

opsdog

WORKFLOW

DO-IT-YOURSELF BUSINESS PROCESS IMPROVEMENT

BPMN 2.0 FORMAT

INFORMATION TECHNOLOGY

Security Incident Management

The OpsDog Support Group Hierarchy

- Information Technology
 - IT Project Management
 - Application Development & Support
 - User Support & Services
 - Network Administration
 - System Analysis
 - IT Security**
 - Security Incident Management**
 - Business Intelligence (BI)
 - IT Procurement
- Finance
- Human Resources
- Marketing
- Legal
- Compliance
- Corporate Services

www.OpsDog.com | info@OpsDog.com | Phone: 201.526.1200 | www.TheLabConsulting.com

Security Incident Management: Workflow

- A** Incident Detection & Reporting
- B** Physical Incident Review
- C** Security Breach Review
- D** Security Investigation

Workflow Description

The identification, reporting, and management of IT security-related incidents. This process includes automatic security alert monitoring, physical incident reporting (lost/stolen equipment), security breach review, and security breach investigation.

Legend

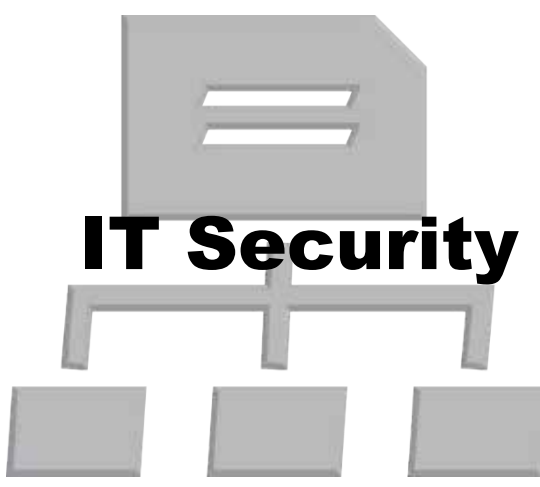
- Start Event
- Intermediate Event
- End Event
- Gateway
- Group
- Task
- Expanded Sub-Process
- Pool
- Sequence Flow
- Message Flow

Copyright © OpsDog, Inc., 2014. All rights reserved.

opsdog.com

Information Technology: Security Incident Management [BPMN 2.0]

Incident Detection & Reporting



KPIs

- Total Security Incidents (serious vs. non-serious)
- Security-to-Value Ratio (STV)
- Incident Prevention Rate
- Incidents per Million Transactions

```

    graph TD
      Start([Receives automatic alert(s)]) --> A[IT Security staff reviews content of automated alert]
      A --> B[Check for suspicious activity related to user account in question]
      B --> C[Determine if there is a potential security threat that requires action]
      C --> D{Pursue threat?}
      D -- No --> E[Alert record kept]
      D -- Yes --> F[Prepare incident documentation to distribute to key IT stakeholders/management]
      F --> G[Notify key management and IT stakeholders of security incident details]
      G --> H[Develop an incident prioritization plan to outline the control impact of the incident]
      E --> End(( ))
      H --> End
  
```

pm_SCO4.IncidentManagementBPMN.150219

opsdog.com **THE LAB**



Login to OpsDog to purchase the full workflow template (available in PDF, Visio)

New users get \$20 off their first purchase (registration is FREE!)