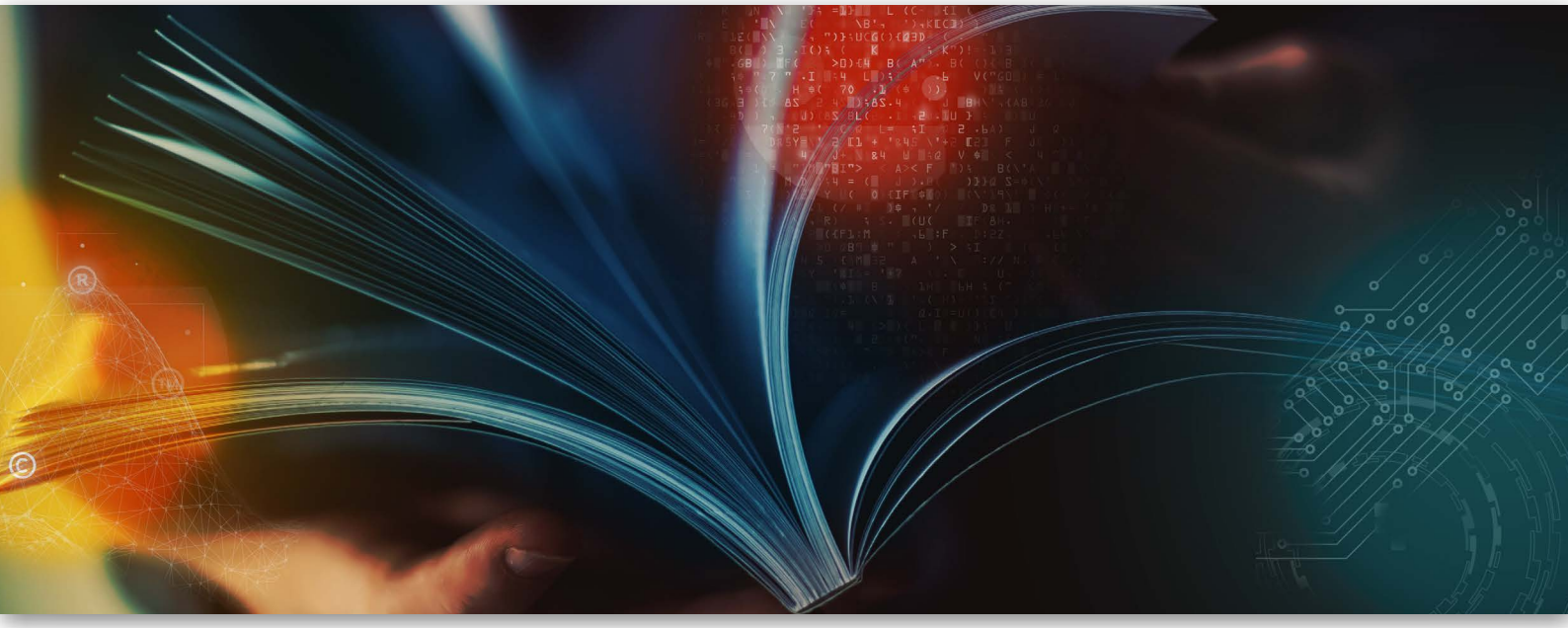
Zacco



Our commitment to Security, Compliance and Privacy

zacco
DIGITAL TRUST

Contents

1. Our commitment to clients, customers and colleagues

The benefits of digital trust and our commitment to the digital trust process.

In this increasingly connected digital world, all organisations, irrespective of their area of operations, need to ensure that they have the appropriate level of digital trust. In other words, the measure of confidence stakeholders will have in an organisation's ability to protect their private information and secure their data. Keeping your organisation's internal employee and client data safe is imperative but it can also contribute to building your brand reputation. It can even help you to identify completely new assets and opportunities for your business. We have developed this whitepaper to offer insight into how we ensure confidentiality and security of data and information, helping our clients to quickly identify any requirements they may have in these areas and to demonstrate how we can accommodate them.

Today, it is rarely enough to secure your intellectual property via the traditional means of registering patents, designs, copyrights and trademarks alone. Securing your digital IP rights and corporate information against data theft and fraud is one of the most critical business priorities, alongside keeping up with technology and rapidly evolving data protection legislation.

We have a comprehensive portfolio of services available, designed to meet the current and future needs of Intellectual Property and Digital Asset protection. Our client's and colleague's needs are often based on extensive regulatory requirements and are often most restricted within the areas of Compliance, Security and Privacy.

By combining traditional IP disciplines with cyber security, software development and online brand protection, we take care of your ideas, innovations, data, private information and all of your other intangible assets that you literally cannot put your finger on. We protect them, give you complete ownership and make them yours to keep – both now and in the future.

More than just words, we take security seriously

We use the same protection systems and processes internally that we offer to clients and partners.

We are dedicated to ensuring that we protect client data, privacy and information security to the highest standards. We are also committed to helping you build trust across all of your systems, connected or otherwise, so that you can focus building your organisation and growing your brand. We have collected a checklist of questions that you can use to maintain assurance that your current service provider ensures your digital trust and you will find this in the appendix.

The Zacco Cyber Defence Centre (CDC) continuously monitors all incoming, outgoing and internal data traffic. We take data security very seriously and have implemented a number of processes to mitigate the risk of unauthorised access. The CDC reports directly to the Zacco Group top management.

1.1 Quality

At Zacco, quality has always been our main priority; we are committed to adhering to the highest standards and to being the best that we can be. Quality continues to remain at the forefront of how we operate and we believe that our hard work and international recognition speaks for itself but our ISO Certification demonstrates an independently certified commitment to quality and to international best practice.

Our TUV SUD accreditation covers our Cyber Defence Centre, our Digital Forensics team in Sweden and our relevant IT Security and Information Management systems under the following International Standards:

- ISO/IEC 27001:2013 for Information Security
- ISO/IEC 27701:2019 for Privacy Information
- ISO 22301:2019 for Business Continuity Management Systems

Stakeholder trust is continuously developed but the standards demonstrate our belief that only the highest level of quality is acceptable in everything that we do. We are implementing the most comprehensive best practice available and we will strive to handle your information appropriately, responsibly and securely as well as endeavour to prepare

for the unexpected. Above all, they offer independent verification of our commitment to privacy, data security and continuity for both our colleagues and our clients. This is a corporate promise and the new certification is a demonstration of our commitment to that fact.

These standards covers much of what goes on behind the scenes, including our information control systems, our underlying IT infrastructure and our business continuity, risk management and incident response processes.

We believe this achievement in all three standards demonstrates our continued commitment to the highest standards. Our Information Security and Privacy Control Functions have also been developed to align with the latest version of the international standard ISO/IEC 27002.

1.2 Digital Trust

We have been helping visionaries and innovators to protect their assets for over 150 years. A role that often requires as much creativity, accuracy and innovation from us as from those we work with. With today's growing need to protect everything from ideas and inventions to algorithms, privacy and data, we have added the expertise necessary to build your digital trust and protect your organisation's assets. When the world changes, so do we, and we want to give you the best possible conditions for you to grow your business while we keep it safe. We identify, protect and secure your assets with a new approach to covering all aspects of intellectual property.

Many clients find our commitment to information security invaluable. We manage their intellectual property, we secure their networks and systems against intrusion and we train their colleagues in how to treat information and data responsibly. It is with this in mind that we consider our ISO achievement to be the foundation for expanding digital trust between our colleagues, clients and partners.

We believe that part of developing stakeholder trust is knowing that those who handle and secure your information are doing so responsibly. We call it Zacco IP 360 and you can learn more about this on our website.

1.3 Zacco – One process to secure digital trust

If you want to establish digital trust, or if you need assistance in identifying and securing your assets, we have the ability and proven experience to help you do so. Working within Intellectual Property, the protection and security of private information governs everything that we do.

Our objective is simple – Work with Zacco and you can rest assured that your data is safe and that we have taken all the precautions we can to mitigate risks of data loss or theft. Data and information security should not be something that our clients worry about and we have taken steps to ensure that this is the case.

We have worked with companies of all sizes, from Fortune 500s to small start-ups, giving us a unique perspective on how each company approaches their private information and data security. This means that we are often able to quickly develop an understanding of how they interact with their systems, what they consider most important and therefore what their individual information security needs are likely to be.

As a client of Zacco, this means that it is easy to take the first step in either direction. If you need assistance with your intangible assets, you can easily switch to our 360° perspective and secure all your organisation's innovation, identity and digital assets collectively. Similarly, if we are already working with you to secure the value if your IP portfolio, we can offer you additional security and protection from potential threats to your underlying network infrastructure, such as from data breaches and unauthorised access.

You can follow the process and read more on our website.

2. Security

Security is an integral part of Zacco operations. We maintain rigorous standards and security procedures to safeguard knowledge, information and business continuity through the adoption of multiple administrative, physical and technical precautions and defences.

Our security processes and organisational measures are regularly tested to assess their effectiveness and all controls are regularly reviewed and adjusted to ensure they remain fit for purpose in maintaining a consistently high level of protection. Such procedures and processes govern all of our operations. Our commitment to information security, information privacy and business continuity is ongoing and will continue to be independently verified as part of our ISO Certification requirements.

We limit access only to areas required for an employee to complete tasks associated with their role, conduct regular reviews of system access lists and implement immediate termination of access for personnel who no longer require it. We also employ minimum complexity and strength requirements for user credentials, Multi-Factor Authentication (MFA) and the use of industry standard levels of encryption.

We have robust and rigorously assessed systems in place that are designed to, wherever possible, mitigate risks to the security of private information. We are committed to maintaining comprehensive business continuity processes to safeguard access and quickly restore service in the event of a catastrophic system failure. All mobile devices are secured and any that are able to access confidential information are encrypted as standard. We also have the ability to track and remotely wipe any relevant device associated with Zacco. The data of every client who has allowed their confidential information to be accessible via the cloud is kept separate from the data of other clients or customers. Access is restricted, monitored and logged, irrespective of who is accessing the system.

Our Cyber Defence Centre (CDC) continuously monitors all incoming, outgoing and internal data traffic, as part of protecting our network infrastructure and communications. The CDC is responsible for our intrusion detection, monitoring and logging capabilities as well as general network health, such as segmentation, updating or patching, and our firewalls.

2.1 Personnel Security

As part of the Zacco on-boarding process all employees:

- sign non-disclosure agreements as standard
- receive a background check during the recruitment process, if they will have access to have sensitive information as part of their role.
- receive training in Zacco's rules and regulations, system access, data security and information awareness
- receive training in 'rules based access' including how to manage data responsibly
- receive a detailed explanation of our approach to quality

This information is continuously updated and reviewed throughout employment.

Access to information is managed dependant on an individual's role and interaction with specific clients. This secures against potential Conflicts of Interest (COI) and ensures Segregation of Duty (SoD) as access is only granted to information relevant or necessary for an individual to fulfil their role. All system and user behaviour is monitored through logging with flows, although such monitoring is defined within strict boundaries to ensure that it maintains adherence to our information security, privacy and data protection obligations as well as our company policies and

standards. It can also be used to identify unusual behaviour, mitigating the risk of a data breach.
Zacco employees receive training and regular updates on organisational policies and procedures as part of a program called BeAware. This includes security requirements and education as well as training on the correct use of information-processing facilities.

We have a comprehensive Information Security Handbook, compliance with which is mandatory for all employees and subcontractors of Zacco. Designed to mitigate the risk of security threats and prevent breaches, the handbook details the appropriate use of systems or mobile devices as well as how to handle printouts, removable media and storage within cloud solutions.

The handbook also acknowledges what we say or do within public spaces or conferences, both online and offline, and the importance of remaining aware of surroundings. The intention of this document is to assist both our colleagues and subcontractors in conducting their day-to-day business while remaining aligned with Zacco's information security requirements and goals.

2.2 Our Security Programme

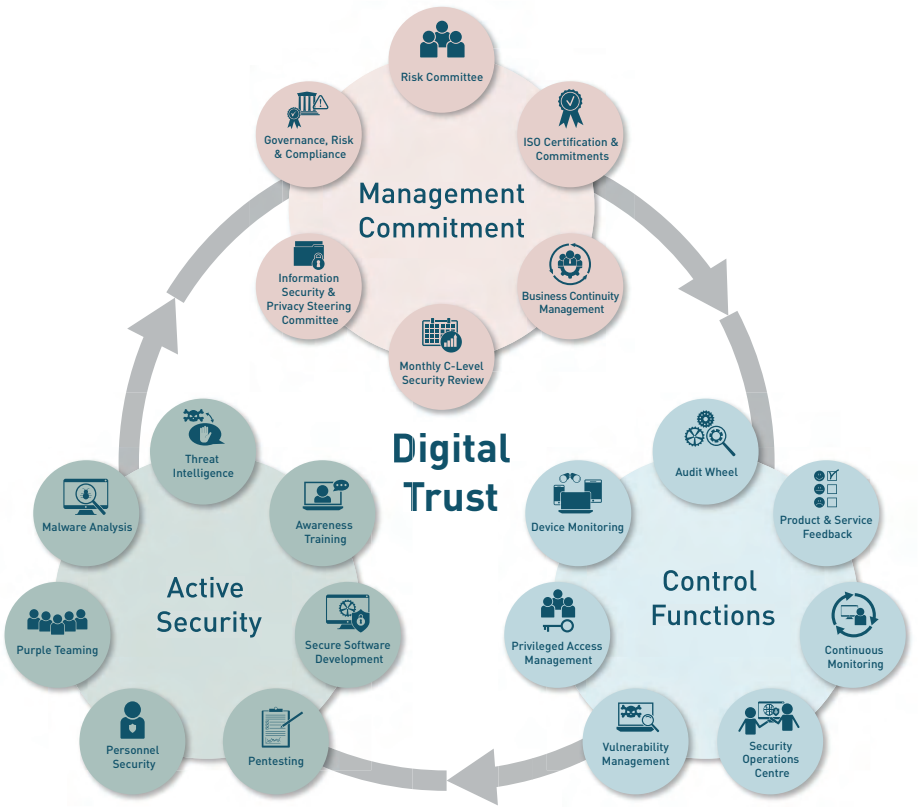
As we meet the needs of our clients and customers, our security programme adapts both internally and to the needs of the marketplace. Part of this adaptation consists of regular security and service reviews between product teams, our privacy steering committee and our management team. This guides our understanding of where we are with respect to security and helps us to identify if this is where we need to be.

Such reviews help us to recognise and counteract emerging threats on the digital landscape, develop our personnel to ensure we have the necessary skills to work together effectively, and maintain our focus on data security and the protection of private information.

Reporting directly to the Zacco Group top management, we have a dedicated Information Security and Privacy Steering Committee (ISPSC). The committee is a cross-functional team of top management and stakeholders responsible for ownership and updating of our Information Security Management Systems, Personal Information Management Systems and Business Continuity Management Systems.

As acknowledged previously, we have robust and rigorously assessed systems in place that are designed to mitigate potential risks to private information wherever possible. We are committed to maintaining comprehensive business continuity processes to safeguard access and quickly restore service in the event of a catastrophic system failure.

An internal audit programme ensures continued compliance to the requirements of the ISO/IEC 27001 and other ISO standards. This will involve regular ongoing audits of the ISMS/PIMS/BCMS as specified in the programme schedule. Zacco carries out the audit programme with input from our information security functions, business management and relevant resources within different employee functions. The resourcing of the internal audit is reviewed on a regular basis as part of the management review and is maintained to ensure continued commitment and compliance. The audit programme covers all information assets within Zacco. Input and discussion with additional involved parties will take place where appropriate.



2.3 Product / Service Security

Zacco offers access to various systems as part of our services and many of these store and process information that is often considered sensitive or confidential. Ensuring the correct processes and procedures are in place to handle such information securely is integral to our commitment to quality.

All of our products and services are designed with security at their core. We adopt a comprehensive security model throughout the development process, assessing potential user interaction, isolating service networks from the wider system, and incorporating encryption as standard wherever necessary.

All software is developed via cross-functional teams incorporating specialists from across the organisation in the areas of information security, cyber defence, secure software development and data protection. We identify, acknowledge and address the security implications of each design decision throughout the development process from design and implementation through testing and verification. Only when we are confident in the secure foundations of a product or service will it be released to market or deployed.

2.4 Internal Security Measures

2.4.1 Access Management and Control

Access to information and servers is limited based on an employee's access requirements and authorisation, ensuring that each employee only has access to that which is required in order to complete their role and responsibility. The principle of Segregation of Duty (SoD) is strictly followed while provisioning access and privileges to users. Privileges and roles that manage critical functions and processes are brought under shared responsibility with more than one person or department. This ensures that information is not inadvertently or deliberately shared with or viewed by those who do not need to access it, which serves to maintain the integrity of the data itself as it cannot be edited by those without authorised access. It also mitigates the risk of breach or data loss from stolen passwords. Access is revoked when an employee leaves or changes position and all access is reviewed periodically to ensure that the system is still fit for purpose.

2.4.2 24/7/365 Data Flow Monitoring and Security Testing

As part of our standard operations, we continuously monitor all of our digital environments to ensure that our internal IT systems remain secure. These managed security services include Security Information and Events Monitoring (SIEM), Privileged Access Management (PAM) and Extended detection and response (XDR) as alongside Threat Intelligence operated by our own SOC and CDC. We also perform vulnerability scans and penetration testing of all environments on a regular basis.

2.4.3 Backup and Data at Rest

All data at Zacco is backed up across multiple sites as part of our general business continuity plans and we conduct regular system and stress tests on backups to ensure ongoing access. Backups that that are kept off-site are contained within locked storage units inside secure monitored sites and are only accessible to authorised personnel, as defined by the organisation's security policies.

Cryptographic protections for backups are employed in accordance with industry standards.

Data 'at rest' is also encrypted for all critical systems and data elements. Encryption follows a standard procedure, using validated encryption algorithms with a minimum decryption key length and Zacco adopts a formal encryption key management process, which itself is subject to regular review by the ISPSC.

2.4.4 Business Continuity and Disaster Recovery

Zacco's Business Continuity, Incident Response and Recovery, and Disaster Recovery Plans are ISO-Certified. They are prioritised according to their formally assessed risk and the level of organisational risk tolerance. Together, the plans form an integral part of our operational procedures and they are regularly reviewed and tested by the ISPSC, and updated as necessary, to ensure they remain proportionate, fit for their intended purpose, and able to restore any affected system in a timely manner should an incident occur.

2.5 External and User-Based Security Measures

We are committed to maintaining comprehensive business continuity processes to safeguard your uninterrupted access. We have implemented a number of restrictions and protections for users when accessing our systems, including the following:

Access Restriction – Password Management Policies, Privilege Access Management (PAM) and Multi-Factor Authentication (MFA) to mitigate the risk of lost or stolen user credentials.

Encryption – Industry standard encryption of data at rest and in transit. When logging in to, or operating within, one of our systems you will be covered by a secured data protocol

Revision Control – Documents and System information can only be viewed or edited by those with the necessary access level. A revision log records every change made and by whom.

Monitored Access - Our Cyber Defence Centre continuously monitors all incoming, outgoing and internal data traffic, to detect and identify malware, unusual behaviour or processes and unexpected activity. Our XDR platform and SIEM correlates security telemetry from within our network, from applications, cloud based services and throughout endpoints to improve threat detection, investigation and response.

Software Updates – We regularly check software capability and security requirements as part of our scheduled maintenance, releasing updates as necessary. In the case of critical issues, we will patch or provide a hotfix as soon as reasonably possible.

Vulnerability Management – We regularly evaluate our systems to identify potential vulnerabilities. We use such ongoing evaluation to recognise possible threats, minimise their attack surface and to mitigate their effectiveness.

3. Compliance

3.1 ISO Accreditation and Certification

Our TUV SUD accreditation covers our Cyber Defence Centre, our Digital Forensics team in Sweden and our relevant IT Security and Information Management systems under the following International Standards:

- ISO/IEC 27001:2013 for Information Security
- ISO/IEC 27701:2019 for Privacy Information
- ISO 22301:2019 for Business Continuity Management Systems

In our quest for quality in everything that we do, we have started the process internally to pursue accreditation in the following International Standards:

- ISO 9001:2015 for Quality Management Systems
- ISO 14001:2015 for Environmental Management Systems
- ISO 45001:2018 for Occupational Health and Safety Management Systems

Our Information Security and Privacy Control Functions have been also developed to align with the latest version of the international standard ISO/IEC 27002.

3.2 Governance

3.2.1 Regulatory

Zacco operates under one single brand but consists of separate legal entities operating across multiple jurisdictions and territories, each with their own regulatory requirements. You can find out more about Zacco entities here: https://www.zacco.com/regulatory/

We adhere to the regulatory requirements of data sharing as laid down by the GDPR and all personal information is stored on servers based within Europe.

When it is necessary to transfer such information outside of Europe we ensure that it is transferred according to the requirements in GDPR, in a secure manner and stored under the same stringent regulations that we follow ourselves.

Your personal data will be retained for the time required to fulfil the purpose for which it was collected and will be governed by our legal obligations throughout that time

3.2.2 Ethical

All of our consultants will have the professional certification necessary to advise in their respective areas of expertise and will be subject to both local and international regulatory restrictions. Many of our colleagues are European Patent Attorneys (EPA) and, as such, subject to all relevant EU legislation.

Our consultants are covered by extensive professional indemnity insurance in their respective practice areas and jurisdictions, which also includes global coverage for those working with international clients.

Please contact us if you require more specific information on adherence to respective regulatory requirements or with any questions about our comprehensive insurance coverage.

3.2.3 Code of Conduct

Zacco's Code of Conduct as defined by policies, guidelines, manuals and business processes provides the framework for how Zacco and its employees shall act in terms of environmental considerations, business conduct, business relations, workplace practices and human rights. The Code of Conduct shall be based on the following principles:

- The UN Universal Declaration of Human Rights
- The UN Global Compact initiative
- The UN Convention against Corruption
- The OECD Convention combatting Bribery of Foreign Public Officials
- The ILO Declaration on Fundamental Principles and Rights at Work

4. Privacy

Working within Intellectual Property and Network Security, Privacy is a critical aspect of our operations, integral to client trust and forms the basis of everything we do.

We are committed to securing personal information. When you request our services or use our website we collect, use and process your personal data. The protection and confidentiality of this personal data is important to us, and we are determined to secure and use it appropriately. Aside from the securing the data digitally within our systems, we also have robust policies and processes in place to ensure that all personal information is handled in adherence to, and often beyond, current regulatory requirements.

Our approach to privacy has been developed from our adherence to the following values:

- **Commitment to Quality** – We are committed to quality of the highest standards and we believe our ISO certification is demonstration of our commitment to Information Security, Privacy and Business Continuity.
- **Privacy as standard** – Information Security and Privacy is built in to all of our products and services as standard and our Privacy Policy acts as a foundation for all current and future development.
- **Data Integrity** – All Information collected is used appropriately. It is retained and used only for its intended proportionate and legitimate purpose, it is kept up to date and it is stored securely.
- **Accountability** – When data is shared with us, we are responsible for keeping it safe. We take that responsibility seriously and handle your data with care by taking steps, wherever necessary, to ensure that it is secured.
- **Control** – You can choose what personal data you share and what such data can be used for
- **Transparency** – You are always able to request an overview of your personal data.
- **Security** – Our responsibilities are backed up by a comprehensive security plan including technical and

physical security measures to ensure that data entrusted to us is kept secure.

- **Third Party Assessment** – We only work with trustworthy vendors and suppliers who are committed to information security and data integrity.

Here you can read our Privacy Policy, describing how we process and protect your personal information: https://www.zacco.com/privacy-policy/

5. Security Operations Centre and Threat Intelligence

Zacco operates our own Cyber Defence Centre (CDC) and Security Operations Centre (SOC) that runs continuously and can be potentially be offered to clients who require additional levels of protection. The SOC is set up to incorporate state of the art services, powered by IBM. The personnel are skilled experts with accreditation and certification including ISACA, ISC2, among others.

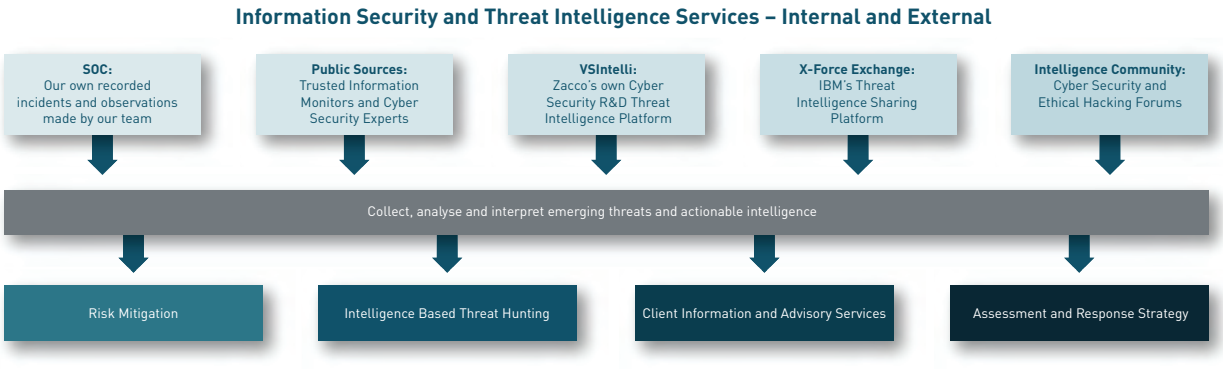
Our SOC provides three main services to our business:

- **Threat Monitoring.** Logs from enforcement points located throughout the network generate most of the alerts, each of which is analysed and assessed.
- **Threat Hunting**. Proactive threat detection and identification.
- **Incident Response**. Combining multiple tools and data points to provide efficient and effective remediation, resolving and removing threats directly where possible.

Part of our CDC includes a Digital Forensics research lab, based out of Sweden, which continuously hunts for new threats and investigates ongoing attacks using the latest in digital forensic technology.

You can find more information here: https://www.zaccodigitaltrust.com/services_area/digital-trust-labs/

6. Risk Management



Managing risk is part of governance and leadership functions. It is fundamental to how an organisation creates and protects its value, as well as supporting the achievement of corporate objectives.

The Zacco commitment to information security, information privacy and business continuity is ISO Certified, and will continue to be independently verified, as part of our ISO obligations. We will work hard to maintain your digital trust as we believe that part of feeling secure is knowing that those who handle your information are doing so responsibly.

We take a strategic approach to risk management and are actively working towards achieving International Risk Management Guidelines ISO 31000:2018. Our Risk Management Framework adopts many of the central tenets of ISO

certification and its purpose is to assist us in integrating risk management processes into all significant business activities and functions. All aspects of risk control are shared with their respective owners and risk remediation is developed collectively with adherence to ISO standards as our foundation.

The scope is designed to be applicable to all Risk Management functions, existing or under development, within Zacco. Any exceptions to these are strictly discouraged and require prior approval by the members of the Zacco Management Team. We have adopted comprehensive measures to identify and mitigate potential risks including regular penetration testing and 'red-teaming' as well as conducting regular security maturity assessments of our systems and users.

As part of our commitment to ISO22301, we have also taken steps to prepare for the unexpected, implementing robust processes and systems in place to mitigate potential risks of data loss or catastrophic network infrastructure damage. This system includes multiple backup sites, all of which are also actively monitored by the SOC and CDC.

7. Verification of our continuous commitment to improvement

We believe that our adherence to ISO standards demonstrates our commitment to both quality and accountability. A requirement of our regular ISO audits commit us to consistently maintaining or improving our current high standards.

We regularly review all of our obligations, systems, processes and policies to ensure that they remain fit for purpose and that we are continuing to adhere to the responsibilities contained therein, as well as to all applicable laws of the territories within which we operate.

For more information, please contact our Chief Information Security Officer at CISO@zacco.com

8. Links

You can find further information on any of the subjects included here through one of the links below:

https://www.zacco.com
https://www.zacco.com/privacy-policy/
https://www.zacco.com/web-privacy-policy/
https://www.zacco.com/environmental-policy/
https://www.zacco.com/quality-policy/
https://www.zacco.com/regulatory/
https://www.zacco.com/terms-of-use/
https://www.zacco.com/terms-of-business/

https://www.zaccodigitaltrust.com/
https://www.zaccodigitaltrust.com/general-terms-and-conditions/

Appendix A – Digital Trust Checklist

What you should expect from your Intellectual Property provider

1. Has your company developed defined data governance policies for handling confidential information?	☐ No such data governance policies exist. ☐ Informal and undocumented policies exist. ☐ Formal policies exists and are documented. ☐ Formal policies exist and are documented. The policies are regularly (at least annually) reviewed and communicated throughout the organisation and to clients.
2. Does your company review its information security and data protection policies to ensure all risks are mitigated wherever possible?	☐ Policies are not reviewed. ☐ Policies are reviewed by internal resources on an ad hoc basis. ☐ Policies are reviewed by external security consultants on an ad hoc basis. ☐ Policies are reviewed internally on a recurrent basis (at least annually), but not by external information security consultants. ☐ In addition to recurrent internal reviews, external information security consultants are engaged to conduct regular reviews (at least annually) of all policies.
3. How does your company receive vulnerability and threat information?	☐ Threat and vulnerability information is not proactively collected. ☐ An internal IT department is responsible for proactively collecting and researching both threat and vulnerability information. ☐ The company has a well documented approach to vulnerability management which leverages internal IT and external consultants to identify threats and vulnerabilities. Automated processes exist to circulate relevant security alerts and advisories to appropriate resources throughout the company.
4. Has your company established risk management processes that are communicated (and agreed upon) to executive leadership and company stakeholders?	☐ Risk management processes are not established. ☐ Risk management processes are informally established. ☐ Risk management processes are formally established and communicated to all relevant personnel. ☐ Risk management processes are established, managed, and agreed upon by all organisational stakeholders. These risk management processes are based on organisational risk tolerance and the organisation's role in its specific sector, supported by executive leadership, clearly communicated, and consistently enforced throughout the organisation. The processes are reviewed and updated on a regular basis (at least annually), and reported to external stakeholders, including teh relevant regulatory bodies in accordance with all reporting and retention requirements.

5. Has your company achieved ISO27001 certification?	☐ No
	☐ No, but we have initiated the certification process
	☐ Yes, and we have initiated renewal process
	☐ Yes, and we have obtained certification or renewal within the past 3 years
6. Does your company centrally administer identities and credentials for both devices and users?	☐ Identities and credentials are not centrally administered for devices or users.
	☐ Identities and credentials are centrally administered for some authorised devices or users.
	☐ Identities and credentials are centrally administered for all devices and users.
	☐ Authorised users and devices are formally administered centrally and according to the organisation's policy.
7. Does the company ensure users, devices, and other assets use authenticated logins (e.g. single-factor, multi-factor)?	☐ The company has no formal policy regarding ensuring authentication methods.
	☐ The company has ad hoc implementation of authentication methods based on transaction risk.
	☐ The comopany has a formal policy ensuring authentication methods are the appropriate strength and mechanisms for transactional risk.
	☐ The company has a formal policy ensuring authentication methods are the appropriate strength an mechanisms for transactional risk and addresses nonorganisational users, services/service accounts, device authentication, and reauthentication.
8. Are all company employees and/or other users informed of and trained in best practice information security and cybersecurity topics? (Including, but not limited to: password management, internet hygiene, phishing/spear phishing, social engineering, mobile security, privacy awareness and data handling?	☐ Employees/Users are not informed or trained.
	☐ Employees/Users are informed or trained informally.
	☐ All employees/users are informed and trained during their onboarding.
	☐ Employees/Users receive mandatory training upon hire and on an ongoing basis (at least annually). Attendance is tracked and non-compliance results in escalation to supervisor and/ or removal of the user's access. An information security development and improvement program is also used to complement security awareness training, which includes specific training reflecting the current threat landscape.
9. What background screening does your company conduct for employees, contractors, temps, interns or volunteers?	☐ None
	☐ Partial at hiring stage, based on needs of the role.
	☐ All during hiring stage.
	☐ All during hiring stage plus partial (selected based role type, level, or random) periodic rescreening

10. Has your company implemented a Data Loss Prevention (DLP) solution or similar controls to protect against data leaks?	☐ No solutions or similar controls have been implemented to protect against data leaks.
	☐ Some informal protections against data leaks are implemented.
	☐ The company has similar controls in place as part of its risk management program.
	☐ The organisation has a full Data Loss Prevention solution in place to inspect and detect potential unauthorised or unintentional transmissions of confidential data for all outbound communications.
11. Does your company continuously improve security processes?	☐ No processes exist to measure continuous improvement of security processes.
	☐ Informal processes exist to assess security processes and implement improvements.
	☐ Formal, documented policies and processes exist to ensure continuous improvement of security processes.
	☐ Formal, documented policies and processes exist to ensure continuous improvement of security processes. The company has applied a capability maturity model to enhance its abilities to reliably collect and use security measurement in a consistent and repeatable manner.
12. Does your company determine, document, implement and review audit and log records, so it can quickly recognise anomalies and detect/prevent malicious actors/activities?	☐ Neither internal audits nor third-party audits are performed for the company.
	☐ Some audit and log records are documented, implemented, and reviewed informally to ensure compliance to company policy.
	☐ Audit processes describe all aspects of the operations that are audited. These are designed to collect adequate evidence to prove that company policies are implemented.
	☐ Audit processes describe all aspects of the operations that are audited. These are designed to collect adequate evidence to prove that company policies are implemented. All audit processes are reviewed and updated on a regular basis to ensure that they incorporate additions to policies and/or new processes that have been implemented. Audit processing is automated and centralised.
13. Does your company analyse detected events as they arise to improve your organisation's risk mitigation capabilities and response plan?	☐ No analysis of detected events is conducted.
	☐ Analysis of detected events occurs on an ad hoc basis, or occurs without a formal analysis process.
	☐ Analysis occurs regularly and, once an anomaly is identified, it is verified and assessed to determine if further analysis/ tracking are needed.
	☐ Automated processes are in place for review, analysis, and reporting. The company correlates events and logs from across all areas of the organisation, including physical access controls, to improve company situational awareness.

14. Does your company aggregate and correlate information surrounding potential events from multiple sources to ensure it has collected as much evidence as possible to prevent future disruptions or an actual breach?	☐ No, event data is not aggregated or correlated from multiple sources.
	☐ Yes, individual host intrusion detection systems (IDS) aggregate and correlate event data from individual systems to a centralised repository.
	☐ Yes, individual host intrusion detection systems (IDS) are used. Log files and monitoring from multiple sources throughout the organisation are then aggregated and centrally correlated.
	☐ Yes, one or more centralised log file monitors are deployed on several different devices of the network, such as firewalls, routers, host IDS, network IDS, physical access controls, and application logs. These log file monitors aggregate and correlate event data so that multiple sources and sensors will automatically detect and alert appropriate parties when events occur.
15. Does your company maintain an Incident Response Plan?	☐ No formal plan exists in order to respond to cybersecurity events.
	☐ Response processes and procedures are informal, or only partially developed and implemented.
	☐ Response processes and procedures are documented, executed and maintained to ensure appropriate response to all detected cybersecurity events.
	☐ A comprehensive Incident Response Plan has been developed and approved by management. It clearly details the steps necessary to respond to events. Formal policies and practices are defined to establish the structure of the company Incident Response capability. The plan is regularly reviewed, updated and tested on a regular basis.
16. Does your company proactively investigate alerts from IT security related systems?	☐ Detection systems have not been implemented.
	☐ The company has implemented detection systems that generate notifications of suspicious activity, but no formal processes exist to investigate these alerts.
	☐ The company has implemented detection systems that generate notifications of suspicious activity, and members of the IT department follow established procedures to investigate and analyse these alerts.
	☐ Formal, documented processes and procedures for investigating notifications of suspicious activity from detection systems are executed and maintained by the cybersecurity team. Information gathered during investigation is reviewed for accuracy. Incidents are analysed and correlated between different parts of the organisation's repositories or detection systems to develop situational awareness.

17. Does your company maintain a disaster recovery plan (DRP) that is executed during or after a cybersecurity event?	☐ No disaster recovery plan exists. ☐ A disaster recovery plan exists and is informally executed after cybersecurity-related events. ☐ A disaster recovery plan exists and is executed after all cybersecurity-related events. ☐ A disaster recovery plan exists and is executed after all cybersecurity-related events. The plan is reviewed and maintained annually to ensure relevant updates of systems or assets affected by such events. Lessons learned from each event are used for continuous improvement.
18. Has your company identified a role that is accountable for data privacy?	☐ Yes ☐ No
19. Does your company maintain a data privacy policy that details the technical and administrative safeguards required to protect individuals' personal information?	☐ Yes ☐ No
20. Is your company able to identify all locations where personal data is stored within your company, including on internal servers and/or cloud storage, as well as those hosted by any third-party providers?	☐ Yes ☐ No
21. Does your organisation conduct regular backups of information, and are these maintained and tested regularly?	☐ There are no backup processes or procedures. ☐ Informal backup processes or procedures do exist but they are not documented ☐ Formal backup processes exist and are documented. Physical access to the backup data and information is restricted only to those authorised, and cryptographic protections are applied, both of which are defined within the organisation's security policies. Backups may also be held in secure off-site facilities. ☐ Formal backup processes exist and are documented. Physical access to the backup data and information is restricted only to those authorised, and cryptographic protections are applied, both of which are defined within the organisation's security policies. Backups may also be held in secure off-site facilities, which are assessed to ensure they have equivalent disaster resiliency, can ensure secure transportation and storage of information, and are located at a defined minimum distance from the organisation.