Synergetic Security Review Template (2021)

Synergetic databases and applications require adequate security configuration through multiple layers of the environment. They main objective of this exercise is to protect the database and system availability to ensure that confidential data is kept private and the system is secured and continually accessible to users who need access. This review focuses on helping to improve system security, however for improved business continuity practices it is recommended to also consider additional options that may provide improved performance, high availability and disaster recovery. The key focus points of this template are for hardening security configuration within a Synergetic environment across the following layers:

- Information Security Management
- Network Security
- Database Security
- Web Server Security
- Application Security
- Supporting Services Security

Refer to Synergetic Data Privacy and Security Information Sheet - Synergetic User Hub - Synergetic Wiki for a top level overview.

The review process aims to highlight risk factors and provide guidance for the organisation in line with:

- Synergetic platform security best practices
- Incorporated aspects of the ISMS ISO 27001 related to application and data protection
- Center for Internet Security (CIS) hardening guide
    - SQL 2016/2017/2019 https://www.cisecurity.org/benchmark/microsoft_sql_server/ - this has been reviewed in detail and the recommended settings incorporated to this guide.
    - IIS https://www.cisecurity.org/benchmark/microsoft_iis/ - note that the CIS IIS benchmark guide should be consulted separately and has not been directly incorporated into this review template.

The Synergetic Security Information Sheet will assist with understanding of the types of sensitive and personal data stored within Synergetic, some of the regulations that may apply to your school and top level technical areas to secure. Each individual school should verify their own regulatory information system and data protection requirements to ensure compliance. This register is not considered comprehensive to overall data and information system protection and should be used as a supplementary guide only. This register is constantly evolving and feedback is welcomed via Discourse to help improve it.

INFORMATION SECURITY MANAGEMENT

This includes policies, procedures and documentation in place to protect sensitive data.

Information from the client system admin and management is required for this section.

Seq	Recommended Controls	Control Reference	Findings	Risk Rating (Critical, High, Medium, Low)
1	Policies for Information Security are: • Defined, approved by management • Published and communicated to staff and external parties • Regularly reviewed for suitability	Management direction for information security A.5.1		
2	Information security and data privacy roles and responsibilities: • are defined and allocated • Staff in roles are aware of the requirement to secure the Synergetic systems and database	Organization of information security A.6.1		
3	Asset, data classification and information flow • asset, data classification and information flow (how data is used or transferred) is documented • risk assessment/registers used	A.8.1		

NETWORK SECURITY

To identify organisational assets and define appropriate protection responsibilities.

Seq	Recommended Controls	Control Reference	R*	Findings	Risk Rating (Critical, High, Medium, Low)

1	All Synergetic servers and data backups are documented in an inventory ideally with supporting network diagram. • Synergetic asset register documentation exists • include test/DR/snapshot systems • include data backup procedures, schedule and locations	Asset Management - Inventory of Assets A.8.1.1 Operational procedures and responsibilities A.12.1			
2	Physical access to the Synergetic database servers and backups is restricted • Physical entry controls • Protection from external/environmental threats	Physical and environmental security A.11.1			
3	Network access • Restricted to authorised users • Database server is only directly accessible to staff network or web servers • Database server is not contactable via guest networks • Only authorised devices can connect to the network that hosts the Synergetic servers	Access Control - Access to networks and network services A.9.1.2			
4	User access provisioning • follows a formal process for creation or deactivation of accounts • follow a formal process for assigning or revoking access rights for Synergetic application and database systems	User Access Management A.9.2.1 A9.2.2			
5	Administrator user accounts • Administrator accounts are restricted and documented • Use of administrator accounts is restricted for admin operations only • Review current Domain Administrator accounts	User Access Management A.9.2.3			
6	Password management • Password and password handling policies are in place and used for staff, service and administrator level accounts • Secure password provisioning and handling procedures are in place (eg. not emailed or stored in plain text)	User responsibilities A.9.3 User access management A9.2.4			
7	Review of User Access Rights • A regular scheduled audit of existing accounts, groups and permission sets allowing access to the Synergetic databases is performed.	User access management A.9.2.5			
8	Inbound access to SQL and Web server is protected by firewall • The minimum ports required for servers/services to function • See here for guidelines: Synergetic Network Port Details / Microsoft SQL Server Network Port Config	Access Control - Access to networks and network services A.9.1.2			
9	Outbound internet access from SQL, Web and Service Suite Servers is restricted by firewall Outbound access may be required for: • SMTP servers • ScreenConnect: Synergetic Remote Access • Octopus Deploy: Automatic Upgrades • VSN from Service Suite server (VIC sites): https://www.eduweb.vic.gov.au/VSRWebService/	Communications Security A.13			
10	Network traffic is protected by Intrusion Prevention System (IPS) or Web Application Firewall (WAF) or other	Protection from Malware A.12.2.1			
11	SMTP relay access from Synergetic servers and application is restricted • Secured via TLS where applicable • Secured via passwords (no anonymous relays) • IP address restrictions (where possible)	Communications Security A.13	Y		

*R= can be assessed remotely without input from stakeholders - y = YES P=Partially but additional info required from the stakeholders.

DATABASE SECURITY

Seq	Recommended Controls	Control Reference	R*	Findings	Risk Rating (Critical, High, Medium, Low)
1	Local administrators group is restricted on the SQL Servers	Management of privileged access rights A.9.2.3	Y		
2	Remote Desktop/server access to SQL Servers: • Remote Desktop Users Users group is restricted • Servers are not directly accessed via RDP or other remote connection software	Management of privileged access rights A.9.2.3	P		
3	Service Accounts • SQL Server service accounts use low level domain users (non-admin accounts)	Management of privileged access rights A.9.2.3 CIS 3.5-3.7	P		
4	File shares and permissions • Database files and backups are not accessible to normal user accounts via file shares • Database server does not allow file share access to non-admin accounts	Management of privileged access rights A.9.2.3	P		
5	Synergetic data and backup files are protected • Backup file locations documented • Secured to authorised system administrators • Access to and use of backups is controlled and data protection is maintained	Access Control - Access control policy A.9.1.1			
6	Database backups are performed • Regular schedule • Allowing for point in time recovery • System RTO and RPO is documented • Backup and DR schedules to meet the defined RTO/RPO	Backup A.12.3	P		
7	Database Version • SQL Server is patched in line with hardware requirements • Latest cumulative updates have been applied • Windows Server patched (get-hotfix | sort InstalledOn -Desc)	CIS 1.1	Y		
8	Database Security • The SQL Server (Windows Server) and instance is dedicated for Synergetic database use • No third party applications are installed to the SQL Server (other than AV)	CIS 1.2	Y		
9	Database Security - use of 'sa' account • 'sa' account is disabled OR • SA account password meets policy and is secured • Password has been updated when admin staff change over • Staff with access to the 'sa' password are known and authorised • The 'sa' password not distributed or used by staff • SA account is not used for daily server maintenance **Renaming of 'sa' account is not supported by Synergetic, even if it is disabled it must still exist as 'sa'	CIS 2.13	P		
10	Database Security - server level SQL logins limited to: • Limited to 'sa' and administrators • Synergetic*_*ServerLogin	Synergetic Security - Best Practices	Y		

11	Database Auditing and Logging • Ensure 'Maximum number of error log files' is set to greater than or equal to '12'	CIS 5.1	Y		
12	Database Logon auditing • Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins' **Important note - this can be considered however note that it will increase the SQL event log size significantly. Please use with caution and monitor disk/log size.	CIS 5.4	Y		
13	Database Security • Users access database via Windows Authentication by Active Directory Group membership • AD groups are used and not individual user accounts	Synergetic Security - Best Practices	Y		
14	Database Security - Orphaned users • Ensure 'Orphaned Users' are Dropped From SQL Server Databases	CIS 3.3			
15	Database Security - Fixed SQL Server Roles • System Admins and other fixed role membership is restricted • Seperate admin accounts are used • Servers are managed by remote tools (SSMS installed to workstation and not run directly on the server)	Synergetic Security - Best Practices	P		
16	Database Security - Fixed SQL Database Roles • Fixed database role membership use is restricted	Synergetic Security - Best Practices	Y		
17	Database Administration - Synergetic Fixed Database Roles • Membership is restricted to Synergetic service accounts	Synergetic Security - Best Practices	Y		
18	Direct Database Permissions for users and third party service accounts • Controlled via restricted dedicated SQL Server roles • Only granted permissions when required (eg. normal Synergetic users don't need direct table access) • Not granted to entire schema (eg. dbo, finance) • Not granted to fixed server or database roles eg. SysAdmin, db_datareader, db_owner • Permissions are only granted to the required objects	Synergetic Security - Best Practices	P		
19	• SQL Transport encryption • Network traffic encryption (TLS)	Cryptography A.10	Y		
20	^Ensure 'Remote Access' Server Configuration Option is set to '0'	CIS 2.6	Y		
21	^Ensure Unnecessary SQL Server Protocols are set to 'Disabled'	CIS 2.10	Y		
22	^Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances For named instance Synergetic config does not allow supplying port number, so needs the browser service to recognise it.	CIS 2.12	Y		
23	^Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role **Note that Windows auth is preferred for users & third party vendors so this should not normally apply.	CIS 4.2			
24	^Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins **Note that Windows auth is preferred for users & third party vendors so this should not normally apply.Authenticated Logins	CIS 4.3			

*R= can be reviewed remotely without input from client - y = YES P=Partially, ie. additional info required from client.

^These are additional checks - experimental and should be applied to test server before sign off for production

Unsupported SQL Server CIS Recommendations

Please note, as of the time of writing the following CIS recommendations are likely to **cause issues with Synergetic funtionality** due to underlying dependencies.

CIS	Description	Reason
2.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0'	Required for underlying logic
2.9	Ensure 'Trustworthy' Database Property is set to 'Off'	Required for CLR access
2.11	Ensure SQL Server is configured to use non-standard ports	Not supported for default instances . May have issue with changing port on default instance as Synergetic config does not allow supplying of port number in the configuration file. However, this would works okay for named instances using the SQL Browser Service but then CIS 2.12 could not be performed to 'hide' the instance.
2.14	Ensure the 'sa' Login Account has been ren amed	Synergetic has dependencies on DB owner matching the user that created the CLRs, which is normally ‘sa’ and set the DB owner to dbo (which is linked to sa).
2.16	Ensure no login exists with the name 'sa'	As above, ‘sa’ user is required but can be disabled
3.1	Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode'	Synergetic requires mixed mode - normal staff and admin user accounts can all use Windows Auth but the application has internal SQL user accounts (zSynergetic_*) managed by the patch process and used for each application
3.4	Ensure SQL Authentication is not used in contained databases	As above, Synergetic uses contained users for the zSynergetic* application user accounts
6.2	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Current Synergetic CLR settings are defined as follows: System.Drawing UNSAFE_ACCESS SynStreamCrypt SAFE_ACCESS Synergetic.Database.CLR UNSAFE_ACCESS GroupConcat SAFE_ACCESS SqlRegEx SAFE_ACCESS Synergetic.Database.CLR.XmlSerializers EXTERNAL_ACCESS

WEB SERVER SECURITY

Please refer to https://www.cisecurity.org/benchmark/microsoft_iis/ for industry standard web server hardening recommendations.

Seq	Recommended Controls	Control Reference	R*	Findings	Risk Rating (Critical, High, Medium, Low)
1	Websites protected by SSL certificates	Cryptography A.10	Y		
2	Application pools operate under app pool identities (not local system)	Synergetic Security - Best Practices	Y		

3	Website folder security • App pool users (eg. IIS AppPool\SynWeb) should only have read & exec access to the website folders Special permission access should only be available as follows: • "C:\Windows\Temp" "IIS_IUSRS" "Modify" • "inetpub\wwwroot\Reports" "IIS_IUSRS" "Read" • "inetpub\wwwroot\SynWeb\App_Sprites" "IIS AppPool\SynWeb" "Modify" • "inetpub\wwwroot\SynWeb\Site" "IIS AppPool\SynWeb" "Modify" • "inetpub\wwwroot\SynWeb\Site\Certificates" "IIS AppPool\SynWeb" "Read, Write" • "inetpub\wwwroot\SynWeb\Uploads" "IIS AppPool\SynWeb" "Modify", "IUSR" "Modify", "IIS_IUSRS" "Modify" • "inetpub\wwwroot\SynergeticCommunityPortal\Site" "IIS AppPool\SynCommPortal" "Modify" • "inetpub\wwwroot\SynergeticCommunityPortal\Site\Certificates" "IIS AppPool\SynCommPortal" "Read, Write"	Management of privileged access rights A.9.2	Y		
4	Authentication for SynWeb and Community Portal • SAML or other SSO auth method is used	Cryptography A.10	Y		
5	Community Portal Administrators • Security role is restricted to system admin users	Management of privileged access rights A.9.2	P		

*R= can be reviewed remotely without input from client - y = YES P=Partially, ie. additional info required from client.

APPLICATION SECURITY

Seq	Recommended Controls	Control Reference	R*	Findings	Risk Rating (Critical, High, Medium, Low)
1	Synergetic Windows Application (SynMain) • User Authentication is via Windows Authentication	Synergetic Security - Best Practices	Y		
2	Synergetic Application Share • Read&Exec only to staff who require Synergetic app access • Write access only to \Forms and \Reports\Site for admin users or report developers • No additional files are stored in the application share (eg. sensitive data extracts)	Management of privileged access rights A.9.2	Y		
3	Group/User Security Maintenance • Accessible only to system administrators (restricted set)	Management of privileged access rights A.9.2	P		
4	SynSuperUser Group membership is restricted to authorised users	Management of privileged access rights A.9.2	P		
5	General Ledger Users • User list is current and only contains authorised users • Permissions to view 'all accounts' is restricted to authorised users	Management of privileged access rights A.9.2	P		
6	Business Unit Users • User list is current and only contains authorised users • Purchase Order super authorisers is restricted	Synergetic Security - Best Practices	P		
7	Payroll (if used) • Payroll Encryption is enabled	privileged A.10	Y		

8	Document Classification Security • Restricted to authorised users	Synergetic Security - Best Practices	P		
9	Synergetic Security Groups - Framework • Security Group framework (eg. tiered, role based) list and each group purpose is documented • Naming standards are defined • Tiered / role based permission sets are used • Redundant groups are renamed or removed	Synergetic Security - Best Practices	P		
10	Synergetic Security Groups - Membership • Groups do not contain inactive staff • Group membership is approved by module data 'asset' owners - eg. General Ledger access is authorised by the Business Manager/Accountant. Enrolments data view or change permissions is approved by the Head of Admissions.	Synergetic Security - Best Practices	P		
11	Synergetic Security Groups - Permissions • Permission change management procedures in place (including request approval and logging) • Change logs are reviewed - no unauthorised changes have occurred in past period (ConfigGroupSecurityHistory) • Permission sets are reviewed on a periodic basis	Synergetic Security - Best Practices	P		
12	Synergetic Permission Extract • Extract is provided regularly for review • Review and sign off from system admin and management	Synergetic Security - Best Practices	P		

*R= can be assessed remotely without input from stakeholders - y = YES P=Partially but additional info required from the stakeholders.

SUPPORTING SERVICES SECURITY

Seq	Recommended Controls	Control Reference	R*	Findings	Risk Rating (Critical, High, Medium, Low)
1	If DocMan Import Service is used: • DocMan UNC share paths are secured by user role	Synergetic Security - Best Practices	Y		
2	Services run under low level domain user account	Synergetic Security - Best Practices	Y		

*R= can be assessed remotely without input from stakeholders - y = YES P=Partially but additional info required from the stakeholders.

Disclaimer:

The items and guidance listed in this register are based on the opinion or view from individual consultants at Synergetic.