

Genesys

Implementation Readiness

Best Practice Document

Platform Operational Best Practices

Document

Genesys

**Version:**



**Value Realization**

Genesys

**Logo Here**

**Customer Name Here**

Date here

**Contents**

[1. Introduction 3](#_Toc511718637)

[1.1. How to use this guide 3](#_Toc511718638)

[2. Technical Considerations 3](#_Toc511718639)

[2.2. Roles and Security 3](#_Toc511718645)

[2.2.1. Roles 3](#_Toc511718646)

[2.2.2. Security 4](#_Toc511718647)

[2.2.2.1. Security Audit 4](#_Toc511718648)

[2.2.2.2. Password management 4](#_Toc511718649)

[2.2.2.3. Named accounts 7](#_Toc511718650)

[2.3. Continuous testing 7](#_Toc511718651)

[2.4. Platform 8](#_Toc511718652)

[2.4.1.1. Data masking 8](#_Toc511718653)

[2.4.2. Back-up 8](#_Toc511718654)

[2.4.3. Browser updates 8](#_Toc511718655)

[**3. Business operations** 8](#_Toc511718656)

[3.1. Routing strategies 9](#_Toc511718657)

[3.2. Planning & staffing 11](#_Toc511718658)

[3.3. Quality management 11](#_Toc511718659)

[3.4. KPIs 12](#_Toc511718660)

[3.4.1. Alignment 12](#_Toc511718661)

[3.5. Real-time management 13](#_Toc511718662)

[3.5.1. Exception handling 14](#_Toc511718663)

[**4. Processes** 14](#_Toc511718664)

[4.1. ITIL Service Operation 14](#_Toc511718665)

[4.2. Business continuity 14](#_Toc511718668)

# **Introduction**

Genesys creates exceptional omnichannel experiences, journeys and relationships because we passionately believe that great customer engagement drives great business outcomes.

But the challenges in the Contact Center business are getting more and more complex with the growing demands on customer experience management and satisfaction, increasing trend of Digital channels and the pressure on cost efficiency and effectiveness for measuring performance. In this dynamic context, it is not easy to keep your Genesys environment optimally aligned for these challenges.

Not to worry, you have partnered with the world’s #1 Customer Experience Platform and we are here to go together through this journey and support you with our best practices and expertise.

Over the years Genesys and our customers have designed, built and deployed a wide range of unique Genesys environments ranging from simple 20 to complex 20,000+ seat deployments. During these times, we have collected a list of best practices implemented within these organizations that aided in the success of these customer environments. Not only before and during the deployment, but after up and running for several years.

Read this Operational Best Practices document to learn how can you run your platform in the most effective way and aligned to your business operations, so you can maximize the investment in the Genesys solutions.

* 1. How to use this guide

This document is intended to provide you with information on best practices used by Genesys customers to support and maintain a Genesys platform. This is not intended to be a mandatory set of rules, but more of a starting point in your process of optimizing your platform management and the business operations. These best practices can be used to create business processes and procedures that work within your organizations culture.

This document is intended to be a living record of best practices used to support, maintain and grow a successful Genesys investment. Please consider this a starting point for your organization, some of the suggestions may fit within your organization and others may not.

# **Technical Considerations**

1.
2.
3.
4. 1.
	2. Roles and Security
		1. Roles

Roles play an important role within the Genesys environment. The Genesys roles and permission concept allows fine granular to features and functions in addition to access control. For a roles and permissions concept to be implemented successfully the following organisational requirements exist:

A clear definition of roles within the Business and IT departments of the Customer. Each of these roles must clearly describe a function or a set of functions to be performed by individuals belonging to this role. Generic approaches, specifically for a large environment are not recommended. Roles must be aligned with the existing, or new to be designed, processes to access the Genesys platform.

In general, the larger the environment the more distinct roles, within reason, will be configured. Specific to Agent roles the recommendation is to split the roles into two parts:

Role-1 a generic agent role which is across all channels allowing certain functionality for all agents.

Role-2 a role per channel allowing certain media specific tuning by media type. If an Agent is multichannel enabled for example a voice and e-mail role can be assigned.

For each of the configured roles a corresponding access group must be configured. This will ensure a consistent approach towards assignment of roles to new and existing persons.

In addition to the roles concept the permissions must be set. As a general guideline, a restrictive approach is recommended. Users should only see and have permissions on objects the need from a platform technical point of view next to their assigned role. Developing the roles and permission concept must be done in parallel keeping in mind what each role requires in terms of feature functionality and the required permission to objects as part of that role.

* + 1. Security

Cloud-based applications require intensive and ongoing corporate vigilance to conform to enhanced security standards. As a global provider of cloud-based applications and services, we understand the importance of our clients’ ability to continuously deliver great experiences to their customers. The security of our service is instrumental in maintaining the trust placed in Genesys by our clients. We recognize how important it is to ensure confidentiality, integrity and availability for client data and the services supporting the data. The following papers provides insight into the defined Genesys approach to Cloud security for PureEngage Cloud platform.

[Genesys Cloud Security: Philosophy and Approach](http://www.genesys.com/resources/Cloud-Security-Philosophy-Approach-WP-EN.pdf)

* + - 1. Security Audit

To ensure integrity in terms of user access to the Genesys platform, a process for managing the user accounts has to be defined and followed. However, in reality, certain situations may occur in which access to the platform is granted ad-hoc, bypassing the process.

Therefore, as an additional measure, it is recommended to perform an audit of user accounts on the platform on a regular basis to identify those dormant ones.

The complexity of both the standard process and the audit heavily depends on the complexity and size of the actual Genesys environment. These may be manual or tool supported.

* + - 1. Password management

Password management and authentication management can be handled internally within Genesys configuration server or handled by a corporate LDAP or AD server. Using an LDAP/AD server has the advantage that corporate policies are automatically enforced. In addition to this Desktops can be modified to allow single sign on (SSO). Integration with LDAP and using SSO is considered best practice and is the preferred method.

If Authentication is handled within the Genesys environment the following option are recommended to be set as a best practice:

**Account-expiration**

Specifies the maximum number of days for which an account can remain idle. After this time interval, the account will be considered expired and the user will not be able to log in until the account has been reactivated by the system administrator. Configuration Server checks for expired accounts when an account belonging to this Tenant tries to log in or authenticate, or when a User object belonging to this Tenant is retrieved or changed.

Related to this feature the following options must be set:

* Last-login
* Last-login-synchronization

**Account-lockout-attempts-period**

Specifies the length of time (in minutes) since the last unsuccessful login attempt in which another unsuccessful attempt will be counted toward the lockout threshold specified by **account-lockout-threshold**. If another unsuccessful attempt is recorded before this time interval expires, the time of this latest attempt becomes the basis from which this time period is calculated. In effect, this period is a sliding window. If no additional unsuccessful attempts occur within this time period, the number of unsuccessful attempts is cleared, and previous attempts are not counted towards the lockout threshold.

**Account-lockout-duration**

Specifies the length of time (in minutes) that the lockout lasts after the lockout condition has been met. Accounts already locked when this option is changed are released after the time specified by this option elapses, regardless of how long they were locked out originally.

**Account-lockout-threshold**

Specifies the number of consecutive unsuccessful login attempts that a user account can make before being locked out. When set to the 0 (the default), no lockout will occur

**Max-account-sessions**

Specifies the number of simultaneous connections that each account can have with a single instance of Configuration Server. If an account tries to exceed the number of connections, login is denied.

**Password-expiration**

Specifies the number of days from when the user password was created and after which the password is considered expired and cannot be used. If set to 0 (the default), the password will not expire.

**Password-expiration-notify**

Specifies the number of days before a user password expires that a notice will be displayed to the user warning that his or her password will expire. To take effect, the specified value must be less than the number of days left before the password expires. If set to 0 (the default), no notification is sent.

**Password-min-length**

Optional. Specifies the minimum length (in characters) of a password used by all users in the Tenant in which the option is defined. If this option is present, it overrides the **allow-empty-password** option. If this option is set to 0, an empty password is permitted (regardless of the value of **allow-empty-password**). If this option is set to a value greater than the maximum allowed value (64), the maximum value is used

**Password-no-repeats**

Specifies the number of password changes that must occur (that is, the number of old passwords) before a prior password can be reused. If set to 0 (the default), no history of used passwords is kept, and a password can be re-used as desired

**Password-req-alpha**

Specifies whether a password must contain at least one US-ASCII alphabetic character (a-z, A-Z). If set to true, and a password being created or changed does not contain one or more alphabetic characters, Configuration Server will not save the changes.

**Password-req-mixed-case**

Specifies whether a password must contain at least one uppercase character (A-Z) and one lowercase character (a-z) from the US-ASCII character set. If set to true, and a password being created or changed does not contain one or more uppercase characters and one or more lowercase characters, Configuration Server will not save the changes.

**Password-req-number**

Specifies whether a password must contain at least one numeric character (0-9). If set to true, and a password being created or changed does not contain one or more numeric characters, Configuration Server will not save the changes.

**Password-req-punctuation**

Specifies whether a password must contain at least one punctuation character from the US-ASCII character set. If set to true, and a password being created or changed does not contain one or more punctuation characters, Configuration Server will not save the changes.

The following punctuation characters are permitted:

* ! “ # $ % &’ ( ) \* + , - . /
* : ; < = > ?
* [ \ ] ^ \_ `
* { | } ~

**Optional:**

**Porce-password-reset**

Specifies whether all applications must prompt all their users to change their passwords at first login. If set to true, all users for whom password reset is enabled (Reset password is checked on the user Configuration tab) will be unable to login unless they reset their password the next time that they log in. Any exceptions to the policy of changing passwords at first login (down-level applications or applications for which the **no-change-password-at-first-login** option is set to true) will not be permitted. The user will not be able to log in until he or she uses the correct application or the administrator clears the Reset password checkbox on the corresponding User object’s Configuration tab

Note that some of the above options do not apply to the default user login. The reader is referred to the respective deployment guides available on the Genesys documentation site before setting up the authentication rules. Specifically, in a multi-tenant environment option hierarchy and override options on lower level objects may affect the desired behaviour.

In addition to this as a best practice the password for the default account must be changed from it’s default value. Once changed this default account must be handled following the policies for administrator or root logins

* + - 1. Named accounts

User access and user maintenance within the Genesys platform must follow the corporate policies. Sharing logins is not a good practice. Each user with access must meet the following criteria:

Each user has a unique and personal login to the Genesys platform.

User authentication is preferably integrated with the corporate LDAP or Active Directory server. If internal authentication is use it is strongly recommend to setup and enforce password policy rules within the Genesys environment. (See the respective paragraph 2.2.2.2 within this document) As a best practice this principle must be applied to all Genesys environments a user has been granted access to. Special attention and care should be taken with the ‘default’ user. As a general best practice the functions requiring high levels of access must be configured and assigned to the proper role and permissions. The ‘default’ user should be used only when required.

* 1. Continuous testing

To provide an additional layer of operational excellence, continuous testing of the processes covered by the Genesys CX platform may be recommended. This kind of testing, which takes place continuously on the production platform contributes greatly to early recognition (hence resolution) of issues which may affect the customer experience.

The testing varies depending on the process being tested, mainly:

* On its technical nature
* Whether only a certain part of the process is to be tested or the process is tested end to end.

In case of end-to-end testing, typically, the testing points are defined for the process, in which data about the interaction is submitted to a central authority (system) responsible for the testing and its evaluation. Please note, that the process being tested may span multiple systems which Genesys CX platform is one of.

Such tests can be executed on different pools of interactions:

* All production interactions
* Subset of production interactions
* Dedicated testing interactions

Alternatively, tests focused on a particular module of the CX platform may be run. A good example with clear business benefits is continuous Voice Health Checks (VHC) that can be setup by Genesys. Continuous testing of the system for any enterprise system ensures consistent and spotless customer experience.

* 1. Platform
		+ 1. Data masking

In nowadays world data privacy and the legislation around personal data are becoming an increasingly important topic. As part of the deployment consideration about what data is sensitive and should be masked is best made upfront. During the deployment of a solution the sensitive data can be masked avoiding sending sensitive data collected in log files etc. As a best practice, all data marked as sensitive must be masked when printed in logfiles. Access to logfiles in general must be restricted to those employees who really need it. Often logfiles are stored in a general accessible file storage system or in the centralized log database. Often access to log information is relaxed. Best practice is to treat logfiles with same corporate policies for accessing sensitive personal data.

* + 1. Back-up

PureEngage Cloud can export GIM and WFM ETL data for storage at a customer’s facility. Recordings can also be requested to be exported. Genesys cloud customer’s general overall backup strategy will be handled by the Genesys team.

* + 1. Browser updates

Customers should be subscribed to browser support updates to ensure that they are aligned with PureConnect Cloud.

1. Business operations

Any technology deployment is initiated to support a business objective. In the Contact Center world we are talking about the Contact Center strategy or better said the Customer Experience Strategy. The Customer Experience Strategy outlines how the contact center should deliver service and hence how the Routing Strategies should work in the Genesys solutions. Periodically reviewing it to ensure it’s still aligned with your organization Strategy is key to clarify contact center priorities with regards to financial investments, new channels, and weak points or gaps in service.

We suggest following items for your Customer Experience Strategy review:

* **Customer segmentation.** Defined characteristics and preferences of customers
* **Priority and high-value customers.** Differentiated service offered to valuable, strategic customers
* **Contact reasons.** Understanding main reasons of contact, self-service options and next best action
* **Contact channels.** Where do you want your customers to contact you and what is driving this (customer preference, efficiency, experience, other)
* **Hours of operation.** Clarifying the level of support 24/7 365 taking into account customer preferences and operational effectiveness
* **Customer experience measurements and objectives**. What measurements best reflect the customer experience (customer satisfaction, customer effort, repeat calls) and the right objectives for our business
* **Business and customer intelligence.** Are you leveraging all the insight from the contact center data to support gaps identification and improvement opportunities
	1. Routing strategies

The goal of routing is prioritizing and matching the right work to the right resource at the right time to optimize engagement and help both customers and organizations reach their goals. With queue-based routing, reporting is centered around queues and agents typically log into queues to process work items. Queue-based routing creates isolated silos that make it hard to service, manage, and report on workload across channels. It’s also hard to blend or load balance agents across queues and channels.

In contrast, agent-based routing has many advantages. Agents log into a universal queue where work is routed to agents based on skills, presence, SLAs and other business rules to cost-effectively deliver the best experience for each customer. The routing can be flexibly configured to leverage additional context such as opportunity value, customer segmentation, customer profile and journey history to get the best available agent versus the first available agent.

In Genesys the routing logic can be configured by using the following priority tuning parameters:

* Increment priority. The amount to increase the priority after the interval time
* Time interval. The time between priority increases
* Starting priority. The maximum priority
* Max priority. The maximum priority

The skill expression to define the target is defined by a combination of skill(s) and skill levels. Best practice is to use the same skill(s) with decreased skill level in subsequent targets to gradually expand the pool of agents after each timeout, rather than using a different skill. Consolidation of agents into larger answering groups is always more efficient than smaller, siloed agent queues.

Skills should be aligned with what the agents’ knowledge and skill levels with their proficiency levels. This is the recommended approach for best customer experience. For best results, the customer identification or accurate call type is needed prior to the call routing to ensure correct distribution to the right skills and skill levels. This information is typically managed in the IVR.

**IVR**

The IVR offers self-service options and lets customers identify the reason for their call and be routed to an agent skilled to handle that issue. Some IVRs also proactively identify information about callers – such as the number they are calling, the number they are calling from, their area code – and use that information to decide how to route the call.

In many cases the IVR is seen as a way to filter the interactions with the purpose to avoid the call being transferred to an agent but in reality the IVR is an important entryway into the organization. In many cases, customers form their first impression of the company based on how easy and effective the IVR is. In the customers’ eyes, the IVR is a reflection of the organization brand, so it is a best practice to have the Customer Experience Strategy in mind when designing the IVR experience for your customers.

Creating an IVR that improves contact center efficiency while satisfying customers often requires tradeoffs and extensive testing. And it never ends. IVR usage should be continually revisited as new technologies become available, the business changes, and we learn more about how customers use it.

**Digital**

We have spoken so far about 2 connected channels used to manage the customer interactions: IVR and Contact Center. But now in the Digital world there are more and more channels that customers prefer to use to interact with the organizations: outbound, SMS, email, chat, video and social media. While adding new channels is driven by the marked demand, the organizations need to be mindful of the pitfalls:

* Operational complexity,
* Inefficiencies when operating in silos,
* Measurement challenges,
* Overwhelming customers with too many choices

A continue analysis on customer preferences, differentiated services and channel integrations would be key to the success on an Omnichannel Customer Experience Strategy.

**Omnichannel**

While you integrate new channels, the analytics will play a very important role, allowing to better understand the customer behaviour across channels and request types. Having strong, integrated analytics can help to make a big step in your Customer Experience Strategy, and move from reactive to proactive care by using analytics to do predictive/intelligent routing, integrating the life-cycle view and determining the channel of choice.

**Workload management**

In addition to the customer facing channels there is also the back-office work that needs to be taken into consideration. The best practice is to aim for automation of the easiest, redundant tasks and route the most complicated tasks to a specialized team for processing. Integrated routing is again useful, to make sure the back-office team has all the details needed to process the request and the first line agents know the status of the request, in case the customers are asking for follow-up. Keeping the customer informed of the progress of their request by proactive notifications is also a key element for a great customer experience.

* 1. Planning & staffing

Workforce Management (WFM) is the art and science of ensuring the right staff is in the right place at the right time to handle customer interactions within performance objectives. While this sounds simple enough, the reality is far more complex. In every contact center, a wide range of universal and unique factors influence the contact center’s staffing requirements and available staff.

While every workforce management team sets their own processes and priorities, most workforce management teams focus their efforts on these four activities:

* **Forecasting Requirements** to determine number agents and associated skills needed for proper staffing.
* **Planning Work Schedules** to ensure staff is placed at the proper times throughout the day/week to meet performance objectives.
* **Managing Employee Time and Adherence** to ensure staff is in place at the right times to meet the performance objectives.
* **Real Time Monitoring and Analyzing** to make adjustments to ensure objectives are being met in real time and improve planning efforts.

Workforce management technology can assist with all of these activities. By optimizing and automating many aspects of the planning process, contact centers can schedule the appropriate employees to tasks at the appropriate times to facilitate business goals.

For best results, the WFM set-up needs to be aligned to the contact center structure and if possible, the 2 systems fully integrated.

* 1. Quality management

Quality management is the process a contact center uses to measure the effectiveness, efficiency, and consistency of the service you deliver to your customers. In most contact centers, the goal is to deliver the best service possible at the lowest possible cost. To do this, contact centers listen to calls, review chats and emails, and assess the quality of those interactions using a consistent quality evaluation form.

Customer satisfaction is your customers’ perception of the service you deliver. For most contact centers, customer satisfaction is the ultimate insight into how your contact center is performing. When customers are satisfied with the service they receive, this drives positive feedback and word of mouth, and increased revenue and customer retention. Customer satisfaction is routinely gathered using customer feedback surveys, customer feedback on social media, or customer interaction behaviors (repeat calls, recorded interactions).

High performing contact centers continually look for every possible insight into their performance and carefully analyze quality and customer feedback results to determine how to improve performance. Many customers use Genesys’s workforce optimization and quality products to support their quality and customer satisfaction-related goals.

* 1. KPIs

In almost every contact center, success is measured hourly, daily, weekly, monthly, and annually using performance metrics. The objective and subjective performance metrics you implement are essential to determine what you’re doing right and where you’re going wrong.

Finding the right mix of objective and subjective metrics that support the organization’s mission and strategy, accurately reflect the desired customer experience, and reflect how efficiently you are running your business is a challenge for every contact center leader.

Selecting a limited number of key performance objectives is part of a comprehensive measurement strategy. If you expect your users to pay attention to every statistic the system makes available, they won’t see the connection between the contact center metrics and their daily activities – or know where to focus their efforts. That’s why it’s vital that the leadership team select the key performance indicators (KPIs) that are most important to the contact center, communicate them across all levels of the contact center, then describe how they are measured and what actions impact them. You could structure your KPIs in the following categories:

* **Customer Experience**: Net Promoter Score, Customer Satisfaction, Customer Effort Score, First Contact Resolution, % Abandoned, # of Calls Transferred, Service Level, Average Speed of Answer, etc.
* **Operational Efficiency:** Utilisation, Average Handling Time, Call Wrap-Up Time, Forecast Accuracy, Calls Per Hour, Conversion Rates, etc.
* **People Management:**  Schedule Adherence, Agent Shrinkage, Attrition Rate, Agent Quality, Employee Engagement Score, etc.
	+ 1. Alignment

You can see from the paragraph above that there is a mix of qualitative and quantitative KPIs. The definitions could also vary slightly from organization to organization, but there are few generic guidelines to follow when deciding on your KPIs:

1. Identify KPIs that are in line with your business objectives and corporate strategy.
2. Identify and define the KPIs that will be measured.
3. Decide which data points will contribute to the KPI calculation and how the data will be acquired (for example FCR can be measured via statistic calculation based on repeated calls, or qualitative evaluation based on a survey question)
4. Define each KPI’s purpose and make sure that the purpose is clear to your entire team.
5. Agree the dimensions to measure and the calculation to aggregate the KPIs: contact center, team or individual level
6. Ensure that the KPIs are measuring different domains to gain a more comprehensive view of the performance of your call center.
7. Follow the less is more rule when selecting the KPIs and pay attention on how the KPIs are influencing each other (for example you can decide to invest more in FCR and allow the system to search for the best available agent to handle the request, meaning possible lower SLA and higher AHT, but in the overall calculation gaining efficiency due to less repeated calls and improved revenue for the organization due to increased customer experience)
8. Set a specific, quantitative target, a range or both for each KPI, making sure not to set conflictual targets
9. Define concrete steps that are required to meet each target.
10. Develop a specific action plan if the KPI falls outside of the target or range.
11. Continually review KPIs, interpret the data in a meaningful way and consider causes for any trends or outliers.
12. Optimize the definition of the KPI, refine the data points included in the KPI calculation and select new KPIs to measure in an effort to constantly improve your approach to measuring your call center’s performance.

In an Omnichannel contact center it is even more challenging to manage a consistent Business Score Card, due to different objectives for each channel, that might impact the realisation of objectives on another channel. For example, while the Outbound channel could be interested only in the Conversion Rate and hence generating campaigns to fulfil their objective, which could lead to an unexpected peak of calls in the contact center, hence leading to lower SLA and customer satisfaction. To avoid this it is recommended to have a set of shared KPIs, focused on Customer Experience and cascaded from the senior level to individuals. This could be the Net Promoter Score or other Customer Experience KPI your organization chooses.

* 1. Real-time management

In Realtime management the most important aspect is the schedule adherence. For every contact center agent not in place when scheduled, there’s a huge impact on the Service Level. If an agent is late returning from break or was not there when the shift starts, this puts a big pressure not only on service pressure but also by multiplying the workload of other team members in the shift. There is an indirect relationship between the Service Level and Average Handling Time, if there are no less agents to handle the calls, the Service Level will depreciate and the Handling Time will increase creating a spin effect and depreciating the Service Level even more. The calls tend to take longer because customers are frustrated about the long waiting time and the agents are tired taking calls one after another.

The below is a good example of how powerful each and every contact center agent has and how every time there is a decrease of one Call Center agent (Available Staff column), there is a sharp decline in the service level (SL20 column)

Also notice the Average Speed of Answer (ASA column), that's how long the customer is listening to a machine or to music before an available agent can answer and it went up from 18 seconds to over 3 minutes.

|  |  |  |  |
| --- | --- | --- | --- |
| Workload Hours | Available staff | ASA | SL20 |
| 50 | 55 | 18sec | 75% |
| 50 | 54 | 28sec | 66% |
| 50 | 53 | 46sec | 55% |
| 50 | 52 | 84sec | 40% |
| 50 | 51 | 201sec | 22% |

This concept is called the Power of One and the impact on service depends largely on two factors: the size of the call center, and what the current level of service delivery. Because of the economies of scale of the larger centers, there is greater efficiency in the call handling process, and therefore the impact of one person is not as significant. The other factor that determines the impact on service of any one single person is the level of service currently being provided. The better the existing level of service, the less the impact of one person. This is why in Realtime Management it is crucial to maintain a consistent service across all intervals.

* + 1. Exception handling

With all the prevention in place there are cases when peaks of calls or drop of resources can happen. A fast reaction and means of remediation are key to minimize the damage to the contact center results. What can you do:

1. First of all, understand what is causing the issue (peak of calls due to outage, lack of resources due to train delay, etc.)
2. Add an outage message in the waiting queue
3. Get additional resources to log on the queue (look at scheduled offline activities, like meetings, trainings that can be cancelled, etc.)
4. Ask agents for overtime hours, if possible and allowed by regulations
5. Cancel outbound campaigns or other planned events that could increase the number of calls
6. Evaluate if other channels can take the overflow and direct customers there (stores or online)
7. Finally, look at the routing parameters and see if any changes could improve the call distribution

For all those measure to produce effects immediately, it is required a collaborative approach with the contact center leadership team. Having assigned floor managers that can quickly identify where the issue is and mobilize the resources is key for a quick reaction on unexpected events. Having a routine in place with steps to take in unforeseen situations is also important for the speed of reaction.

1. Processes
	1. ITIL Service Operation

While beyond the scope of this document, Genesys recognizes the value of processes used to manage operation IT services, including Genesys CX Platform. Genesys encourages our customers to adopt and embrace these processes to get most of our technology.

As an industry standard for managing operational aspects of a service, ITIL Service Operation can be recommended.

* 1. Business continuity

It is important to implement a Disaster Recovery Plan within your organization and periodically execute the plan to ensure the Genesys processes will react as expected. Many organizations deploy Genesys High Availability processes which are designed to maintain service in the even an outage occurs (like host machine crash, process fault, etc…).

If you are running in such an environment, it is suggested that periodically (say once a quarter) different scenarios are executed in a controlled environment to determine the effects on the environment. Scenarios should cover some of the following:

* Single Process Outage
* Single Host Machine Outage (where multiple processes are running)
* Multiple Host Outages
* Data Center Outage
* Connectivity Loss

Periodic controlled execution of these test cases will help to identify the following issues:

* Backup processes don’t not have the proper access due to network changes that were previously deployed
* Backup applications having configuration different then the primary process
* Client connectivity not properly implemented to backup process
* Poorly designed routing tables
* Band width concerns at backup process location