



Global Enablement & Learning



Checklist of SAS[®] Platform Administration Tasks

Document Type: Checklist

Date: February 26, 2015

Version: 1.0

Contact Information

Name: David Stern

Title: Senior Technical Architect, SAS Global Enablement & Learning

Phone Number: +44 1628 490851 Cell: +44 7775 754259

E-mail address: David.Stern@sas.com

**THE
POWER
TO KNOW[®]**

1 Introduction

This document contains two lists of tasks, and a schedule for the second list, which you, as an IT administrator or a SAS® administrator, should consider running for the SAS environments you look after. Perform all tasks that are relevant to your environment to keep your SAS platform operating at its best over the long term.

The first list contains tasks which are normally performed as a one-off activity, usually shortly before, while or soon after the SAS platform is installed and deployed. Most of these tasks should be reviewed whenever you make significant changes to your platform (such as adding new hardware or software to it, migrating it, or upgrading the version of SAS or other major components). Significant project work to deliver custom SAS application functionality on your platform will often require these tasks to be repeated or revised.

The second list contains regular tasks, which should be performed regularly at a variety of frequencies, in order to keep your platform healthy, secure and performant.

Some tasks contain additional commentary – and in one cases, for Backup and Recovery, quite substantial extra notes. The checklist intentionally does not contain technical detail of *how* most¹ of the tasks are performed. All these tasks are equally applicable to Windows and UNIX/Linux SAS installations, and most are applicable to z/OS (the exceptions are obvious: those relating to solutions not available on z/OS such as SAS® Visual Analytics).

In the task descriptions, the word *server* always means one or more programs² running on a physical or virtual host machine, rather than to the host machine itself. When talking about the Metadata Server, we mean the process, not the host machine.

1.1 How to use this checklist

Many of the tasks suggested in this checklist will take significant effort to complete. It is not likely that an administrator will simply ‘check them off’ as they go, unless he or she is reviewing the administration framework already in place for an established SAS platform. For this reason (among others) do not leave administration and housekeeping tasks to the end of your implementation project, as an afterthought. Consider every item on this checklist at the beginning of an implementation project, and plan the project to include deliverables

¹ In one task, it contains two additional technical steps to perform after following referenced instructions.

² Sometimes such a program is called a *service* or *process* or even a *daemon*

relating to each task you choose to include, with appropriate timescales, dependencies and resource/effort allocation to ensure they can be completed.

The regular housekeeping tasks in the second list can be used as part of the role and responsibility definition for a SAS administrator or IT administrator. If you are not sure what a SAS administrator does, the second checklist serves as a good starting point for his or her job description, to which duties more unique to your environment can be added. The tasks in the first list stray freely into the areas of enterprise and technical architecture, installation and deployment, implementation and customization. Some tasks may not be the responsibility of a SAS administrator in some organizations, but it's vital for the administrator to know whether and how they have been done by the project implementation team. Some of these tasks have significant overlap with general IT administration and governance.

While this document is presented as a checklist, the checkboxes may be of modest use to you, which is why they are quite small. You may wish to use them to capture your environment's current and planned conformity with the list of completed one-time tasks, and assess your SAS and IT administrator's conformity with the suggested list of regular housekeeping tasks, like this:

Not yet considered Rejected, not applicable To be done Completed satisfactorily, or done regularly

We would welcome comments and feedback of any sort on these task lists. Please contact me directly, or my colleagues in the Global Enablement and Learning team, if you have questions, comments or suggestions for improvement.

1.2 Intended Audience

This checklist is intended for distribution to a wide audience both within and outside SAS. Some of the documents and pages referenced within this document are held on SAS internal systems (such as ToolPool), and will not be accessible to readers outside SAS.

You may share this document with SAS customers, as described in section 1.6 "Permission to share this document".

It is intended for both new and experienced SAS and information technology administrators, and also for experienced SAS technical staff in consulting, architecture, customer support, pre-sales, installation (STIC) and other technical functions. If you feel this document could be enhanced for a particular audience, please contact me with your suggestions.

1.3 Platform Administration training and certification

Consider taking the **SAS Platform Administration** course:

<https://support.sas.com/edu/schedules.html?ctry=us&id=1764>³. To measure your knowledge of SAS platform administration skills with a standard assessment and enhance your résumé, take the SAS Platform Administrator for SAS 9 exam:

<http://support.sas.com/certify/creds/pa.html>.

If your SAS installation includes **SAS® Grid Manager**, consider taking the SAS Grid Manager: Administration course:

<https://support.sas.com/edu/schedules.html?ctry=us&id=1846>⁴.

If your SAS installation includes a distributed **SAS® Visual Analytics** environment, consider taking the SAS Visual Analytics: Administering a Distributed Deployment course:

<https://support.sas.com/edu/schedules.html?ctry=us&id=1989>⁵.

1.4 Applicability to SAS versions

At the time this document was published, the current publically available version of SAS is second maintenance release of SAS® 9.4 (sometimes written as SAS 9.4 M2), which shipped in August 2014. The authors intend that all of the guidance in this note is relevant to any version of SAS® 9, where the products concerned existed. We expect all of the guidance in this document will remain correct for the third maintenance release of SAS 9.4. However, we can take no liability for errors or omissions in the content, which is written based on individual consultant's field experience and shared here in good faith that it is correct.

1.5 Applicability to SAS solutions and products

The checklists in this document are focused on administration of the SAS® Intelligence Platform, and include tasks specifically for SAS Grid Manager and SAS Visual Analytics. At present, it does not contain advice for other SAS solutions. Since many SAS implementations to include an industry-specific or analytically-focused SAS solution, I would encourage you to discuss the specific platform administration tasks you should perform for that solution with your implementation team, or with your SAS account manager who can refer you to appropriate expert support.

³ This link is for the US class schedule; use the dropdown on that page to select your country.

⁴ Ditto

⁵ Ditto

1.6 Permission to share this document

SAS Institute Inc. (“SAS”) allows any person obtaining a copy of this document to use, copy, modify, merge, publish, distribute and share this document, on the basis that this document and its contents are provided "as is" without warranties of any kind whatsoever.

This document does not form part of any agreement between you and SAS (or any SAS companies or affiliates) and neither the authors or copyright holders of this document shall be liable for any claim, damages or other liability whatsoever arising from the use or other dealings with this document.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2015 SAS Institute Inc. Cary, NC, USA. All rights reserved.

2 Checklists

2.1 One-time Task Checklist

Tasks 1 to 34 in the checklist are larger tasks, which you should consider performing once, but should revisit if major elements of the SAS platform, or the business requirements change. Tasks in this section do not need to be repeated on a regular, scheduled basis.

Task	When
<p>1 <input type="checkbox"/> Ensure you can identify the components of SAS and third party software which make up the SAS platform, and on which hosts they run, and ensure that you have a basic awareness of what each component does.</p> <p>If you don't already have one, create a shared location where all relevant documentation describing your SAS platform can be stored, for use by all SAS or IT administrators, and project delivery staff working on the SAS environments in your organization. Use this location to store up-to-date architecture documents (including the document known as a D30_ArchitecturePlan in the SAS Intelligent Platform Implementation methodology, if one was created for your deployment of SAS), installation checklists, post-installation documents, security models, log locations, this administration checklist and other documentation describing the structure and operation of your SAS platform.</p> <p>Administrators are encouraged to maintain bookmarks in their preferred web browser to online versions of the SAS System Administration Guide, SAS Security Admin Guide, etc. for the versions of SAS which they support, on the support.sas.com website.</p> <p>Discover what SAS software components are installed on a particular host machine in the Deployment Summary (<i>SAS-installation-directory/InstallMisc/InstallLogs</i>), or in the Deployment Registry Report (see http://support.sas.com/kb/35/968.html).</p>	After platform changes
<p>2 <input type="checkbox"/> For enterprise-scale deployments, define a Service Level Agreement stating the measures you will use for service level monitoring and reporting, and how they will be calculated. Implement a service level reporting product to calculate these measures when based on time-history data from a service level monitoring component.</p> <p>Consider measuring service level performance for the system as a whole, and for specific subsystems which can operate independently.</p> <p>Measure the service level performance using metrics such as: availability (over specific periods of time), duration of each period of unavailability which is considered an outage, duration of planned outages, mean time between unplanned outages, actual recovery time from unplanned</p>	Outline pre-install, review and adjust post-install

outages vs recovery time objective, when recovery is successfully achieved to a point within the stated in the recovery point objectives vs when you are forced to recover to an earlier recovery point due to eg corrupt backups etc.

3 **Write and maintain a Security Policy** which covers the SAS platform.

Before and/or after platform changes

Most organizations will have a wider Security Policy in place. We recommend you include section within that, or a separate document to define policies specific to the SAS platform.

This should preferably be defined with the assistance of an experienced SAS architect *before* SAS software is installed, since the installation process involves making a number of decisions relating to security regarding features which are much likely to be disruptive if applied during or immediately after installation than if applied retrospectively. The Security Policy should be periodically reviewed and revised as necessary throughout the lifetime of the platform.

The Security Policy should cover such things as:

- How users of the SAS platform will be authenticated
 - From SAS® 9.3 and later, the SAS® Metadata Server typically uses a small number of SAS internal accounts, which are authenticated by the Metadata Server and do not need to exist outside it
 - All other accounts, both those for real people and those for batch and service accounts, are recognized by the Metadata Server, but are authenticated by the local operating system, usually using a directory server. Many other options are possible for authentication in SAS – consult with SAS pre-sales or post-sale architects on this advanced topic.
- Authorization (access rights and permissions) in SAS, any databases accessed via SAS, and for OS-managed assets (eg files and directories on the filesystem) used by SAS, at a high level. Detailed authorization design is addressed in the next task, by the Security Model.
- Encryption of content at rest (eg data, files, code, passwords and datasets stored on disk, data stored in databases)
- Encryption of data in motion (eg data, credential and message transmission using SAS/SECURE™ software or Transport Layer Security).
- Standards of encryption and the management, complexity, reuse, protection and lifespan of cryptographic keys, passwords etc.
- Protection of system integrity (including physical security, availability, backup and recovery objectives, security of power, cooling etc)

- 4 **Write and maintain a Security Model** which implements certain requirements of your Security Policy, and describes how users should be organized into groups, for the purposes of managing their access to resources such as metadata, data and application functionality. Define also how users and groups will be added to, updated in and removed from the SAS platform.

Before and/or after platform changes, and in tandem with organizational changes in the business

Define what operating-specific settings and rights are required for users of the SAS platform, and whether any specific password management policies should apply (complexity, lifetime etc).

These are the major components of a Security Model for the platform. You should maintain two documents of your Security Model: a relatively static document which defines the overall principals and guidelines for how users are managed and granted/denied permissions, but which avoids user-specific detail, and a more frequently-changing 'living document' part which records the specific state in which users and groups (within the context of the SAS platform) should be at the present time.

Many organizations implement scripts to automate the process of creating, modifying and removing users and groups in the SAS platform (primarily SAS Metadata Identities, but this sometimes also includes accounts in other platform components such as a scheduling tool or database), to keep them synchronized with users and groups in an external LDAP directory server such as Active Directory. For guidance in doing this, see the SAS® 9.4 Intelligence Platform: Security Administration Guide, especially the Appendix on User Import Macros, at <http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/n012hp5m00a1z2n1b598q4pknfih.htm>. Similar sections can be found in the Security Administration Guide for earlier releases of SAS.

If you have SAS Visual Analytics, create a SAS LASR™ Administrator (lasradm) user, as described in step 32 below, to differentiate the administration role for Visual Analytics from the SAS Administrator user used to manage the rest of the SAS platform.

- 5 **Secure the SAS platform on the filesystem** to prevent inappropriate read and write access.

Post-install, and after platform changes

Ensure that users who are not administrators, installers or appropriate types of developer do not have access they do not require to resources on the filesystem which contain sensitive information, or access to change resources such as configuration files and scripts which are crucial to the integrity and stability of the SAS platform.

These resources include metadata repository data sets (files inside the Repository folder under Metadata Server), SAS and other configuration files, server startup, shutdown and status scripts, and server logs.

Ordinary users should not be able to alter these.

However, note that some processes both execute as, and write log files as the user, eg SAS Workspace Server sessions write workspace server logs as the user, so users require write access to the workspace server log directory in order to be able to use the workspace server.

6 **Maintain a secure, encrypted password-protected password database, using an appropriate software tool.**

KeyPass is popular, good, free and open-source choice. Other password database tools are available.

Maintain the passwords in this database for batch and administrative accounts, external database outbound logins etc.

Keep the password database on a machine which is physically better protected than a desktop or laptop PC (ie store the database on a host in the datacenter), so that it cannot easily be stolen.

Consider implementing two-factor authentication for access to the hosts in the datacenter on which the password database is stored.

Post-install, after platform changes and when any 'shared' or 'headless' account's password changes

7 **If you store any passwords for outbound logins in metadata, establish a procedure to ensure that they are changed whenever the passwords are changed in the external system.**

This is most commonly a consideration for database passwords. It is a good practice for database passwords to be very tightly guarded, known only to a limited group of administrators. These administrators should be shown how to log in to SAS® Management Console and change the password in an outbound login, as an alternative to having them share the password with a SAS administrator.

The need to change passwords in databases, especially for service or shared credentials, may naturally conflict with your desire to protect the SAS system's stability. However, if service or shared account passwords must be changed regularly to meet the requirements of the security policy, please maintain a documented procedure to follow in order to change those passwords. Assuming your development, test and pre-live environments reflect the configuration of your production environment, then you should rehearse your password update procedure in those environments, to establish a reasonable level of confidence that the procedure is correct and that it will work well when applied to your production environment.

When passwords in external system change

8 **Ensure that you know how to change the passwords for SAS internal accounts, in case they are compromised.**

Also, periodically update internal account passwords, and the passphrase used to encrypt stored passwords.

In the SAS® 9.4 Intelligence Platform: Security Administration Guide, Second Edition, or a more recent equivalent, see:

- "Update a Managed Password",

After platform changes
See regular task 35

<http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#p0kb2gtuynjrn1hduu5by88u4f.htm>

- “How to Re-Encrypt Stored Passwords”,
<http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#n1p18cmmqzjwpin19f7mbu9yrx0f.htm>

9 **Ensure you know how to check the status of all the SAS and third party servers, ad hoc at any time.**

For this task you may use a combination of tools, including third party monitoring tools, and SAS® Environment Manager or the SAS® Audit, Performance and Measurement Package.

After platform changes
See regular task 36

10 **Ensure you know how to start and stop (and in some cases, how to pause, resume and refresh) all the SAS and third party servers** which make up the complete SAS platform, on every host on which they run, and you know how to do so in an appropriate order.

Where appropriate, use scripts or some other network service administration tool to ensure the correct startup and shutdown sequence of the SAS and third party servers which make up the whole platform.

Make sure that the relevant SAS platform services are configured to be started automatically as the server starts up.

If you work for SAS (and thus have access to SAS’s ToolPool database) and are configuring a SAS 9.4 environment, you should consider using the GEL Startup/Shutdown framework (<http://sww.sas.com/tp-bin/tplog?L05930>). This well-documented framework contains scripts to manage coordinated startup and shutdown of SAS servers, spawners and the Environment Manager and Deployment Agents, across multi-machine SAS deployments. It will manage startup and shutdown of SAS® Grid Computing nodes and SAS Visual Analytics distributed environments, and including the SAS mid-tiers and clustered metadata servers, all in the correct order, for a variety of multi-machine server topologies on all our supported operating systems.

After platform changes

11 **Set up automated monitoring to regularly (per a schedule) check the status of SAS and third party servers**, using a SAS-provided tool (such as SAS Environment Manager), third-party monitoring tool, your own custom built tool, or a combination of these.

Based on these status checks record measurements which allow you to calculate and keep a history of key metrics over time such as availability (several definitions exist: select one or more specific definitions), mean time to failure, mean time to repair, administrative, planned and unplanned downtime etc. Track these metrics at the individual component, subsystem and overall system level.

SAS Environment Manager, available with SAS 9.4 as part of the middle-tier, is a web-based administration solution for a SAS environment. The

Post-install, after platform changes

See also one-time task 9 and regular task 36

application can administer, monitor, and manage SAS resources, including administering the SAS® Web Application Server and monitoring SAS foundation servers. The application collects and charts data on metrics for monitored resources, providing a comprehensive view of resource health and operation. More information about SAS Environment Manager can be found at

<http://support.sas.com/software/products/sev/index.html>.

For earlier versions of SAS, consider deploying and using the SAS Audit, Performance and Measurement Package, which is deprecated for SAS 9.4 and later. See <http://support.sas.com/rnd/emi/APM94/index.html> to learn whether it would be of use in your environment.

- 12** **Set up automated monitoring to regularly (per a schedule) check free and used disk space, memory usage, network and disk usage on each host.** Post-install, after platform changes

Keep a history of these metrics for a rolling period of eg 30 days, to allow trends to be identified.

See also regular tasks 37 and 38

- 13** **Set up alerts to raise an alarm if a SAS or third party service stops running or responding for longer than an acceptable amount of time, per the SLA. Similarly set up alerts for low disk space, high memory usage, high CPU usage for extended periods, specific error messages in log files etc.** Post-install

It will likely take some time for you to determine which metrics are most worthwhile setting alerts on, and at what thresholds, and whether raise an alert immediately, or after having detected an exceptional value for what period of time. Similarly, it will take some time to learn what error messages in log files should trigger alerts.

Ideally, configure the ability to define periods of planned downtime in the alerting system's configuration interface both ad-hoc, and scheduled in advance, to suppress false-positive alerts during planned and administrative downtime.

- 14** **Define a backup and recovery strategy.** After platform changes

This should describe which components of the SAS platform should be backed up, how frequently, and for how long the backups should be retained in what locations. This seemingly simple task can be extremely complex for a distributed multi-machine SAS implementation, and the administrator should bear the following notes in mind while designing and revising this strategy.

Of importance equal to the backup process, define how you will recover the system from an outage. How will you restore eg accidentally deleted data, or restore service to the business using a substitute system in the event of a disaster, using the backups, both to test the integrity of the

backups and the recovery procedure, and in the event of a real outage. If the recovery procedure involves taking backups at intermediate stages, ensure those backups cannot overwrite existing 'good' backups.

Note that it is not generally possible (or is at least not trivial) to restore a SAS backup to another server, due to the presence of many internal identifiers and links between system components, eg hostnames of servers stored in metadata. (Utilities do exist for updating the hostnames in metadata, but they can require expert skills to apply completely successfully, and depend to some extent on how hostnames have been entered – eg hostname only or FQDN). A full disaster recovery strategy is required to provide this capability, and such a strategy is beyond the scope of the basic administration checklist given here.

Be aware that some SAS components (eg such as the Metadata Server, the contents of certain data and configuration directories on each server, the SAS® Content Server, and the SAS® Web Infrastructure Platform Database) must all be backed up synchronously (ie at the same time, to create a consistent recovery point). When these backups are restored, they must all be restored to the same recovery point, in order for integrity of references between the restored components to be maintained. This requires tight coordination of backups across multiple physical hosts, since these components are usually distributed across different hosts. The [SAS Deployment Backup and Recovery Tool](#), supports automated backup and recovery across a distributed deployment for SAS 9.4 multi-machine platforms.

Be aware that for a SAS platform, using incremental backups for components where possible (typically filesystem and third party database backups) is efficient and uses less space when the incremental backup for that component is taken at a given recovery point. However, the process of restoring the system to that recovery point is more involved, as a full backup for the component must be restored first, and then all the incremental backups between the full backup and the desired recovery point must also be restored. This tends to increase the recovery time; the time taken to complete the restoration process. If using incremental backups for some components helps you meet your system availability targets (so that the system is unavailable for batch and interactive use for a shorter time each day) and recovery point objective targets (so that you can take more frequent backups, and the most-recent backup is typically more recent), make sure it doesn't prevent you meeting your recovery time objective targets (the amount of time you are without a working system while you recover from the backup). Taking an incremental backup every hour instead of once a day might seem attractive, but not if it means it will take you a week to restore from those backups instead of a day.

More complex or demanding requirements defined in your backup strategy may lead to a plan for handling backups in which backed-up files are eg:

- kept on-site for a period of eg 1 week to allow rapid restoration of

recently-lost work files to a recovery point no older than ~2 days ago, then

- moved off-site to expensive highly-secure storage for eg 4 weeks to allow recovery to a point between 1 week and 4 weeks ago in event of a major disaster (eg total loss of hosting site), and then
- moved back on-site for a period between eg a further 5 months and several years, in order to maintain an archive for regulatory or audit purposes
- some backup data may need to be stored separately, in such a way that allows it to be destroyed permanently in the event that you are no longer authorized to hold it, eg if the customer who ultimately owns the data ceases to allow you to hold it as a result of their terminating a services contract with your company. You should aim to avoid being in a position in which you are obliged to destroy *all* historic backups of your SAS environment because you are no longer authorized to hold some part of the data they contain.

Obviously the schedule above is just an example; your organization's IT system administrators are responsible for designing an appropriate schedule for handling backup files which meets the business's objectives for resilience and cost. The point here is that enterprise-scale backup and recovery is a complex subject which requires expert attention from both the SAS platform administrators, and the wider IT functions in a business.

The backup regime described above is well suited to restoring the entire SAS platform following a major incident. Consider also regularly exporting SAS Package Files (.spk) containing selected metadata objects – eg the jobs, deployed jobs, flows, tables, libraries, transforms, stored processes and other similar assets used to create your custom applications in the SAS platform, and backing up the SAS Package files so produced in your filesystem backup. Keep a history of eg 2 weeks' worth of daily backups of these files. This will create the opportunity for you to restore individual metadata assets (jobs, flows, tables, libraries, transforms etc) which are later reported to have been inadvertently changed or deleted, without having to commit to restoring the entire platform to an earlier state, and losing everything else you have done to the platform since that point. This extends the ways in which you can restore from a backup, beyond being an all-or-nothing operation.

Maintain a compact and ordered metadata repository by including the 'reorganize' step in the weekly or daily metadata backup.

15 **Record the filesystem location of all the SAS and third-party product log files, and keep this record up to date.**

After platform changes

It is not unusual for SAS platform customization work to result in the location of log files being changed. There are two common patterns, and some combination of the two is occasionally seen:

- Log files for each SAS server are kept in a log directory

underneath the SAS Server's configuration directory

- Log files for all SAS servers are kept in a single common directory

Log files for third-party products are usually written somewhere within the directory structure for the individual product. The person who performed the installation or the product's documentation should be able to direct you to them.

16 Implement one or more scripts to archive and delete log files.

After platform changes

For example, you may wish to clear down log files older than eg 30 days, and run the script daily.

See regular task 49

Most SAS servers, especially at the more recent versions of SAS 9 are configured for automatic daily log rotation – they create a new log file each day, while continuing to run. Some servers (such as the SAS/CONNECT® server) don't support automatic log rotation, and instead have just one log file which they keep open and keep appending to, the entire time they are running. If you have such servers as part of your SAS installation, identify or create a script or task which will restart them, causing the log file to be rotated.

17 Set up log syndication, parsing and interpretation using a SAS-provided or third party system monitoring tool, your own custom built tool, or some combination of these, to capture and keep a historical record of significant events.

After platform changes

One useful event worth scanning SAS logs for, and raising an alert when it occurs, is notices in logs about upcoming expiry of a SAS or third-party component license. Even the healthiest SAS platform will need a new license to be applied from time to time, usually once a year. As discussed in item 30 below, it is possible for the licenses of different components in your SAS platform to expire on different dates.

See regular task 50

We sometimes see SAS platforms where much of the system's total processing is done in batch, and because no-one normally needs to look at the SAS logs, the license can expire before anyone notices there had been warning and grace period notes in the logs for some weeks.

Two of the most useful logs to scan are the Object Spawner and Metadata Server logs. Look in the Metadata Server logs for messages indicating successful and failed backups – eg you should raise an alert for a failed metadata server backup.

You should also scan the logs of third party products for warnings and errors. Scan the logs created by Platform Suite for SAS components, and by the SAS® Web Server acting as a reverse proxy. Both of these product's logs can contain highly useful and important messages which require remedial or preventative action.

18 Consider adding user and network application audit reports, to see what users and applications are

Post-install
See regular

connecting to the system, and to look for connections from users or applications that should not be connecting. task 41

Similarly, look for accounts in SAS Metadata who have not connected to the system recently. After a period of inactivity, consider adding those users to a Dormant group in metadata, to restrict their access to the system. If they remain inactive, remove or disable the unused accounts.

19 **Ensure that all SAS platform administration staff are familiar with how to contact SAS Customer Support (aka SAS Technical Support) for help.**

Post-install, and after platform or organizational changes

SAS Customer Support can be contacted by email, phone or online, and you should ensure you know which local support office to call – usually one in your country if there is one. The first-line customer support consultant will ask you for some basic information during the initial conversation, including information about the SAS platform (eg its site number, from which they can look up the operating system, and the SAS software licensed for that site) and your contact details. Many organizations have multiple SAS platforms or environments, and it is common for these to have different site numbers: do not assume the site number from one of your environments is shared by another of your environments.

SAS Customer Support representatives will also often ask to see log files from servers, so knowing where to find these logs simplifies the process of raising the issue.

In certain situations, other departments within SAS Professional Services may be better able to assist you than SAS Customer Support. Eg consider engaging SAS Professional Services consultants or technical architects if you are planning a new installation, a hardware or software upgrade or a migration. Contact your usual SAS account representative, or SAS sales representative in your country if you are interested in using or trying additional SAS software.

Also, ensure that all SAS platform administration staff are familiar with the content of your shared repository of documentation for the SAS platforms they support, as discussed in step 1.

20 **Establish a means for keeping up-to-date with SAS maintenance releases, hotfixes, announcements and support notes.**

After platform changes
See regular task 51

SAS maintains several mailing lists to which you can subscribe to be notified of important technical announcements, including maintenance releases and hotfixes. The main list is called TSNEWS-L. Details of how to subscribe, as well as how to find and install hotfixes are available from the SAS Technical Support Hot Fixes page:

<http://ftp.sas.com/techsup/download/hotfix/hotfix.html>

You can learn more about the excellent SAS Hot Fix Analysis, Download and Deployment (SASHFADD) tool from a link on that page.

The Deployment Summary (*SAS-installation-directory/InstallMisc/InstallLogs*), and the Deployment Registry Report (see <http://support.sas.com/kb/35/968.html>) are good ways to see what SAS software is installed on each host machine, at what version.

- | | | |
|-----------------------------|---|--|
| 21 <input type="checkbox"/> | Familiarize yourself with the utility to clean up abandoned SASWORK directories left behind by abruptly-terminated SAS workspace sessions.

You may use the SAS Cleanwork Utility for Unix or SAS Disk Cleanup Handler for Windows to perform this task. | Post-install
See also one-time task 29 and regular task 46 |
| 22 <input type="checkbox"/> | If you have SAS® Scalable Performance Data Server, write and test a script to delete old SPDS work tables. | Post-install, or after platform changes to SPDS server components
See regular task 47 |
| 23 <input type="checkbox"/> | Ensure you know how to promote metadata content between SAS environments , eg as part of a release management process.

Release management specifically, and configuration management more generally are complex topics, closely related to SAS platform administration. They are managed in a variety of ways according to customer preference, project size, and system complexity. Ensure you know what role you will perform in any release management and change management processes, and ensure you know how to perform it. | After platform changes |
| 24 <input type="checkbox"/> | If you have SAS Visual Analytics, set up Autoload to automatically load tables into SAS Visual Analytics when it start, and to refresh them periodically while it is running.

Maintain the latest version of the tables you wish to be loaded automatically into SAS Visual Analytics in the AutoLoad folder, schedule the SAS Visual Analytics Administrator's AutoLoad.sas agent to run eg every 15 minutes, which will load data into the public LASR server and periodically refresh it. | After platform changes affecting SAS Visual Analytics
See regular task 53 |
| 25 <input type="checkbox"/> | If you have SAS Visual Analytics 7.1 or later, enable Visual Analytics Audit Reporting.

Visual Analytics 7.1 introduced a new capability to audit user and table activity and provide near real time reporting for this data. This feature is not turned on by default. A pre-defined library and table are automatically configured as the source for reporting. SAS Environment Manager | After platform changes affecting SAS Visual Analytics |

records this data and the Autoload process collects the data and loads it into the Environment Manager Autoload library. Standard reports are then available to report on the recorded activity.

This blog post on SAS Communities explains how to enable Audit Reporting: <https://communities.sas.com/docs/DOC-10094>.

See regular task 53

26 **Tune your SAS Web Application Server middle-tier performance**, to optimize Visual Analytics web application server startup time and run-time performance.

In particular, consider optimizing the values for the size of memory used by each Java Virtual Machine (JVM) in your configuration, using the -Xms, -Xmx, -XX:PermSize and -XXMaxPermSize options in the JVM configuration file. Your SAS consultant should be able to help guide you in choosing appropriate values for single-JVM and multiple-JVM configurations of different sizes of SAS Visual Analytics deployment, for example. SAS employees can refer to http://www.sas.com/toolpool/pool/Visual_Analytics_7.1-Recommended_Post-Install_Activities/index.html, or search for more recent equivalents for later versions of SAS Visual Analytics in our internal ToolPool system for suggested values.

For all readers, see “[SAS® 9.4 Web Applications Tuning for Performance and Scalability](#)”.

Post-install, or after platform changes affecting SAS Visual Analytics

27 **If you have SAS Visual Analytics, relocate SAS® LASR Analytics Server signature and log files.**

LASR signature files are created when a LASR server is started and additional files are created for each table that is loaded into memory. The default location for LASR signature files is in the Linux temporary files directory, /tmp. This location may not be ideal for some customers as they may have cleanup tasks that remove files resulting in a LASR failure or because they are “exposed” for everyone to see. As a result relocating the LASR signature and log files may reduce the risk of LASR failures. Relocating these directories underneath the configuration directory will cause the signature and log files to be backed up along with the remaining configuration files when performing a full backup.

The following are suggested locations for signature and log files. Permissions for the “LASR” directory and sub-directories should be set to 777 to ensure LASR administrator accounts can create directories and files used in managing LASR signature files.

```
<SAS_CONFIG_ROOT>/Lev1/Applications/SASVisualAnalytics/LASR/Signatures
```

```
<SAS_CONFIG_ROOT>/Lev1/Applications/SASVisualAnalytics/LASR/Logs
```

SAS employees can refer to http://www.sas.com/toolpool/pool/Visual_Analytics_7.1-Recommended_Post-Install_Activities/index.html for more detailed guidance.

Post-install, or after platform changes affecting SAS Visual Analytics

28 **If you have SAS Visual Analytics, reconfigure it to use**

Post-install, or

an Application Server Context other than SASApp.

There are situations when it is advantageous to have a dedicated Application Server context for VA. For example, when VA is deployed alongside other SAS software, such as SAS® Enterprise BI Server, it's a good idea to let Enterprise BI Server use SASApp, and to reconfigure Visual Analytics to use an alternate context, like SASAppVA. Note that this context could point to resources on the same machine as SASApp, or to a totally different machine.

To make this change, follow the instructions in <http://supportprod.unx.sas.com/fusionpreview/previewhtml/52/135.html>. Note that for a Non-Distributed LASR server, it will be critical to set the memsize value to 0 for the Workspace Server and the Batch Server. You must also change the metadata permissions to allow only the LASR Administrator user (lasradm, and other LASR administration accounts) to use the new SASAppVA application server context. Deny "Read Metadata" to other users to prevent them from using it. Then change the default context for the workspace server to SASAppVA using SAS Management Console > Plug-ins > Application Management > Configuration Manager > SAS Application Infrastructure > Visual Analytics 7.1 properties, to set `va.defaultWorkspaceServer = SASAppVA`. If in doubt about how to apply or validate these changes, please contact SAS Customer Support or seek assistance from SAS Professional Services.

after platform changes affecting SAS Visual Analytics

29 Set the default location for the SAS Work directory on SAS compute servers to a more appropriate filesystem location than the default.

On Linux the SAS WORK library is assigned to /tmp by default. On Windows it defaults to the user's home directory. SAS users can write these locations by default on almost every host filesystem, which is why they were chosen, but in many cases they are far from ideal. These locations may not contain enough free space to accommodate multiple large temporary files and running out of space may result in SAS task failure or possibly system failure. In addition some sites may have cleanup tasks that periodically remove files from the /tmp file system. Therefore we recommend that the SAS Work location be assigned to a file system dedicated for SAS temporary files, and that the utilities mentioned in step 21 above are used to periodically delete old abandoned work files, usually left behind when SAS does not delete them itself, eg because it exits abruptly.

During installation or post-install
See also one-time task 21

30 Learn and document how to apply updated licenses to SAS and third party components used in the SAS platform.

You can find guidance specific to your version of SAS and your specific SAS and third-party products at <http://support.sas.com/techsup/license/>. Platform Suite for SAS is typically licensed annually, but as it comes from

After platform changes
See regular task 54

another vendor, it is controlled using a separate license to that used by SAS. For a variety of possible reasons, it may not always issue license expiry warnings in the logs, or actually expire, on the same dates as your main SAS licenses.

There are many circumstances in which licenses may NOT follow a regular pattern of being applied annually on the same date. The licensed components in your system may not have all been bought at the same time. Be familiar with the validity dates of all the SAS and third-party licenses which are initially applied to the platform, and keep a precise record over time detailing of the dates for every replacement license, however temporary. Implement some means of reminding yourself when you need to obtain a new license. Be aware license requests to SAS may have a multiple-day turnaround time, and if there is any discussion required, determining what replacement license to issue can take longer. Request new licenses plenty of time (I suggest at least 1-2 weeks) ahead of when you will need them.

- 31** **If necessary, ensure you know how to obtain or create new SSL certificates for your SAS platform.** Then ensure you know how to apply them to any servers which are configured to require them. After platform changes

Use of Secure Sockets Layer (SSL) to encrypt data in transit may be required by the Security Policy (see one-time task 3) and should be described in the Security Model documentation (see one-time task 4).

Record who signed each certificate, on what date, and when they expire, in a place where other administrators in your organization can find that record. You may require this information again when you obtain a renewed or replacement SSL certificate.

Set a reminder for yourself (or another administrator) in your diary to obtain or create new SSL certificates when the existing ones are about to expire, and to then update the servers with the new certificates. Certificates are typically valid for 1 or 2 years, but may be valid for another duration.

- 32** **If you have SAS Visual Analytics, create a LASR Administrator user (username: 'lasradm') on the operating system, and in metadata.** Post-install, or after platform changes affecting SAS Visual Analytics or SAS LASR Analytics Servers

Consider whether to enable guest access to SAS Visual Analytics, by enabling the Anonymous Web Access and the SAS Anonymous Web User internal account (called webanon@saspw by default).

Create a LASR Administrator (lasradm) user, to differentiate the administration role for Visual Analytics from the SAS Administrator user used to manage the rest of the SAS platform. This user should have an account which can be authenticated in operating system of each machine hosting a LASR server. It requires SSH keys to be created and shared to allow it password-less SSH between all LASR nodes. Also

create this user in metadata, and make it a member of the following groups: Management Console: Advanced, Visual Analytics Data Administrators, Visual Data Builder Administrator. Test that it works by connecting to the SAS Visual Analytics Hub, and starting a LASR Analytic Server on one host. The server should start successfully. Please contact SAS Customer Support if you require assistance in applying or testing this.

33 If you have SAS® Grid Manager, ensure you are familiar with Grid management administration tasks.

You should familiarize yourself with administration of SAS Grid Manager components, including the grid monitoring plug-ins in SAS Management Console, Platform Enterprise Grid Orchestrator (EGO), and Platform RTM for SAS. Learn how to query the status of grid queues, hosts, and jobs from the command line as well as in Platform RTM.

Ensure you understand the concepts of scheduling and managing workload on a grid, including defining and managing job queues, job and queue priorities, submitting and killing grid jobs, and in administering grid-enabled SAS workspace sessions. Seek some training – whether informal or formal – on identifying and troubleshooting a SAS Grid environment.

These skills will enable you to how understand and manage horizontally-scaled distributed computing on your SAS Grid, and how to keep the several interrelated components of the Grid working well.

SAS offers the SAS Grid Manager: Administration course: <https://support.sas.com/edu/schedules.html?ctry=us&id=1846>.

Post-install, or after platform changes affecting SAS Grid Manager and grid nodes
See regular task 56

34 Design and maintain a schedule of SAS platform administration housekeeping activities, to specify when regular tasks should be performed.

The next section suggests what those regular, housekeeping tasks should be, and the section after that suggests a frequency to run each of those tasks.

After platform changes

2.2 Regular Task Checklist

Tasks 35 to 56 in the checklist are run more frequently, ad-hoc as required or as specified in the schedule of housekeeping tasks you created in task 34.

Task	When
35 <input type="checkbox"/> Change the passwords for SAS internal accounts, and update the passphrase to re-encrypt stored passwords.	Regularly, per housekeeping schedule See also one-time task 8

36	<input type="checkbox"/>	Check the status of SAS servers, to see if they are running and responding.	Regularly, per housekeeping schedule See also one-time tasks 9 and 12
37	<input type="checkbox"/>	Monitor disk space, especially the disk space used for SASWORK and for permanent SAS libraries.	Regularly, per housekeeping schedule
38	<input type="checkbox"/>	Monitor memory usage, CPU usage, network IO usage, disk throughput usage eg input/output operations per second (IOPS) Take measurements regularly (eg every 5 minutes) and maintain a time history of these measures for eg 30 days. Analysis of the time history is usually more insightful than a single point measurement.	Regularly, per housekeeping schedule
39	<input type="checkbox"/>	For systems accessed via a Terminal Server or Citrix server (eg those hosted by SAS® Solutions OnDemand), monitor and regularly check terminal server sessions' memory usage. User sessions can become unresponsive or slow if the terminal server runs out of memory and has to begin paging to disk. If this happens regularly, consider adding more memory, or more terminal servers.	Regularly, per housekeeping schedule
40	<input type="checkbox"/>	If you use a job scheduler (eg Platform Suite for SAS, also known as Platform LSF & Platform PM), inspect the state of all job flows, both currently running and recently ended. Note which job flows are on hold (disabled). Note which job flows are running, which runs have failed with an error, and which have completed successfully. The specific things to look for are unique to each SAS installation. Consult with colleagues who maintain the job flows if you need help in determining whether the state of current and recent job flows is subjectively 'good' or 'bad', 'busy' or 'quiet' etc. Be especially sensitive to job flows which run much longer than usual (even if only in rare or error conditions), or flows which are triggered regularly (eg daily, or hourly) and which run for so long that they could be triggered to run again while the earlier instance is still running. If the application logic in these flows is designed to allow two copies of the same flow to run simultaneously without adverse impact, this may not be a problem, but in our experience it is not very common for SAS developers to consider designing job flows so as to intentionally allow	Regularly, per housekeeping schedule

multiple instances to run simultaneously. You can schedule flows in Flow Manager so that only one instance can run at a time, preventing a second instance from starting even though the triggering conditions are met.

41 **Run user and network application audit reports, to see what users and applications are connecting to the system, and to look for connections from users or applications that should not be connecting.** Regularly, per housekeeping schedule
See one-time task 18

42 **Monitor the performance of jobs and queries running on the system – this includes interactive jobs and user workload as well as batch job flows.** Regularly, per housekeeping schedule

Identify the top 10 worst performing jobs and/or database queries every day/week/month, and investigate whether they can be made more performant. This is an effective way to identify and efficiently remediate the causes of poor-performing systems.

SAS Environment Manager, available for SAS 9.4, provides a convenient administration and monitoring interface for your system, though it does not currently show historical performance data.

Platform Flow Manager is the main client interface in the Platform Suite for SAS, used for monitoring scheduled and ad-hoc job flows.

If your SAS applications or solutions push query processing down into a database, either using in-database technologies or explicit SQL pass-through, you should work with the database administrators to review the queries and their performance. Study things such as explain plans in the database to identify opportunities to optimize their performance.

43 **Execute backups regularly as specified in your backup strategy, as part of your housekeeping schedule.** Regularly, per housekeeping schedule

Development and Test environments may be sufficiently valuable that you must back them up with as much care as you back up Production.

Also your backup and restore procedures may be developed, tested, and refined more safely in Dev and Test than they are in Prod.

And you should consider keeping Dev and Test as much like Prod as is reasonable, including backing them up (with the inherent service and performance impacts that go with running a distributed backup process), so that you experience how the live backup strategy impacts your application in Dev and Test before you see the impact in Prod.

Also, before and after any platform changes are made

44 **Periodically test the process to restore from backups.** Regularly, per housekeeping schedule

Backups which cannot be successfully restored to recover a fully working platform are arguably more harmful to the overall wellbeing of your system than taking no backups at all. You must test backups, and rehearse the procedure defined in the backup and recovery strategy to restore them.

Plan for at least 3 types of restoration:

- Restore a few files, datasets etc, which were eg changed or deleted by mistake, from a specific backup, but do NOT otherwise restore the rest of the system to an earlier state
- Restore the entire system to an earlier state at a specific recovery point, on the existing hardware
- Restore the entire system to a specific recovery point, on different hardware: such disaster recovery is a large subject in itself and is beyond the scope of this basic platform administration checklist. It is generally not so very different for SAS platforms than for other large and complex IT systems, and the design and operation of a Disaster Recovery capability for your SAS systems, and for other systems on which you rely, should be included in your organization's business continuity plans.

45 <input type="checkbox"/>	Check for long-running SAS sessions which may be 'rogue', orphaned, abandoned and otherwise no longer connected to a user session of batch process.	Regularly, per housekeeping schedule
<p>Check also for Enterprise Guide sessions which users have left running overnight, locking SAS tables. These sessions can interfere with the nightly back processes.</p> <p>Both these tasks can be (and have been at many customer sites) successfully scripted. Your SAS consultants can help you find and adapt such scripts in your environment.</p>		
46 <input type="checkbox"/>	Run the utility to clean up abandoned SASWORK directories left behind by abruptly-terminated SAS workspace sessions.	Regularly, per housekeeping schedule
<p>You may use the SAS Cleanwork Utility for Unix or SAS Disk Cleanup Handler for Windows to perform this task.</p>		See one-time task 21
47 <input type="checkbox"/>	If you have SAS Scalable Performance Data Server, run your script to delete old SPDS work tables.	Regularly, per housekeeping schedule
		See one-time task 22
48 <input type="checkbox"/>	Restart Java Web Application Servers in the mid-tier periodically.	Regularly, per housekeeping schedule
<p>It has become far less common than it once was for SAS's Java Web Applications to have memory leaks which caused them to gradually run out of memory and eventually crash, needing to be restarted. Field experience shows it can still happen, so the best approach is to observe or monitor (with a tool) the memory (heap) used by SAS mid-tier servers, and look for possible signs of memory leaks. If you see</p>		

behavior which implies they are leaking, schedule a script to restart the Web App servers periodically (eg daily or weekly, outside regular business hours) which should mitigate the issue.

49	<input type="checkbox"/>	Run your scripts to clear down log files.	Regularly, per housekeeping schedule See one-time task 16
<p>Some sites choose to archive log files older than 7 days to a compressed file archive (eg .zip), and keep them compressed between the ages of 7 and 30 days, in order to save disk space.</p> <p>If you have servers which need to be restarted in order to rotate their logs, schedule a daily task to restart each of them.</p>			
50	<input type="checkbox"/>	If you have set up log syndication, parsing and interpretation, check the output of the log analysis for events which require your attention due to their severity or frequency.	Regularly, per housekeeping schedule See one-time task 17
<p>Examples may include expiring licenses, unauthorized access attempts, multiple failures to authenticate from the same user in a short time period, messages which indicate a server was unreachable etc.</p>			
51	<input type="checkbox"/>	Periodically check for hotfixes available for your deployed SAS components. Also check for important SAS announcements, and support notes which are relevant to you and the SAS platforms you manage.	Regularly, per housekeeping schedule See one-time task 20
<p>As mentioned in task 20, see http://support.sas.com/rnd/migration/procmigrate/validtools.html for more information on SAS Hotfixes.</p>			
<p>SAS provides a SAS Hotfix Analysis, Download and Deployment tool, which is able to compare a list of deployed SAS components, at their specific versions, plus the list of hotfixes already applied to your platform, with a list of all available hotfixes available for those components. It can then identify new hotfixes for your components, and is capable of assisting you in the process of downloading and applying them. It is designed to be used for SAS servers both with and without direct internet connections.</p>			
52	<input type="checkbox"/>	Monitor the Autoload feature in SAS Visual Analytics (if you have this product), to ensure it is periodically refreshing tables periodically while SAS Visual Analytics is running.	Regularly, per housekeeping schedule See one-time task 24
53	<input type="checkbox"/>	Monitor the Audit Reports in SAS Visual Analytics (if you have this product), to review information about the usage of your Visual Analytics environment.	Regularly, per housekeeping schedule See one-time task 25

54	<input type="checkbox"/>	Apply new license files to SAS and third party components.	Before (or much less ideally, when) they expire See one-time task 30
You can find guidance specific to your version of SAS and your specific SAS and third-party products at http://support.sas.com/techsup/license/ .			
55	<input type="checkbox"/>	If necessary, obtain and apply new SSL certificates to components in your SAS platform which are configured to require them.	Just before SSL certificates expire
56	<input type="checkbox"/>	If you have SAS Grid, monitor its state. Evaluate the health of interactive grid workload, as well as the health of batch workload submitted for processing on the grid.	Regularly, per housekeeping schedule See one-time task 33

3 Example Housekeeping Schedule

The housekeeping schedule below is an example which a specific customer might determine is appropriate for their needs, in consideration of their business requirements. You should adapt it according to the particular circumstances, priorities and resource you have available for each specific SAS environment for which you are responsible. Not all tasks are applicable on all environments; in your adapted schedule, include only those tasks which are relevant and which you decide you will do.

Weekly tasks are intended to be completed *in addition* to daily tasks. Similarly, monthly and annual tasks are intended to be *in addition* to the daily tasks and any weekly tasks they may happen to coincide with.

The choice of frequencies (daily, weekly, monthly, annually) is only illustrative. Determine the frequencies appropriate to your particular SAS infrastructure and run your selected tasks at those frequencies.

Task / Frequency	Daily	Weekly	Monthly	Annually
35 Change the passwords for SAS internal accounts, and update the passphrase to re-encrypt stored passwords				x
36 Check the status of SAS servers	x			
37 Monitor disk space	x			
38 Monitor memory, CPU, network IO, disk IO	x			
39 Monitor terminal server memory usage	x			
40 Monitor job flows	x			
41 Run user and network application audit reports			x	
42 Monitor the performance of jobs and queries		x		
43 Execute backups	x			
44 Test the process to restore from backups				x
45 Check for long-running SAS sessions Check also for Enterprise Guide sessions which users have left running overnight	x			
46 Run the cleanwork utility or SAS Disk	x			

	Cleanup Handler to clean up abandoned SASWORK directories left behind by abruptly-terminated SAS workspace sessions		
47	If you have SPDS, run your script to delete old SPDS work tables	x	
48	Restart Java Web Application Servers		x
49	Run your scripts to clear down log files		x
50	If you have set up log syndication, parsing and interpretation, check the output of the log analysis for events which require your attention due to their severity or frequency		x
51	Periodically check for hotfixes available for your deployed SAS components Also check for important SAS announcements, and support notes which are relevant to you and the SAS platforms you manage		x
52	Monitor the Autoload feature in SAS Visual Analytics, to ensure it is periodically refreshing tables periodically while SAS Visual Analytics is running	x	
53	Monitor the Audit Reports in SAS Visual Analytics (if you have this product and have enabled these reports), to review information about the usage of your Visual Analytics environment		x
54	Apply new license files to SAS and third party components		As required
55	Obtain and apply new SSL certificates to components in your SAS platform which are configured to require them		As required
56	If you have SAS Grid, monitor its state. Evaluate the health of interactive grid workload, as well as the health of batch workload submitted for processing on the grid.	x	

4 Credits and Acknowledgements

This checklist is the result of contributions and source material from many SAS consultants. It could not have been as complete as it is without their tremendous help, but any errors are mine.

I am indebted to Mike Huels, Nicolas Adamek, Stuart Levine and Philip Gove for their work on the excellent 2008 GBIDI paper “Proven Practices for SAS Intelligence Platform System Administration”, <http://www.sas.com/tp-bin/tplog?F04169>. Written for SAS 9.1.3, much of its content is still relevant for SAS 9.4.

Some tasks specific to SAS Visual Analytics are adapted from an internal SAS paper “SAS Visual Analytics 7.1 - Recommended Post Install Steps”, <http://www.sas.com/tp-bin/tplog?L05985>, by Mark Thomas with contributions from Gilles Chrzaszcz and Erwan Granger.

Many tasks suggested here are based on contributions from consultants in the SAS EMEA & AP Professional Services practices, especially those in the Architecture, Premium Support, Analytic Platform Practices and Education. They submitted suggestions based on their experience implementing, supporting and enhancing and teaching users about SAS Intelligence Platform environments. My thanks go to Stephen Wallace, David Sobo, Mark Wastney, Rob Peatheyjohn, Dipesh Meghani, Peter Hobart, Alex Pilcher, Arfan Ali and Ian Sedgwick for their submissions – some of them substantial.

I thank my colleagues Scott McCauley, Simon Williams, Gerry Nelson and Dave Naden for reviewing and commenting on the initial drafts of this checklist, and for suggesting further changes and additional tasks.

SAS employees may wish to use the D27_SystemMaintenance document template from SAS’s Intelligence Platform Implementation (IPI) methodology. This ‘D27’ template allows the SAS implementation team to document administration and maintenance procedures for a customer’s own specific implementation. Some of the topics it covers are not addressed, or are only briefly discussed, in this checklist. For example, it has sections for describing how administrators should monitor and manage ETL processing, SAS® Business Intelligence components (for SAS® Information Delivery Portal, SAS® Business Intelligence Dashboards and SAS® Web Report Studio and related technologies), SAS® Enterprise Miner, scheduling and security.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. © indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2015 SAS Institute Inc. Cary, NC, USA. All rights reserved.