AimBetter

REGULATION COMPLIANCE FEATURES

AimBetter capabilities provide the needed tools for complying with regulatory subjects. In the following table, we present for each capability, the regulatory subject addressed and the correspondent regulation items.

Unauthorized Remote-Control Activation			
Regulatory subject: Access Control Authorizations			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.9.4.4 - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	CC6.1 - Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets	AC-3 - Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	IAM-06 - Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.

Presenting Unauthorized Commands To Your SQL Server			
Regulatory subject: RBAC Authorizations			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.9.2.3 - The allocation and use of privileged access rights shall be restricted and controlled.	CC6.3 - Uses Role-Based Access Controls — Role-based access control is utilized to support segregation of incompatible functions.	IA-2 - Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	IAM-08 - Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
Regulatory subject: Monitoring controls			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.12.4.1 - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	CC7.1 - Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	CA-7 - Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy.	AIS-04 - Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

Presenting Unauthorized Commands To Your IIS Server			
Regulatory subject: RBAC Authorizations			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.9.2.3 - The allocation and use of privileged access rights shall be restricted and controlled.	CC6.3 - Uses Role-Based Access Controls — Role-based access control is utilized to support segregation of incompatible functions.	IA-2 - Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	IAM-08 - Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
Regulatory subject: Monitoring controls			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.12.4.1 - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	CC7.1 - Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	CA-7 - Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy.	AIS-04 - Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

Actively login attempts tracing and detects any Failed Login Attempts - Ransom Attack Detection			
Regulatory subject: Monitoring controls			
ISO 27001:2013	**COSO**	**NIST 800-53**	**CCM**
A.12.4.1 - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	CC7.1 - Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	CA-7 - Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy.	AIS-04 - Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.