ITSM Maturity Model

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
Incident management	• No standardized incident management process exists • Incident management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing incident management • Incident urgency, impact and priority arbitrarily assigned • No single owner of the process • Existing tools are either inadequate or not used to full capabilities • Incident sources are not captured • Cannot determine whether all incidents are either reported or captured	• Policies governing incident management are published and enforced • Incident management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • Incident urgency, impact and priority classes are clearly defined and used in a consistent manner • Incident lifecycle established • Incident sources are captured and documented • Key performance indicators for resolving incidents are employed and tracked (response and resolution targets based on urgency, impact and priority; first call resolution rates tracked) • Single point of process ownership • Hierarchical and functional escalation paths established • Incident resolution progress is monitored • Knowledgebase established and employed • Incidents with an unknown root cause are passed to problem management • Automated tool in place to support incident management and capabilities and functions are being properly used	• Incident management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all incident management roles • Clear interface between incident management and problem management (problem/known error database information available to incident management) • OLAs between and among other process areas and functions established • Incident lifecycle KPIs measured: ✓ total number of incidents ✓ average resolution time ✓ average resolution time, by priority ✓ averages resolved within SLAs ✓ percentage of incidents resolved by first-line support (without routing) ✓ number of incidents (or percentage) with initial incorrect classification ✓ number of incidents (or percentage) routed incorrectly • Procedures in place to manage incident backlogs • Incidents are correlated to changes • Clear interface between incident management and service level management • Integration of incident management tools and automated monitoring tools	• Policies, procedures and process formally reviewed for continued applicability (on a set schedule; i.e., every six months) • Process monitored for gaps and inefficiencies • Costs per incident – by service – known and continuously tracked • Reconciliation of conflicting goals between incident and problem management • Complete alignment between incident and service level management • User satisfaction measured and tracked • Trend analysis of all KPIs and process parameters • Known costs of each incident by service broken out by CI and urgency	• Incident management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
Problem management	• No standardized problem management process exists • Problem management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing problem management • Root cause analysis is not performed on incidents that do not have a known root cause • Known errors and workarounds are not published • Organization does not distinguish between incidents and problems • No single owner of the process • Existing tools are either inadequate or not used to full capabilities	• Clear differentiation between incidents and problems – all incidents that cannot be resolved or have an unknown root cause trigger the problem management process • Policies governing problem management are published and enforced • Problem management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • Problem classification criteria is established and employed (i.e., category, impact, urgency, priority & status) • Single owner of process • Problems are investigated to determine root cause • Known errors and workarounds are documented and added to the knowledgebase • Clear path of advancing problems to known errors • RFCs are raised when applicable to resolve known errors • Problem database is maintained and up to date • Automated tools in place to support the problem management process with linkage between incident records and problem tickets.	• Problem management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all problem management roles • Clear interface between problem management and incident management (problem/known error database information available to incident management) • Problem management database is integrated with CMDB • Known error elimination is tracked and weekly status reports of outstanding KEs, action taken to date and ETCs for each. • Formal and structured analysis techniques are made a part of SOP and employed • Recurring problems are tracked and analyzed for root causes	• Policies, procedures and process formally reviewed for continued applicability (on a set schedule; i.e., every six months) • Process monitored for gaps and inefficiencies • Trend analysis of problems fed to availability and capacity management • Costs of problem management activities are known and are linked to CIs • .	• Problem management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • Proactive posture – MTBF data from availability management used to predict problems and proactively address them • CIs with identified high incident or problem rates are flagged and analyzed to support financial, service continuity and availability management process goals
Change management	• No standardized change management process exists • Change management procedures are ad hoc • No formal, written standard	• Policies governing change management are published and enforced • Change management process is established and followed	• Change management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly	• Policies, procedures and process formally reviewed for continued applicability (on a set schedule; i.e., every six months)	• Change management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing change management • Changes are made without impact analysis and/or approval • No clear definition of what constitutes a change • Changes often require backouts or trigger incidents • No single owner of the process (change manager) • Lack of a CAB • Existing tools are either inadequate or not used to full capabilities	• Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A change manager has been assigned and is the process owner • A CAB is chartered and members identified • Changes are classified by type, priority and severity • Changes are assessed before submission to the CAB • CIs associated with RFCs are clearly identified • Changes are linked to incidents and problems • RFCs have clearly defined implementation, communication and backout plans • PIRs are performed when changes are made to resolve an incident, problem or known error, and when the change is backed out or deviates from the implementation plan • The CMBD is updated before the change is closed out • A centralized, automated change management tool is in use • KPIs are established and tracked. Example KPIs include: ✓ number of changes implemented in a period (overall and per CI-category) ✓ list of the causes of changes and RFCs ✓ number of successfully implemented changes ✓ number of back-outs and their reasons ✓ number of incidents related to	defined and understood by all change management roles • Clear interface among change, release, configuration, incident and problem management • All process circumventions are visible • Additional KPIs are tracked, including: ✓ rate at which changes are implemented (aggregate and by CI) ✓ number of rejected changes • Graphing and trending of KPIs established • PIR lessons learned are published to promote process improvement	• Process monitored for gaps and inefficiencies • Costs of changes known for each CI • Integration of change management tool and CMDB • Time values established for change implementations by CI to more accurately forecast implementation costs and schedules.	cause investigated when actual values are not equal to forecasts • Analysis of problems and incidents triggering changes to determine opportunities for infrastructure improvement. • Proactively finding cost savings/avoidance opportunities in implementations by CI • Incorporation of known CI MTBF into predict problems and associated changes • Incorporation of capacity trending to predict changes

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
		implemented changes			
Configuration management	• No standardized configuration management process exists • Configuration management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing configuration management • No CMDB, or CMDB is inadequate • Asset focus vs. CI focus • No relationships between and among CIs defined or relationships are inaccurate or out of date • Changes are made without updating CIs • No Configuration Manager assigned • CMDB, if it exists, is not useful to IT Service Continuity Management process and process owner	• Policies governing configuration management are published and enforced • Configuration management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A configuration manager has been assigned and is the process owner • CMDB has been established, populated and has proper relationships between and among CIs • Clear distinction between assets and CIs. • An asset repository, definitive hardware store (DHS) and definitive software library (DSL) have been established • Control by the configuration manager is established by ensuring that the CMDB is always up-to-date, and that no CI is added, changed, replaced or removed without appropriate documentation (completed change request, invoices for new CIs, notification of retiring assets, etc.) • CMDB is available to change management roles to assist in assessing changes • CMDB is updated after every change • CMDB has sufficient level of detail to support IT service continuity management	• Configuration management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all configuration management roles • Clear interface among IT service continuity, change, configuration, incident and problem management • Status monitoring and verification audits are performed • There is a reconciliation procedure to managed rectify discrepancies among the CMDB, asset repository, DHS and DSL, and physical CIs • The following KPIs, at a minimum, are tracked: ✓ delta report - number of observed differences between the CMDB and the actual infrastructure systems that were found during an audit. ✓ number unauthorized changes to CIs found during an audit. ✓ number of assets that could not be located during audits. ✓ number of CIs that could not be located during verification audits. ✓ Number of CIs that were discovered during an audit that did not match attributes recorded in the CMDB (i.e., wrong software license, different physical or logical location, different capacity, etc.)	• Auto-discovery and monitoring tools integrated into CMDB • CI and asset lifecycle costs are tracked • Configuration management tightly integrated with IT service continuity management and financial management	• Configuration management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • MTBF established for each CI to support availability and financial management processes • Incidents and problems associated with CIs analyzed to support reliability analysis by availability management, and TCO and vendor performance by financial management

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
Release management	• No standardized release management process exists • Release management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing release management • No Release Manager assigned • No automated release tools to promote and release	• Policies governing release management are published and enforced • Release management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A release manager has been assigned and is the process owner • The release manager is a permanent member of the CAB • Close integration with the configuration management process to assure that the DSL and DHS are up-to-date and accurate • Established build and testing environments, and where applicable automated release tools are employed (i.e., Serena Mover, Microsoft SMS, etc.), and testing tools • All releases are performed within the change management process • All releases are tested • Rollouts are planned and managed • Post implementation validation is performed on all releases	• Release management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all release management roles • Clear interface between release and change management • All process circumventions are visible • Releases are packaged whenever possible	• Tracking the following KPIs and quality metrics: ✓ number of discrepancies discovered in release notes, build analysis, installation manual(s) and/or defects in media or equipment during release process ✓ time in minutes that maintenance window is exceeded during the release process ✓ number of post release incidents reported within 48 hours of release ✓ number release back-outs required • Release management KPIs and metrics are used to improve CI sources (i.e., development, technical teams and architects, vendor management) • Release management KPIs are aligned to service level management	• Release management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • Continuously evaluating new tools and techniques for quality, build and release activities • Forecasting the impact of new releases to availability and capacity management (i.e., network bandwidth, memory, CPU cycles, etc.). • Analysis and trending of post release incidents, problems and changes to predict support and financial ramifications
Capacity management	• No standardized capacity management process exists • Capacity management procedures are ad hoc • No formal, written standard procedures, or procedures are	• Policies governing capacity management are published and enforced • Capacity management process is established and followed • Formal written procedures that	• Capacity management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all	• Modeling and advanced analytical techniques employed to predict capacity impacts caused by new systems and releases • Discovery and monitoring	• Capacity management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	out of date or not followed • Lack of, or unenforced policies governing capacity management • No Capacity Manager assigned or capacity management is decentralized • Capacity is not aligned to cost justification • Addressing capacity is reactive • No automated capacity management tools	are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A capacity manager has been assigned and is the process owner • Capacity requirements are tied to financial management (cost justification) and are based on availability and service level management • Performance management and application sizing are integrated into capacity planning and management • There are established methods for determining capacity requirements (i.e., vendor release notes, applications and systems technical manuals that give sizing requirements, and internally-developed or commercial tools) • Automated tools are used to monitor capacity metrics • A capacity database is established • Capacity plan is maintained • KPIs employed: ✓ expected increase/decrease of the capacity utilization in the short term and long term ✓ thresholds that, when reached, will require the acquisition of additional capacity.	capacity management roles • Clear interface among capacity, availability, financial and service level management • Capacity is differentiated among business, service and resource and each managed • Clear understanding of business, technical and operational drivers that affect capacity • CMDB is integrated with (or interfaced to) capacity database • Capacity management tools can send automatic alerts to the incident management tool to automatically open tickets • Close coordination between capacity manager and process and availability manager and process • KPIs employed: ✓ discrepancies between the actual and planned capacity utilization ✓ trends in the discrepancies ✓ impact on service levels	tools are integrated • Capacity costs are proactively managed through modeling and prediction • Continuously keeps abreast of emergent technologies that improve capacity at a lower cost	values are not equal to forecasts • Internal technology and business trends are monitored to forecast capacity based on predicted customer demand • Demand is accurately forecasted and met • Continuous service improvement plan in effect
Availability management	• No standardized availability management process exists • Availability management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced	• Policies governing availability management are published and enforced • Availability management process is established and followed • Formal written procedures that are up-to-date and followed	• Availability management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all availability management roles	• MTBF, MTTR and MTBSI are known for every CI • Understanding and quantification of the costs of unavailability • Analysis of incident and problem records to determine threats to availability	• Availability management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	policies governing availability management • No Availability Manager assigned or availability management is decentralized • Availability is not aligned to service level management • Disconnect between IT service continuity and availability management • Addressing availability incidents is reactive • No automated availability management tools	• Roles and responsibilities have been clearly defined and assigned • An availability manager has been assigned and is the process owner • Reliability, serviceability and maintainability are addressed • Service level management governs the process • Automated tools are in place to monitor availability and send alerts to incident management and open tickets • System outage analysis is performed for every instance of an outage • KPIs: ✓ detection times ✓ response times ✓ repair times ✓ recovery times ✓ aggregate availability statistics ✓ percentage availability (uptime) per service or group of users	• Clear interface among capacity, IT service continuity, financial and service level management • Vital business functions clearly defined and methods to assure their availability implemented • Provides recovery criteria to IT service continuity management • Serves on CAB to ensure that RFCs will not adversely affect availability • Establishes availability patterns for IT architecture to ensure that the correct infrastructure availability posture is maintained (resilience, fault-tolerance, continuous operations, etc.) • Proactively identifying and managing single points of failures • Clearly defined availability plan is in place • Uses advanced techniques, such as Component Failure Impact Analysis, Fault Tree Analysis, and CCTA Risk Analysis and Management Method to discover availability vulnerabilities and to model reliability.	• Closely monitors business requirements and SLAs to ensure that availability management anticipates requirements • Modeling availability using tools and advanced techniques • Cost-effectively managing maintenance • Employment of technical observation posts for all vital business functions that cannot be otherwise monitored through automation or because of unresolved problems that affect availability	• Proactive preparations for faults based on MTBF and MTBSI statistics (ability to accurately forecast faults and minimize the MTTR) • Actively engaged in reducing MTTR for CIs that support vital business functions
Service continuity management	• No standardized service continuity management process exists • service continuity management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced	• Policies governing service continuity management are published and enforced • Service continuity management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and	• Service continuity management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all service continuity management roles • Clear interface among	• Understanding and quantification of the costs of outages to each service supporting a vital business function • Understanding and quantification of costs associated with outages from the perspectives of: ✓ regulatory compliance	• Service continuity management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • Continuous service

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	policies governing service continuity • No service continuity manager assigned or service continuity management is assumed to be under the purview of BCP/DR • No cross-functional awareness of service continuity initiatives • No prioritization of services to be recovered • Service continuity is not aligned to service level management • Disconnect between IT service continuity and availability management • No version control tool to manage service continuity plans and documents	assigned • A service continuity manager has been assigned and is the process owner • All stakeholders have visibility into the service continuity process • Vital business functions have been identified and used as a basis for service recovery • Service level requirements from SLAs, and [any] regulatory requirements are used as a basis for business impact analyses • Risk assessments and business continuity strategies are in place for all services supporting vital business functions • Detailed recovery plans are in place for services that support vital business functions • Version control tool exists to manage all plans and related documents	availability, capacity, financial and service level management • Changes to availability and capacity plans, or SLAs trigger updates to recovery plans • CMDB continuously monitored for changes to CIs that are associated with services supporting vital business functions • Serves on CAB to ensure that RFCs will not adversely affect service continuity or recoverability • Recovery plans and procedures are reviewed and audited on a scheduled basis • Manages ongoing training and awareness • KPIs established and tracked •	✓ loss of customers or customer goodwill ✓ loss of market share ✓ loss of revenue • Closely monitors business requirements and SLAs to ensure that service continuity management anticipates requirements • Recovery plans and procedures are live tested on a scheduled basis • KPIs refined and tracked	improvement initiative in place • Uses analytical modeling tools to develop and model recovery scenarios • Recovery scenarios live tested
Financial management	• No standardized financial management process exists • financial management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing financial management • No financial manager assigned or financial management activities are focused on budget management • Accounting, other than budget management, and charging strategies are not used • No knowledge of the total cost	• Policies governing financial management are published and enforced • Financial management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A financial manager has been assigned and is the process owner • Budgeting and accounting techniques, and changing strategies are employed • Total costs to support or deliver a service are known	• Financial management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all financial management roles • Total costs of ownership are known for each service • Underpinning contracts and associated payments are routinely audited • Costs of compliance known and factored into total costs of ownership • If charge backs are used a P&L is established • Costs for each service unit are	• Established time values in place for frequently performed activities • Activity based cost management employed • Cost benefit analysis uses NPV as a key factor • SLAs incorporate value-based charges (if charge back is used) • Business has visibility into financial management process, including all cost drivers associated with delivery or support of a service • Uses budget forecast accuracy KPI that is within statistical control and monitored using	• Financial management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • Continuous analysis of cost drivers to find cost elimination or avoidance opportunities • Modeling and forecasting of key cost drivers

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	to support or deliver a service • Makes acquisitions or expenditures without a quantifiable cost benefit • Acquisitions or expenditures not traceable to business requirements • Tools are non-existent or based on individually or group developed spreadsheets and ledgers	• Cost benefit analysis performed for each acquisition or expenditure over a defined threshold • Acquisitions and expenditures are made to support identified business requirements • Charge backs, if used, are regularly audited • Basic KPIs established (i.e., allocated vs. actual, over- and under-runs, number of times supplemental funding needed) • Standardized tools are employed	provided in the service catalog • Additional KPIs established (examples: earned value for project-based activities, validating cost/benefit assumptions after an acquisition or expenditure has been made and is incorporated into the service suite)	X-Bar/R chart • Input into renewal or exercise of additional option years of underpinning contracts to eliminate or avoid cost overruns and scope creep • Completely aligned to all regulatory requirements • Formal governance of all acquisitions and expenditures over a defined threshold	
Service level management	• No standardized service level management process exists • Service level management procedures are ad hoc • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing service level management • Business unhappy with, or neutral about, level of service provided • Lack of SLAs or SLAs not based on service specifications and service level requirements jointly developed with customer • SLAs from each process area presented to customers • No operational level agreements between and among process areas and functions • Lack of, or wrong, KPIs • Vital business functions unknown or not adequately addressed • Management by personality	• Policies governing service level management are published and enforced • Service level management process is established and followed • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A service level manager has been assigned and is the process owner • SLAs are negotiated with each customer based on: ✓ service level requirements ✓ service level specifications ✓ service quality plan • A service catalog is established and kept up to date • OLAs are established between and among each process area and function associated with an SLA to assure service levels are delivered per agreement • When a service is provided that is based wholly on an	• Service level management process is aligned to ITIL framework • Interrelationships between and among other ITIL processes and functions are clearly defined and understood by all service level management roles • Ongoing review of operational level agreements, underpinning contracts and service level agreements to ensure that all terms, conditions, requirements and specifications continue to reflect valid business needs • Customers have visibility into the service level management process • Performance scorecard for each process area or function covered by an OLA developed and employed	• Service improvement program established • Customer satisfaction measured • Vendor scorecards employed • Cost for each service catalog unit is known • Reporting to customer contains line item showing value of service level delivered • Active involvement in RFI/RFP process, and contract negotiations when underpinning contracts affect service level management • Underpinning contracts are results based with penalty clauses • Anticipates new business requirements • TQM techniques employed	• Service level management process continuously reviewed for improvement opportunities • Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • Service quality board established with partnership between service level manager and customer • SIP in continuous improvement mode based on 6-Sigma

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
	instead of process	underpinning contract the service level manager uses service level requirements and specifications as the basis for contract negotiation and contract management • SLAs governing vital business functions are identified and managed at a high prioriity • All KPIs associated with an SLA are monitored and reported as agreed to in the SLA and service quality plan • SLA governs the IT/customer relationship			
Service Desk (Function)	• No governing service desk process exists (i.e., incident management) • No formal, written standard procedures, or procedures are out of date or not followed • Lack of, or unenforced policies governing service desk • Service desk is not always the initial point of contact within the organization for service requests or error reports – customers often go around the service desk to 'get things done' • Tools are not aligned to ITIL Service desk function or key processes such as incident management • Service desk assumes default ownership of incident management (problematic when the service desk model is a distributed service desk)	• Policies governing service desk are published and enforced • Service desk is governed by a process or processes (at a minimum by the incident management process) • Formal written procedures that are up-to-date and followed • Roles and responsibilities have been clearly defined and assigned • A service desk manager has been assigned and is the function owner • Provides monitoring and reporting of the attainment of all service level requirements associated with governing processes are met (i.e., if an SLA contains a requirement that an outage to a service supporting a vital business function is resolved in 4 hours or less then the service desk would report the unfulfilled requirement) • Establishes basic KPIs (i.e., time to answer, number of	• Interrelationships between and among ITIL processes and the service desk function are clearly defined and understood • Service desk performance is included in SLAs • Customer satisfaction surveys are conducted, compiled and reported • Customer self-service is implemented (i.e., service requests can be directly opened by customers using email integration, web based forms or other methods)	• Service improvement program implemented • Incidents are correlated with changes • Incidents are not closed without customer concurrence (although they may be marked as completed) • If the service desk is also governed by the change management process changes are not closed until PIRs have been completed	• Regression analysis applied to KPIs; gap analysis and root cause investigated when actual values are not equal to forecasts • SIP in continuous improvement mode based on 6-Sigma

	1- Ad Hoc	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimizing
		incidents incorrectly assigned, number of first call resolutions) • Tools used by the service desk support the processes that govern the service desk			