

## CESG Memo 22, GCSx Code of Connection Compliance



*Application Logs, Database Logs,  
 System Logs, Firewall Logs, Bespoke Logs....*

*The list is endless. What can **you** do?*

You can take a pragmatic approach and talk to PTC about PTC Message Manager or you can take a silo approach and purchase tools specific to each type of log file you need to manage. This approach will of course mean you end up with many tools, multiple training requirements and significant purchase/rental/support costs over time.

Initial **CoCo** compliance requires you to store log data for six months and have the ability to interrogate this data. This requirement can be satisfied quickly with the deployment of PTC Message Manager.

PTC Message Manager is however much more than just a log archival tool and will therefore enable you to satisfy future **GCSx** compliance requirements.

### 2009 Value for Money

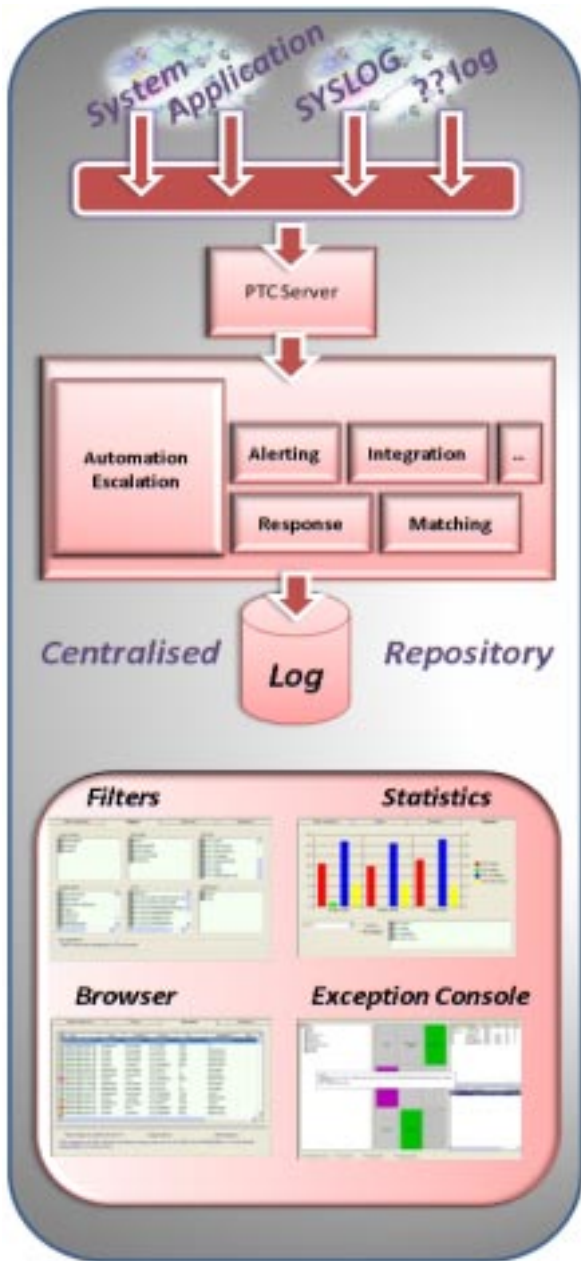
You may tick a number of boxes with regards to security and compliance by capturing and archiving log data, but is that really giving you value for money?. Where is your upside, where are the cost savings in hardware and human resources, where are the incremental savings associated with applying process automation, where are the savings associated with picking up issues from logs that are not identified by your monitoring tools. To realise your upside you need to understand that effort and a fit for purpose utility tool is required, a utility type tool such as PTC Message Manager.

**Log management, although of great value with respect to Audit, Security and Compliance, is really only the tip of the iceberg once you start to take control of your Logs:**

- *Business Process Risk Management*
- *Real Time Security Warnings, i.e. failed logins*
- *Automatic application, system and operational responses*
- *Network, System, Operations and remote Exception Log/Exception console bridge*
- *Additional automation capabilities unique to your environment*
- *Automatic Escalation and Alert response management*

***A utility approach provides value for money and the flexibility required now and in the future***

## Process Automation



## PTC Message Manager enables:

### · GCSx Code of Connection Memo 22 compliance:

#### Stage One

- Collect Logs into log server – put the tick in the box

#### Stage Two and beyond (VFM)

- Filter by functional area (Operations, Network, Application, Security, etc.)
- Apply functional filters (reduce the noise, informational messages)
- Match Messages
- Identify, evaluate, action and escalate

- **Centralised Syslog Server**
- **Storage of Raw and Structured Log files**
- **Real Time Log File Monitoring**
- **Automatic Log File Creation Recognition**
- **Retrospective Log File Monitoring**
- **Log File Investigation and Interrogation**
- **Automation rules (policy enforcement)**
- **Escalation (security/ infrastructure issues)**

The SANS Institute reports that up to 30% of storage is used for log file retention!

MONITOR

MEASURE

MANAGE

**PTC**  
CONSOLE