

KPIs for the real world

By Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT,
Six Sigma Black Belt Certified
ramses.gallego@me.com

- Percentage reduction in number of external attacks
- Improved cost-efficiency of a determined process
- Percentage reduction in time-to-access applications
- Number of people accessing critical systems with super-user privileges
- Number of employees accessing certain documents that do not belong to the department of the owner
- Number/percentage of unstructured data without an owner
- Number of 'toxic' combinations regarding roles
- Percentage of people who is domain/admin and which other entitlements they have in other environments
- Staff productivity (number of deliverables) and morale (through surveys)
- Amount of errors and reworked (linked to corporate Service Desk)
- Benchmark comparisons (such as SANS Institute)
- Percentage reduction in number of Configuration Items (CIs) attribute errors found in CMDB
- Improved speed on patching & fixing vulnerabilities
- More accurate results from risk analysis audits due to available and accurate asset information
- Percentage reduction of blank passwords on critical systems
- Percentage improvement on time-to-access applications
- Improved bandwidth use due to only-professional web surfing
- Percentage reduction in average time to update AV
- Percentage reduction in average time to set up a user account
- Increase in the percentage of reports produced on scheduled
- Percentage reduction in routers and switches causing incidents/failures
- Percentage efficiency improvement based on number of RFCs (Request For Change) processed regarding vulnerabilities
- Percentage reduction in the use of software and hardware releases that have not passed the required quality checks
- Percentage reduction in installed software not taken from DSL (Definitive Software Library)
- Increased percentage on incidents resolved within target times by priority (linked to corporate Service Desk)
- Percentage reduction in the overall average time to resolve incidents (linked to corporate Service Desk)
- Percentage reduction in repeat security incidents

- Percentage reduction in the unavailability of services and components (linked to corporate Service Desk)
- Frequency and review of the type of security events to be monitored
- Number and type of obsolete accounts
- Number of unauthorized IP addresses, ports and traffic types denied
- % of cryptographic keys compromised and revoked
- Number of access rights authorized, revoked, reset or changed