{"records":[{"payment_information":{"type":"DROP_DOWN","value":null},"record_number":{"type":"RECORD_NUMBER","value":"9"},"access_permissions":{"type":"USER_SELECT","value":[]},"personal_information":{"type":"DROP_DOWN","value":null},"requestor_business_unit":{"type":"SINGLE_LINE_TEXT","value":""},"number_of_records":{"type":"DROP_DOWN","value":"High
'>100,000'"},"Attachment":{"type":"FILE","value":[]},"project_name":{"type":"SINGLE_LINE_TEXT","value":"Qlik Sense instance from Data
Technology"},"project_types":{"type":"CHECK_BOX","value":["System"]},"confidential_radio":{"type":"RADIO_BUTTON","value":"Yes"},"created_datetime":{"type":"CREATED_TIME","value":"2020-11-17T11:09:00Z"},"third_party_hosting_radio":{"type":"RADIO_BUTTON","value":"Yes"},"updated_datetime":{"type":"UPDATED_TIME","value":"2020-11-23T16:57:00Z"},"confidential_information":{"type":"DROP_DOWN","value":null},"Drop_down":{"type":"DROP_DOWN","value":"Both - In-house & 3rd
Party"},"Status":{"type":"STATUS","value":"Submitted to
Infosec"},"Assignee":{"type":"STATUS_ASSIGNEE","value":[]},"attestation_table":{"type":"SUBTABLE","value":[{"id":"4596","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Provide suitable security for backup
data"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S39"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup
destinations."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Azure backups of each VM instance into Recovery services
vault"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4599","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Provide suitable security for backup
media"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S38"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud
services."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Backups are encrypted at rest.
(SSE)"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4600","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Test backup media regularly"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S37"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly
working."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Back ups are restored Bi-Annually for testing purposes by Data Technology
support."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4601","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Backup schedules should be put in
place"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S36"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly

restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Azure backups of each VM instance.\nDaily snapshot is taken and stored for a week.\nWeekly snapshot is taken and stored for 2 weeks."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4602","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that a Web Application Firewall (WAF) is placed in front of externally facing servers"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S35"},"acknowledgement":{"type":"DROP_DOWN","value":"Control planning underway (add comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Place web application firewalls (WAF) in front of externally facing applications to verify and validate the traffic. Any unauthorized services or traffic should be blocked and an alert generated."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Currently not in place because access is managed by NSGs and an application gateway is to configured for new architecture"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4603","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that servers are deployed away from the Internet unless they are required externally"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S34"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"External users require access to the Qlik Sense platform via Port 443. All other ports closed to public."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4604","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that port scanning is in place with the IT security team"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S33"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization?s approved baseline is discovered, an alert should be generated and reviewed."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Network Watcher is enabled for port scanning, which generates alerts."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4605","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Restrict ports and protocols to minimum required"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S31"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that only ports, protocols, and services with validated business needs are running on each system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4606","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Enable anti-exploitation

features"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S30"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4607","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Deploy Anti-virus to systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S29"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.\n\nRefer to the IT Security team to assist with software installation.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"MS Default anti-malware software in place (Windows Defender) can liase with IT Security if this needs to be upgraded"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4608","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Utilise SPF for emails (if sending emails to customers)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N11"},"acknowledgement":{"type":"DROP_DOWN","value":"Not applicable (add comment)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Euromoney control the domains associated with email distribution from Qlik server"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4609","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Remove any unnecessary scripting languages from supporting systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S27"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that only authorized scripting languages are able to run in all web browsers and email clients installed on developer devices.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4610","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Remove any unnecessary services from supporting systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S26"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Uninstall or disable any unauthorized browser or email client plugins or add-on applications."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4611","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the system is appropriately logging to the centralised SIEM solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S25"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in

place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Approach IT Security to ensure that the system is integrated with the group Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4612","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Arrange for IT security to run reports to check for anomalies"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S24"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4613","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that adequate local logging space is available"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S23"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4614","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all systems are logging relevant information, consistently"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S22"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that local logging has been enabled on all systems and networking devices. System logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4615","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that appropriate time sources are used"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S21"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4616","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use a non-administrative account where possible"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S20"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4617","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all admin access is via multifactor authentication

(MFA)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S19"},"acknowledgement":{"type":"DROP_DOWN","value":"Control planning underway (add comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.\n\nWhere multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Auth0 will be used"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4618","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that unsuccessful login of admin accounts are logged"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S18"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4619","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure default passwords are changed for devices and systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S17"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4620","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Control of administrative accounts"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S16"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4621","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Only use administrative accounts where absolutely necessary"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S15"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.\n\nAdministrators must not use privileged accounts for day-to-day tasks (email, internet browsing etc.)"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4622","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Regularly receive and review vulnerability scans to ensure issues have been resolved."},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S14"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Regularly compare the

results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. Utilise a risk-rating process to prioritise the remediation of discovered vulnerabilities. Remediate according to Company approved
timescales."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4623","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that, where possible, updated take place
automatically"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S13"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air
gapped."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4624","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Properly configure vulnerability scanning in authenticated
mode"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S12"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nPerform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.\n\nContact the IT Security team to assist you with this. "},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Scans are running but not using a dedicated
account."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4625","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that vulnerability reports are sent to the central logging
solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S11"},"acknowledgement":{"type":"DROP_DOWN","value":"Control planning underway (add
comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be
vulnerable."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"The first requirement is in place, but need guidance on the
second"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4626","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the application is setup to be scanned by the vulnerability assessment tool (arranged via IT
security)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S10"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Business owner to approach IT Security and ensure that the application/system is added to the Qualys and Netsparker vulnerability scanning shedules.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4627","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that an automated configuration monitoring

system is in
place"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S9"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Implement automated
monitoring that verifies all remotely testable secure configuration elements,
and alerts when unauthorized changes occur. This includes detecting new
listening ports, new administrative users, changes to group and local policy
objects and new services running on a system.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4628","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Setup remote acces to your application
securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S7"},"acknowledgement":{
"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Perform all remote
administration of servers, workstation, network devices, and similar equipment
over secure channels. Protocols such as telnet, VNC, RDP, or others that do not
actively support strong encryption should only be used if they are performed
over a secondary encryption channel, such as SSL, TLS or
IPSEC."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comm
ents":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4629","value":{"summary":{"
type":"SINGLE_LINE_TEXT","value":"Ensure that underlying operating systems are
appropriately
secure"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S6"},"acknowledgement":{"t
ype":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Maintain documented
security configuration standards for all authorized operating systems and
software. Hardened operating system images should be used. \n\n*Refer to the IT
Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Documentation will be
provided, Qlik does not guarantee its software will work correctly if operating
systems are hardened, it can lead to failure. However some hardening can be
carried out, but must be
tested"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4630
","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that any
software or components that you're using are on the whitelist (IT Security can
provide
guidance)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S5"},"acknowledgement":
{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nMaintain an
up-to-date list of all authorized software that is required in the enterprise
for any business purpose on any business
system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_com
ments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4631","value":{"summary":{
"type":"SINGLE_LINE_TEXT","value":"Use certificates in order to authenticate
client
devices"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S4"},"acknowledgement":{"
type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use client certificates
to validate and authenticate systems prior to connecting to the private
network.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4632","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Ensure that the asset inventory is created and
updated with all system components for this

project."},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S2"},"acknowledgement":{
"type":"DROP_DOWN","value":"Control planning underway (add
comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"It is the
responsibility of the business owner to maintain an accurate and up-to-date
inventory of all technology assets with the potential to store or process
information. This inventory shall include all software and hardware assets,
whether connected to the organization's network or
not."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Data Technology
will work with business owners to provide this
information."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id"
:"4633","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use of DHCP in
assigning IP
addresses"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S1"},"acknowledgement":
{"type":"DROP_DOWN","value":"Not applicable (add
comment)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"If the organization
is dynamically assigning addresses using DHCP, then deploy dynamic host
configuration protocol, (DHCP) server logging, and use this information to
improve the asset inventory and help detect unknown systems.\n\n*Refer to the IT
Security and/or Network team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Addresses not
dynamically assigned. There is no DHCP
server."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"463
4","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure host-based DLP
tools are
operating"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N9"},"acknowledgement":
{"type":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use host-based data
loss prevention (DLP) to enforce ACLs even when data is copied off a server. In
most organizations, access to the data is controlled by ACLs that are
implemented on the server. Once the data have been copied to a desktop system,
the ACLs are no longer enforced and the users can send the data to whomever they
want. Work with the infrastructure team to put this in place. The business is
accountablefor this control but the infrastructure team and/or the development
teams may be responsible for implementation.\n\n*Refer to the Network &
Infrastructure team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4635","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Put in place network based
encryption"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N8"},"acknowledgement"
:{"type":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"All data with a
confidentional classification is to be sent over encrypted connections
(internally and
externally)"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Data has not
been classified as confidential as of
yet."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4636",
"value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Put in place integrity
checking
tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N7"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":"Control not in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Put in place integrity
checking tools. The development team, in conjunction with infrastructure, should
implement an integrity checking tool to ensure that changes to configuration
files do not go unnoticed. The business is accountable for this and the

development teams and/or infrastrcture will be reponsible for the implementation."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4637","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Secure remote access to the network"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N6"},"acknowledgement":{"type":"DROP_DOWN","value":"Control planning underway (add comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication. This control is likely to need to be implemented by the application developers but also refers to remote access provided to the servers upon which the application sits. The business is accountable for ensuring that these controsl are in place for this application. Supporting infrastructure or developers may be responsible for implementing the control.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Internal users have two factor authentication only. Auth0 will need to be implemented. Further guidance required from IT Security team"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4638","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Appropriate segregation of network devices (not sharing infrastructure with lower risk applications)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N3"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. This control requires the requestor to ensure that this high risk application is segregated from lower risk applications. The infrastructure supporting team will be responsible for doing this but the business is accountable for ensuring that it happens.\n\n*Refer to the Network & Infrastructure team before answering."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4639","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Keep network devices updated"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N2"},"acknowledgement":{"type":"DROP_DOWN","value":"Control not in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Engage with IT security and infrastructure teams to ensure that all in-scope components are added to the Qualys scanning schedule.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Further guidance required from IT Security team"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4640","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Manage network device securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N1"},"acknowledgement":{"type":"DROP_DOWN","value":"Control in place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Manage network devices using two-factor authentication and encrypted sessions. This control requires any administrative access to infrastrastructure and network devices to enfore two-factor authentication. Web sessions should use HTTPS. Console sessions should be over SSH.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4641","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that high risk systems are segregated from less-trusted/lower risk systems.
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S40"},"acknowledgement":{"type":

"DROP_DOWN","value":"Not applicable (add
comment)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Physically or
logically segregated systems should be used to isolate and run software that is
required for business operations but incur higher risk for the
organization."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Data
Technology has not assessed the risk factor of each dataset: it is all lumped
together in a secure Azure environment.\nWe need guidance from infosec on risk
categories/levels.\nFor software - we are only using a single software
suite."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4642
","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure system patches
are automatically identified.
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S41"},"acknowledgement":{"type":
"DROP_DOWN","value":"Control planning underway (add
comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Deploy automated
software update tools in order to ensure that the operating systems are running
the most recent security updates provided by the software
vendor."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Software update
downloads are automated, but updates are manually executed in order to avoid
service disruption to end
users"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4643"
,"value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Limit access to
scripting
tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S42"},"acknowledgement":{"t
ype":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Limit access to
scripting tools (such as Microsoft PowerShell and Python) to only administrative
or development users with the need to access those
capabilities."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"securi
ty_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4644","value":{"summ
ary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the system is appropriately
logging to the centralised SIEM
solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S43"},"acknowledgement":
{"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nEnable system logging
to include the following information:\n\nevent source\nevent date\nevent
timestamp \nsource addresses \ndestination addresses \nuser ID\nsuccessful and
failed login attempts\nlogouts\nall modifications to user accounts
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4645","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Protect event logs
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S44"},"acknowledgement":{"type":
"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Using logical access
controls; protect logs from unauthorised modification, deletion, or overwriting.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4646","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Sandboxing for incoming emails (if receiving emails
from customer and/or other
systems)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S45"},"acknowledgement":
{"type":"DROP_DOWN","value":"Not applicable (add
comment)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use sandboxing to
analyze and block inbound email attachments with malicious behavior. We already
have Mimecast fulfilling this
function."},"project_comments":{"type":"MULTI_LINE_TEXT","value":"Qlik has no

function or feature to receive inbound
emails."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"464
7","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that access to
systems is explicitly
defined"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S46"},"acknowledgement":{
"type":"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nProtect systems with
firewalls or port filtering tools. Ensure tools are configured with a
default-deny rule that drops all traffic except those services and ports that
are explicitly allowed.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4648","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Network permiter firewall
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S47"},"acknowledgement":{"type":
"DROP_DOWN","value":"Control in
place"},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that network
perimeter firewalls are in front of externally facing servers, actively blocking
network threats and receive regular signature updates.\n\n*Refer to the IT
Security and/or Network teams before
answering"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4649","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Third party hosted network devices to be
securely
managed"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N12"},"acknowledgement":{
"type":"DROP_DOWN","value":"Control planning underway (add
comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"If any internally
owned network devices are situated at a third party site (e.g WAN/MPLS
extension), remote administrative access must take place over a secure VPN
tunnel. \n\n*Refer to IT Security before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"VPN tunnel to be
created. \nFor now internal users are
whitelisted."},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id"
:"4650","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Complete Data
Privacy Impact
Assessment"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"P01"},"acknowledgement
":{"type":"DROP_DOWN","value":"Control planning underway (add
comments)"},"attestation":{"type":"MULTI_LINE_TEXT","value":"As personal data is
in scope for this project, you are required to ensure that a Data Privacy Impact
assessment has been completed and approved by the Data Protection Officer.
Please contact your Data Guardians for more information.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":"II Research Business
has completed a Data Privacy Impact assessment, but not specifically about Qlik.
Asking if a further assessment is required.
"},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}}]},"risk_score":{"
type":"NUMBER","value":"50"},"payment_radio":{"type":"RADIO_BUTTON","value":"No"
},"personal_radio":{"type":"RADIO_BUTTON","value":"Yes"},"$revision":{"type":"__
REVISION__","value":"10"},"created_by":{"type":"CREATOR","value":{"code":"gchitt
y@iilondon.com","name":"Graham
Chitty"}},"requestor":{"type":"USER_SELECT","value":[{"code":"gchitty@iilondon.c
om","name":"Graham
Chitty"}]},"Text_area":{"type":"MULTI_LINE_TEXT","value":"Qlik Sense is a
Business Intelligence/Analytics platform. It is provided via a Qlik Partner,
Data Technology. \n\nData Technology provides hosting in Azure, development and
support. \n\nThe Azure servers require upgrading to support increased demand

from multiple Euromoney businesses to align with development best practices.\n\nThis covers security relating to the Qlik platform:\nhttps://help.qlik.com/en-US/sense-admin/November2020/Subsystems/DeployAdministerQSE/Content/Sense_DeployAdminister/QSEoW/Deploy_QSEoW/server-security-overview.htm\n"},"Date":{"type":"DATE","value":"2020-12-14"},"risk_level":{"type":"DROP_DOWN","value":"High"},"requestor_email":{"type":"LINK","value":"gchitty@iilondon.com"},"requestor_phone":{"type":"LINK","value":""},"updated_by":{"type":"MODIFIER","value":{"code":"gchitty@iilondon.com","name":"Graham Chitty"}},"Link":{"type":"LINK","value":"https://confluence.euromoneydigital.com/display/TechSvc/Qlik+Sense"},"internet_availability_radio":{"type":"RADIO_BUTTON","value":"Yes"},"$id":{"type":"__ID__","value":"9"}},{"payment_information":{"type":"DROP_DOWN","value":null},"record_number":{"type":"RECORD_NUMBER","value":"8"},"access_permissions":{"type":"USER_SELECT","value":[]},"personal_information":{"type":"DROP_DOWN","value":null},"requestor_business_unit":{"type":"SINGLE_LINE_TEXT","value":""},"number_of_records":{"type":"DROP_DOWN","value":"Moderate '<100,000'"},"Attachment":{"type":"FILE","value":[]},"project_name":{"type":"SINGLE_LINE_TEXT","value":"User Service API"},"project_types":{"type":"CHECK_BOX","value":["System"]},"confidential_radio":{"type":"RADIO_BUTTON","value":"Yes"},"created_datetime":{"type":"CREATED_TIME","value":"2020-11-10T15:18:00Z"},"third_party_hosting_radio":{"type":"RADIO_BUTTON","value":"No"},"updated_datetime":{"type":"UPDATED_TIME","value":"2020-11-10T15:18:00Z"},"confidential_information":{"type":"DROP_DOWN","value":null},"Drop_down":{"type":"DROP_DOWN","value":"In-House"},"Status":{"type":"STATUS","value":"In Progress"},"Assignee":{"type":"STATUS_ASSIGNEE","value":[{"code":"elliott.weaver@euromoneyplc.com","name":"Elliot Weaver"}]},"attestation_table":{"type":"SUBTABLE","value":[{"id":"4539","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Provide suitable security for backup data"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S39"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4540","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Provide suitable security for backup media"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S38"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4541","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Test backup media regularly"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S37"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4542","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Backup schedules should be put in place"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S36"},"acknowledgement":{"t

ype":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"
Ensure that each system is automatically backed up on at least a weekly basis,
and more often for systems storing sensitive information. To help ensure the
ability to rapidly restore a system from backup, the operating system,
application software, and data on a machine should each be included in the
overall backup procedure. These three components of a system do not have to be
included in the same backup file or use the same backup software. There should
be multiple backups over time, so that in the event of malware infection,
restoration can be from a version that is believed to predate the original
infection. All backup policies should be compliant with any regulatory or
official
requirements."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"securi
ty_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4543","value":{"summ
ary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that a Web Application Firewall
(WAF) is placed in front of externally facing
servers"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S35"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"Place web application firewalls (WAF) in front of externally facing
applications to verify and validate the traffic. Any unauthorized services or
traffic should be blocked and an alert
generated."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_
comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4544","value":{"summary
":{"type":"SINGLE_LINE_TEXT","value":"Ensure that servers are deployed away from
the Internet unless they are required
externally"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S34"},"acknowledgement
":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","val
ue":"Verify any server that is visible from the Internet or an untrusted
network, and if it is not required for business purposes, move it to an internal
VLAN and give it a private
address."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_co
mments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4545","value":{"summary":
{"type":"SINGLE_LINE_TEXT","value":"Ensure that port scanning is in place with
the IT security
team"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S33"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"P
erform automated port scans on a regular basis against all key servers and
compared to a known effective baseline. If a change that is not listed on the
organization?s approved baseline is discovered, an alert should be generated and
reviewed."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4546","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Restrict ports and protocols to minimum
required"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S31"},"acknowledgement":
{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value
":"Ensure that only ports, protocols, and services with validated business needs
are running on each
system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_com
ments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4547","value":{"summary":{
"type":"SINGLE_LINE_TEXT","value":"Enable anti-exploitation
features"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S30"},"acknowledgement":
{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value
":"Enable anti-exploitation features such as Data Execution Prevention (DEP) or
Address Space Layout Randomization (ASLR) that are available in an operating
system or deploy appropriate toolkits that can be configured to apply protection
to a broader set of applications and

executables."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"securit
y_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4548","value":{"summa
ry":{"type":"SINGLE_LINE_TEXT","value":"Deploy Anti-virus to
systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S29"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"Employ anti-malware software that offers a centralized infrastructure that
compiles information on file reputations or have administrators manually push
updates to all machines. After applying an update, automated systems should
verify that each system has received its signature update.\n\nRefer to the IT
Security team to assist with software installation.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4549","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Utilise SPF for emails (if sending emails to
customers)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N11"},"acknowledgement
":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","val
ue":"To lower the chance of spoofed or modified emails from valid domains,
implement Domain-based Message Authentication, Reporting and Conformance (DMARC)
policy and verification, starting by implementing the Sender Policy Framework
(SPF) and the DomainKeys Identified Mail(DKIM)
standards."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_
comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4550","value":{"summary
":{"type":"SINGLE_LINE_TEXT","value":"Remove any unnecessary scripting languages
from supporting
systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S27"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"Ensure that only authorized scripting languages are able to run in all web
browsers and email clients installed on developer devices.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4551","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Remove any unnecessary services from supporting
systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S26"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"Uninstall or disable any unauthorized browser or email client plugins or
add-on
applications."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"securi
ty_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4552","value":{"summ
ary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the system is appropriately
logging to the centralised SIEM
solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S25"},"acknowledgement":
{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value
":"Approach IT Security to ensure that the system is integrated with the group
Security Information and Event Management (SIEM) or log analytic tool for log
correlation and
analysis."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4553","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Arrange for IT security to run reports to
check for
anomalies"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S24"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Have security personnel and/or system administrators run biweekly reports
that identify anomalies in logs. They should then actively review the anomalies,
documenting their
findings."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4554","value":{"summary"

:{"type":"SINGLE_LINE_TEXT","value":"Ensure that adequate local logging space is available"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S23"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic
basis."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4555","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all systems are logging relevant information,
consistently"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S22"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that local logging has been enabled on all systems and networking devices. System logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4556","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that appropriate time sources are used"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S21"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are
consistent."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4557","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use a non-administrative account where possible"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S20"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of
systems."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4558","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all admin access is via multifactor authentication
(MFA)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S19"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.\n\nWhere multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4559","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that unsuccessful login of admin accounts are
logged"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S18"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Configure systems to issue a log entry and alert on any unsuccessful login to an administrative

account."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_co
mments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4560","value":{"summary":
{"type":"SINGLE_LINE_TEXT","value":"Ensure default passwords are changed for
devices and
systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S17"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"Before deploying any new devices in a networked environment, change all
default passwords for applications, operating systems, routers, firewalls,
wireless access points, and other systems to have values consistent with
administration-level
accounts."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4561","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Control of administrative
accounts"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S16"},"acknowledgement":
{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value
":"Use automated tools to inventory all administrative accounts and validate
that each person with administrative privileges on desktops, laptops, and
servers is authorized by a senior
executive."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_
comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4562","value":{"summary
":{"type":"SINGLE_LINE_TEXT","value":"Only use administrative accounts where
absolutely
necessary"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S15"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Minimize administrative privileges and only use administrative accounts when
they are required. Implement focused auditing on the use of administrative
privileged functions and monitor for anomalous behavior.\n\nAdministrators must
not use privileged accounts for day-to-day tasks (email, internet browsing etc.)
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4563","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Regularly receive and review vulnerability scans to
ensure issues have been
resolved."},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S14"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Regularly compare the results from consecutive vulnerability scans to verify
that vulnerabilities have been remediated in a timely manner. Utilise a
risk-rating process to prioritise the remediation of discovered vulnerabilities.
Remediate according to Company approved
timescales."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security
_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4564","value":{"summar
y":{"type":"SINGLE_LINE_TEXT","value":"Ensure that, where possible, updated take
place
automatically"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S13"},"acknowledgem
ent":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","
value":"Deploy automated patch management tools and software update tools for
operating system and software/applications on all systems for which such tools
are available and safe. Patches should be applied to all systems, even systems
that are properly air
gapped."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_com
ments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4565","value":{"summary":{
"type":"SINGLE_LINE_TEXT","value":"Properly configure vulnerability scanning in
authenticated
mode"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S12"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"\

nPerform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.\n\nContact the IT Security team to assist you with this.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4566","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that vulnerability reports are sent to the central logging
solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S11"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4567","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the application is setup to be scanned by the vulnerability assessment tool (arranged via IT security)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S10"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Business owner to approach IT Security and ensure that the application/system is added to the Qualys and Netsparker vulnerability scanning shedules.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4568","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that an automated configuration monitoring system is in
place"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S9"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Implement automated monitoring that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects and new services running on a system.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4569","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Setup remote acces to your application securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S7"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4570","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that underlying operating systems are appropriately
secure"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S6"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Maintain documented security configuration standards for all authorized operating systems and software. Hardened operating system images should be used. \n\n*Refer to the IT Security team before answering.

```
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4571","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that any software or components that you're using are on the whitelist (IT Security can provide guidance)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S5"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nMaintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4572","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use certificates in order to authenticate client devices"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S4"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use client certificates to validate and authenticate systems prior to connecting to the private network.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4573","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the asset inventory is created and updated with all system components for this project."},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S2"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"It is the responsibility of the business owner to maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all software and hardware assets, whether connected to the organization's network or not."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4574","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use of DHCP in assigning IP addresses"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S1"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol, (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.\n\n*Refer to the IT Security and/or Network team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4575","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure host-based DLP tools are operating"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N9"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server.  In most organizations, access to the data is controlled by ACLs that are implemented on the server.  Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want. Work with the infrastructure team to put this in place. The business is accountablefor this control but the infrastructure team and/or the development teams may be responsible for implementation.\n\n*Refer to the Network & Infrastructure team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4576","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Put in place network based encryption"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N8"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
```

e":"All data with a confidentional classification is to be sent over encrypted connections (internally and externally)"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4577","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Put in place integrity checking tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N7"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Put in place integrity checking tools. The development team, in conjunction with infrastructure, should implement an integrity checking tool to ensure that changes to configuration files do not go unnoticed. The business is accountable for this and the development teams and/or infrastrcture will be reponsible for the implementation."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4578","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Secure remote access to the network"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N6"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication. This control is likely to need to be implemented by the application developers but also refers to remote access provided to the servers upon which the application sits. The business is accountable for ensuring that these controsl are in place for this application. Supporting infrastructure or developers may be responsible for implementing the control.\n\n*Refer to the IT Security team before answering.\n"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4579","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Appropriate segregation of network devices (not sharing infrastructure with lower risk applications)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N3"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. This control requires the requestor to ensure that this high risk application is segregated from lower risk applications. The infrastructure supporting team will be responsible for doing this but the business is accountable for ensuring that it happens.\n\n*Refer to the Network & Infrastructure team before answering."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4580","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Keep network devices updated"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N2"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Engage with IT security and infrastructure teams to ensure that all in-scope components are added to the Qualys scanning schedule.\n"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4581","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Manage network device securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N1"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Manage network devices using two-factor authentication and encrypted sessions. This control requires any administrative access to infrastrastructure and network devices to enfore two-factor authentication. Web sessions should use

HTTPS. Console sessions should be over SSH.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4582","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that high risk systems are segregated from less-trusted/lower risk systems.
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S40"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4583","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure system patches are automatically identified.
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S41"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4584","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Limit access to scripting tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S42"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4585","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the system is appropriately logging to the centralised SIEM solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S43"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"\nEnable system logging to include the following information:\n\nevent source\nevent date\nevent timestamp \nsource addresses \ndestination addresses \nuser ID\nsuccessful and failed login attempts\nlogouts\nall modifications to user accounts
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4586","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Protect event logs
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S44"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Using logical access controls; protect logs from unauthorised modification, deletion, or overwriting.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4587","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Sandboxing for incoming emails (if receiving emails from customer and/or other systems)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S45"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use sandboxing to analyze and block inbound email attachments with malicious behavior. We already have Mimecast fulfilling this function."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4588","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that access to systems is explicitly defined"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S46"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"

:"\nProtect systems with firewalls or port filtering tools. Ensure tools are configured with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4589","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Network permiter firewall
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S47"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that network perimeter firewalls are in front of externally facing servers, actively blocking network threats and receive regular signature updates.\n\n*Refer to the IT Security and/or Network teams before answering"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4590","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Third party hosted network devices to be securely
managed"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N12"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"If any internally owned network devices are situated at a third party site (e.g WAN/MPLS extension), remote administrative access must take place over a secure VPN tunnel. \n\n*Refer to IT Security before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4591","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Complete Data Privacy Impact Assessment"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"P01"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"As personal data is in scope for this project, you are required to ensure that a Data Privacy Impact assessment has been completed and approved by the Data Protection Officer. Please contact your Data Guardians for more information.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}}]},"risk_score":{"type":"NUMBER","value":"40"},"payment_radio":{"type":"RADIO_BUTTON","value":"No"},"personal_radio":{"type":"RADIO_BUTTON","value":"Yes"},"$revision":{"type":"__REVISION__","value":"1"},"created_by":{"type":"CREATOR","value":{"code":"elliott.weaver@euromoneyplc.com","name":"Elliot
Weaver"}},"requestor":{"type":"USER_SELECT","value":[{"code":"elliott.weaver@euromoneyplc.com","name":"Elliot
Weaver"}]},"Text_area":{"type":"MULTI_LINE_TEXT","value":"API is used by Front-end sites to obtain the preferences for a specific authenticated Users, Back-end systems can search or access specific Users Preferences to extract items e.g. Newsletter distribution lists. Change events to User Preferences can trigger change request to other systems e.g. Marketo, Salesforce, Preference Centre."},"Date":{"type":"DATE","value":"2020-12-07"},"risk_level":{"type":"DROP_DOWN","value":"High"},"requestor_email":{"type":"LINK","value":"elliott.weaver@euromoneyplc.com"},"requestor_phone":{"type":"LINK","value":""},"updated_by":{"type":"MODIFIER","value":{"code":"elliott.weaver@euromoneyplc.com","name":"Elliot Weaver"}},"Link":{"type":"LINK","value":"https://confluence.euromoneydigital.com/display/BAC/User+Service+API"},"internet_availability_radio":{"type":"RADIO_BUTTON","value":"No"},"$id":{"type":"__ID__","value":"8"}},{"payment_information":{"type":"DROP_DOWN","value":null},"record_number":{"type":"RECORD_NUMBER","value":"7"},"access_permissions":{"type":"USER_SELECT","value":[]},"personal_information":{"type":"DROP_DOWN","value":null},"requestor_business_unit":{"type":"SINGLE_LINE_TEXT","value":""},"number_of_records":{"type":"DROP_DOWN","value":"Moderate

'<100,000'"},"Attachment":{"type":"FILE","value":[]},"project_name":{"type":"SINGLE_LINE_TEXT","value":"BCA Chart Explorer"},"project_types":{"type":"CHECK_BOX","value":["Application"]},"confidential_radio":{"type":"RADIO_BUTTON","value":"No"},"created_datetime":{"type":"CREATED_TIME","value":"2020-11-02T21:17:00Z"},"third_party_hosting_radio":{"type":"RADIO_BUTTON","value":"Yes"},"updated_datetime":{"type":"UPDATED_TIME","value":"2020-11-03T15:29:00Z"},"confidential_information":{"type":"DROP_DOWN","value":null},"Drop_down":{"type":"DROP_DOWN","value":"In-House"},"Status":{"type":"STATUS","value":"In Progress"},"Assignee":{"type":"STATUS_ASSIGNEE","value":[{"code":"carlos.lopes@ndr.com","name":"Carlos Lopes"}]},"attestation_table":{"type":"SUBTABLE","value":[{"id":"4489","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that servers are deployed away from the Internet unless they are required externally"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S34"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4492","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that port scanning is in place with the IT security team"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S33"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization?s approved baseline is discovered, an alert should be generated and reviewed."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4493","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Restrict ports and protocols to minimum required"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S31"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that only ports, protocols, and services with validated business needs are running on each system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4494","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Enable anti-exploitation features"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S30"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4495","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Deploy Anti-virus to systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S29"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.\n\nRefer to the IT Security team to assist with software installation.

"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4496","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Remove any unnecessary services from supporting systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S26"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Uninstall or disable any unauthorized browser or email client plugins or add-on applications."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4497","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all systems are logging relevant information, consistently"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S22"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that local logging has been enabled on all systems and networking devices. System logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4498","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use a non-administrative account where possible"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S20"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4499","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that unsuccessful login of admin accounts are logged"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S18"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4500","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure default passwords are changed for devices and systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S17"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4501","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Control of administrative accounts"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S16"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4502","value":{"summary

":{"type":"SINGLE_LINE_TEXT","value":"Only use administrative accounts where absolutely
necessary"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S15"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Minimize administrative privileges and only use administrative accounts when
they are required. Implement focused auditing on the use of administrative
privileged functions and monitor for anomalous behavior.\n\nAdministrators must
not use privileged accounts for day-to-day tasks (email, internet browsing etc.)
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4503","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Regularly receive and review vulnerability scans to
ensure issues have been
resolved."},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S14"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Regularly compare the results from consecutive vulnerability scans to verify
that vulnerabilities have been remediated in a timely manner. Utilise a
risk-rating process to prioritise the remediation of discovered vulnerabilities.
Remediate according to Company approved
timescales."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security
_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4504","value":{"summar
y":{"type":"SINGLE_LINE_TEXT","value":"Ensure that, where possible, updated take
place
automatically"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S13"},"acknowledgem
ent":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","
value":"Deploy automated patch management tools and software update tools for
operating system and software/applications on all systems for which such tools
are available and safe. Patches should be applied to all systems, even systems
that are properly air
gapped."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_com
ments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4505","value":{"summary":{
"type":"SINGLE_LINE_TEXT","value":"Properly configure vulnerability scanning in
authenticated
mode"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S12"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"\
nPerform authenticated vulnerability scanning with agents running locally on
each system or with remote scanners that are configured with elevated rights on
the system being tested. Use a dedicated account for authenticated vulnerability
scans, which should not be used for any other administrative activities and
should be tied to specific machines at specific IP addresses.\n\nContact the IT
Security team to assist you with this.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4506","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Ensure that vulnerability reports are sent to the
central logging
solution"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S11"},"acknowledgement":
{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value
":"Correlate event logs with information from vulnerability scans to fulfill two
goals. First, personnel should verify that the activity of the regular
vulnerability scanning tools is itself logged. Second, personnel should be able
to correlate attack detection events with prior vulnerability scanning results
to determine whether the given exploit was used against a target known to be
vulnerable."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security
_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4507","value":{"summar
y":{"type":"SINGLE_LINE_TEXT","value":"Ensure that the application is setup to

be scanned by the vulnerability assessment tool (arranged via IT security)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S10"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Business owner to approach IT Security and ensure that the application/system is added to the Qualys and Netsparker vulnerability scanning shedules.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4508","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Setup remote acces to your application securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S7"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4509","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that underlying operating systems are appropriately secure"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S6"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Maintain documented security configuration standards for all authorized operating systems and software. Hardened operating system images should be used. \n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4510","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Use of DHCP in assigning IP addresses"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S1"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol, (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.\n\n*Refer to the IT Security and/or Network team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4511","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Secure remote access to the network"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N6"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication. This control is likely to need to be implemented by the application developers but also refers to remote access provided to the servers upon which the application sits. The business is accountable for ensuring that these controsl are in place for this application. Supporting infrastructure or developers may be responsible for implementing the control.\n\n*Refer to the IT Security team before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4512","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Keep network devices updated"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N2"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Engage with IT security and infrastructure teams to ensure that all in-scope components are added to the Qualys scanning schedule.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":

{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4513","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Manage network device securely"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N1"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Manage network devices using two-factor authentication and encrypted sessions. This control requires any administrative access to infrastrastructure and network devices to enfore two-factor authentication. Web sessions should use HTTPS. Console sessions should be over SSH.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4514","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Don't deploy development artefacts to production systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A25"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4515","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Train software developers in secure coding techniques (they must be up to date on their training)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A24"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensure that all software development personnel receive training in writing secure code for their specific development environment."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4516","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Harden databases"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A23"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4517","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Separate production and non-production systems"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A22"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Maintain separate environments for production and non production systems. Developers should not have unmonitored access to production environments."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4518","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Do not display system error messages to end-users"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A21"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Do not display system error messages to end-users (output sanitization)."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4519","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Arrange application vulnerability scanning with IT security"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A20"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular

recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.\n\n*Refer to IT Security before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4520","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure error checking is in place for all input"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A19"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4521","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that all versions of supporting software are up to date"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A17"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4522","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure authentication credentials are hashed (and salted)"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A16"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Verify that all authentication files are hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4523","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure attempts to access deactivated accounts are logged centrally"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A12"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Monitor attempts to access deactivated accounts through audit logging. Logs should be forwarded to the central SIEM managed by IT Security.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4524","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Setup account lockouts after failed login attempts in line with policy"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A11"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Use and configure account lockouts such that after 5 failed login attempts the account is locked for at least 30 minutes."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4525","value":{"summary":{"type":"SINGLE_LINE_TEXT","value":"Monitor accounts by linking to the Identity and Access Management solution or by implemeting manually. Seek guidance from Information Security"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A10"},"acknowledgement":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Monitor account usage to determine dormant accounts, notifying the user or user?s manager. Disable such accounts if not needed, or document and monitor

exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce
members."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_co
mments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4526","value":{"summary":
{"type":"SINGLE_LINE_TEXT","value":"Create a process to identify and disable users after a period of
inactivity"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A9"},"acknowledgement"
:{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","valu
e":"Accounts exceeding 90 days of inactivity should be automatically disabled.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4527","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Link account disabling processes to Identity and Access Management solution or setup and document a manual
process"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A8"},"acknowledgement":{"
type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":
"Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails. No direct action is required if the application/system is integrated with Active Directory for user authentication. Non-active directory accounts and non-permanent staff require attention.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4528","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Ensure that all accounts have an expiration date in line with
policy"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A7"},"acknowledgement":{"t
ype":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"
Ensure that all non-permanent/contractor accounts have an expiration date that is monitored and enforced. Ensure all accounts are disabled after 90 days of inactivity.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4529","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Ensure appropriate access control lists are in place"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A3"},"acknowledgement":{"ty
pe":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"P
rotect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their
responsibilities."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"se
curity_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4530","value":{"
summary":{"type":"SINGLE_LINE_TEXT","value":"Ensure system patches are automatically identified.
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S41"},"acknowledgement":{"type":
"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Deplo
y automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_com
ments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4531","value":{"summary":{
"type":"SINGLE_LINE_TEXT","value":"Limit access to scripting

tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S42"},"acknowledgement":{"t
ype":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"
Limit access to scripting tools (such as Microsoft PowerShell and Python) to
only administrative or development users with the need to access those
capabilities."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"securi
ty_comments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4532","value":{"summ
ary":{"type":"SINGLE_LINE_TEXT","value":"Ensure that access to systems is
explicitly
defined"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S46"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"\nProtect systems with firewalls or port filtering tools. Ensure tools are
configured with a default-deny rule that drops all traffic except those services
and ports that are explicitly allowed.\n\n*Refer to the IT Security team before
answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4533","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"Network permiter firewall
"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"S47"},"acknowledgement":{"type":
"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"Ensur
e that network perimeter firewalls are in front of externally facing servers,
actively blocking network threats and receive regular signature
updates.\n\n*Refer to the IT Security and/or Network teams before
answering"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4534","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Third party hosted network devices to be
securely
managed"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"N12"},"acknowledgement":{
"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value"
:"If any internally owned network devices are situated at a third party site
(e.g WAN/MPLS extension), remote administrative access must take place over a
secure VPN tunnel. \n\n*Refer to IT Security before answering.
"},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comments":
{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4535","value":{"summary":{"type":
"SINGLE_LINE_TEXT","value":"DAST/SAST
tools"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A34"},"acknowledgement":{"t
ype":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","value":"
Apply static and dynamic analysis tools to verify that secure coding practices
are being adhered to for internally developed
software."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_c
omments":{"type":"MULTI_LINE_TEXT","value":""}}},{"id":"4536","value":{"summary"
:{"type":"SINGLE_LINE_TEXT","value":"Enable contact from external security
researchers"},"ctrlID":{"type":"SINGLE_LINE_TEXT","value":"A35"},"acknowledgemen
t":{"type":"DROP_DOWN","value":null},"attestation":{"type":"MULTI_LINE_TEXT","va
lue":"Establish a notification process to accept and address external reports of
software vulnerabilities, including providing a means for external entities to
contact your security
group."},"project_comments":{"type":"MULTI_LINE_TEXT","value":""},"security_comm
ents":{"type":"MULTI_LINE_TEXT","value":""}}}]},"risk_score":{"type":"NUMBER","v
alue":"10"},"payment_radio":{"type":"RADIO_BUTTON","value":"No"},"personal_radio
":{"type":"RADIO_BUTTON","value":"No"},"$revision":{"type":"__REVISION__","value
":"2"},"created_by":{"type":"CREATOR","value":{"code":"carlos.lopes@ndr.com","na
me":"Carlos
Lopes"}},"requestor":{"type":"USER_SELECT","value":[{"code":"carlos.lopes@ndr.co
m","name":"Carlos Lopes"}]},"Text_area":{"type":"MULTI_LINE_TEXT","value":"Chart

Explorer is the Interactive Charting platform at BCA that replaces the BCA Analytics platform. It consists of two React SPA apps hosted in the PHP-based www.bcaresearch.com website: the Chart Rendering app, which is responsible for the rendering of financial charts using the D3 library; the Chart Desktop app, which allows users to search, save, and build chartbooks from the interactive charts."},"Date":{"type":"DATE","value":"2021-01-11"},"risk_level":{"type":"DROP_DOWN","value":"Low"},"requestor_email":{"type":"LINK","value":"carlos.lopes@ndr.com"},"requestor_phone":{"type":"LINK","value":""},"updated_by":{"type":"MODIFIER","value":{"code":"carlos.lopes@ndr.com","name":"Carlos Lopes"}},"Link":{"type":"LINK","value":"https://ndrbugz.atlassian.net/wiki/spaces/BCA/pages/504627215/Chart+Explorer+-+Technical+Description"},"internet_availability_radio":{"type":"RADIO_BUTTON","value":"Yes"},"$id":{"type":"__ID__","value":"7"}}],"totalCount":null}