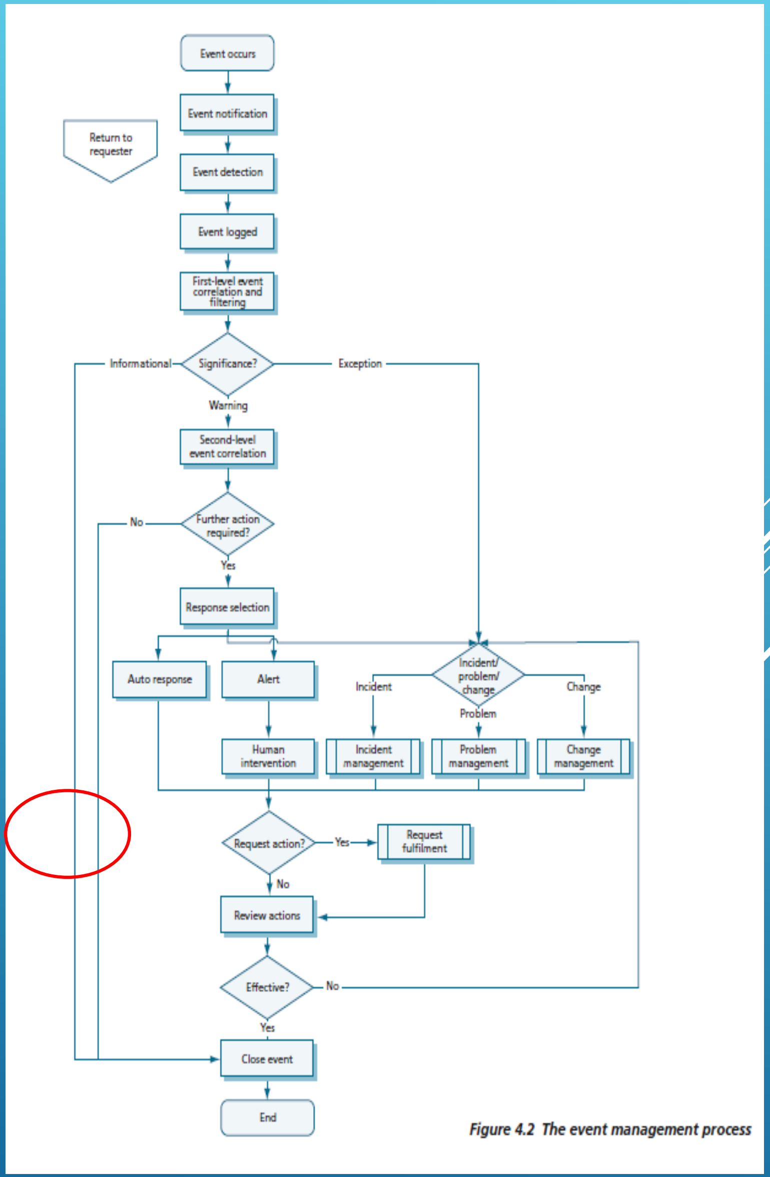


Figure 4.2 The event management process

CLOSURE

Not all events can be "closed"

Automatic closure by other events (i.e. monitoring

Initiate formal closure procedures in case of exceptions

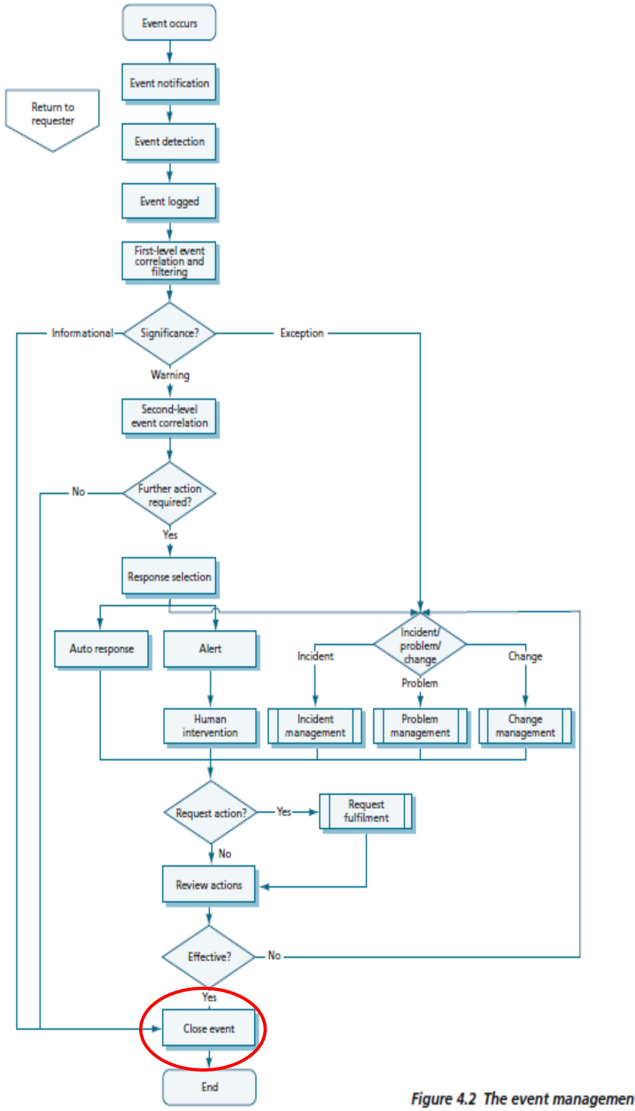


Figure 4.2 The event management process

- Close Integration with Design phase: Availability, Capacity, Continuity, Security management
- Close integration with Change, and Release management
- Involve Supply management into problem solving with the help of external suppliers
- Financial efficiency should be taken into consideration

BEST PRACTICES