SENTIS
Managed Solutions

IT Guide for Manufacturers

Contents

Keeping up with (and utilising!) tech

Manufacturers know how important new technologies are to their operations. They have the power to boost consistency, accuracy, productivity and security, making for a more competitive business with increased sales and profits. The supply chain disruption of recent years, and its economic implications in the form of higher inflation, have also underlined the need for greater resilience. However, many manufacturers aren't sure where to start with new technology, even though it's essential that you **respond quickly to trends and continually innovate.**

When you're busy running a complex operation, finding the time to keep up with developments can be tricky. And with a myriad of options all claiming to be the next big thing, knowing which will deliver the results you need is no easy feat either. As such, outdated and underutilised technology has become the norm in manufacturing. So, we've put together these tips to help you harness the opportunities of technology.

The big focuses for 2024 & 2025

What you should be paying attention to.

Cloud

Systems are more secure and available when hosted in the cloud, which can reduce downtime, enhance productivity and mitigate risk

Automation

Processes are streamlined, leading to improved accuracy, efficiency and capacity to grow. Transform competitiveness and profitability

AI and machine learning

Predictive maintenance means no unplanned equipment downtime and cost-effective upgrades

CRM

Integrate with other systems for the full picture, and use insights to reinvigorate customer care, fostering loyalty and extending the customer lifecycle

The manufacturing IT Golden Rules

The nature of manufacturing means that benefits of new technology can be felt almost immediately. To ensure that your investments are well spent, and their positive effects felt across the entire operation, we recommend **working with an IT specialist** who will follow these three golden rules.

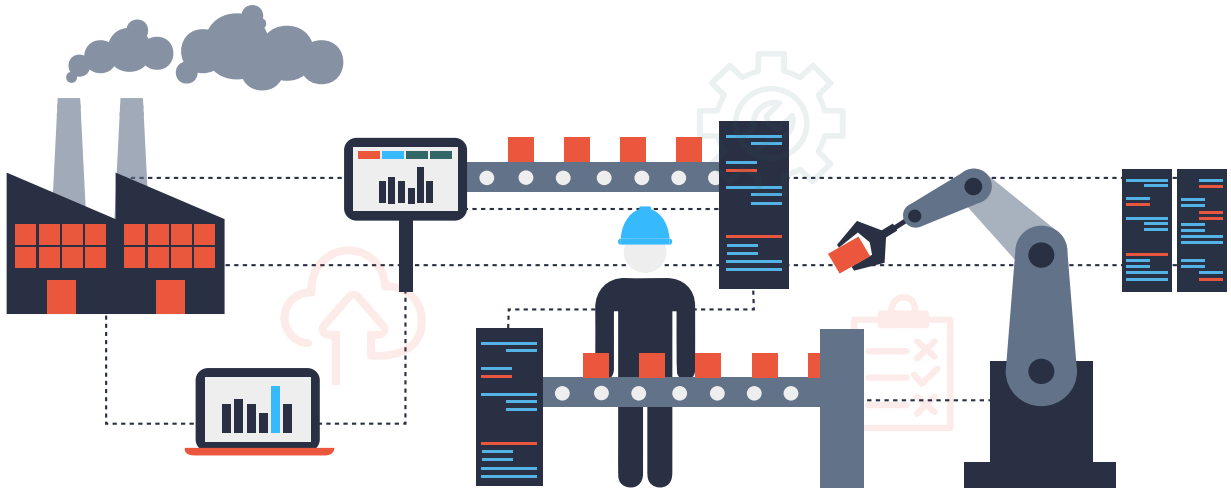
1. **Pick the right product.**
   Does it solve one or more problems and satisfy business objectives? Will it integrate with existing systems? Will it add value to secondary areas (such as customer service or distribution)? Depending on your business, you may need a multitasker, several independent pieces of software or a more radical change.

2. **Properly configure, straight away.**
   This will save costly remedial action later down the line, streamline the bedding in period and avoid disrupting the factory floor. There's nothing worse than having to rip something out and start again.

3. **Use it to its full potential.**
   Tech solutions are there to make things work smarter, but without your people getting on board, you face inefficiency and expense. An IT specialist will ensure teams are trained and start using new tech immediately.

At Sentis, we don't simply manage your ERP. Using our Six Sigma methodology, we go to great lengths to understand the inner workings of a business, and where challenges lie. The insights gained from this important preparation work allows us to deliver a strategic solution that focuses on improving processes and ensures that they work exactly as you want them to.

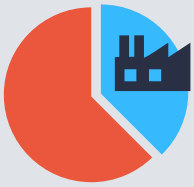
We work with a host of manufacturers to adopt a lean business process, lowering costs and resources associated with each step to ensure you stay competitive in today's increasingly challenging and technologically advanced market.



Book an IT audit 0345 862 2930 itaudit@sentisms.com

Cybersecurity and managing risk

The **manufacturing sector** is the **third most hit** by cyberattacks **in the UK**



Half of UK businesses reported a **cybersecurity breach or attack in 2023**

45% of manufacturers believe that they don't have the tools to ensure cybersecurity

59% of manufacturers have been asked to demonstrate **cybersecurity robustness by customers.**

Manufacturers operate in a state of constant and extreme vulnerability to the effects of a cyberattack. Reliant on IT for every aspect of operations – from machine programming to production, and dispatch to customer service – it's no exaggeration to say that a cyberattack can be disastrous for a manufacturer.

If successful, a cyberattack will render your systems inoperable, data inaccessible and customers unreachable. Infecting your network and corrupting the applications that power your operation, the worst-case scenario is a total shutdown until IT recovery is completed.

Depending on the cybersecurity measures in place at the time of an attack, recovery may take up to several weeks and even then, you may lose significant data. All the while you're haemorrhaging money by the minute with staff and suppliers on standby, orders unfulfilled and the costs of remedial action.

Hackers and other cybercriminals know the damage that they can inflict on a manufacturer all too well. This makes the sector an attractive target for ransomware attacks in particular, with perpetrators acutely aware of how desperate a manufacturer may become to resume business as usual.

With large sums of cash often being processed and a reputation for lacklustre cybersecurity, hackers also see manufacturers as easy targets for quick wins, deploying tactics such as phishing emails to fraudulently elicit cash.

Keep reading to find out how cybersecurity risk can be mitigated in any manufacturing business.

The must have cybersecurity software

Managed firewall:

Continual management, monitoring and advanced detection technologies ensure that your firewall is effective in preventing malicious activity from reaching your network, data and systems. Without this solution, you can't be sure it's performing.

Antivirus:

Intercepts harmful viruses and other malware from infecting and disabling your systems and business applications. Shields you from one of the most common cyberthreats.

Email filtering:

Identifies and blocks malicious email content such as infected files and some spam emails in real time, reducing network downtime and mitigating staff errors.

Web filtering:

Ensures that duty of care is in place while driving workforce productivity. Helps you to avoid advanced web-based threats from disabling both online and offline systems.

Anti - ransomware:

Provides an added layer of protection to network devices, protecting you from one of the fastest growing and most difficult to diffuse issues faced by manufacturers today.

Security patch management

Have you ever assumed that you're protected against cyberthreats because you have security software installed? Think again! Without updates, the same software that's meant to protect you from cyberthreats could actually increase your vulnerability.

A security patch management solution, like that offered by Sentis, provides a crucial management layer needed for effective IT security. With the click of a button, we get a complete view of your IT world, report on its status and identify any issues. A SaaS solution will also manage all updates and approvals automatically, streamlining this arduous but absolutely essential daily task.

If you do one thing...

Ensure that your staff receive robust, continual and up-to-date cybersecurity training. After all, the best tool in defeating the myriad of cyberthreats is an educated and united workforce. Staff training can help you to:

- ☑ Raise awareness of dangerous and manufacturing-specific cyberthreats
- ☑ Improve compliance and meet your customers' cybersecurity criteria
- ☑ Ensure that staff can recognise breaches, malware and other cyberthreats and respond appropriately
- ☑ Build a culture of security competence

The lifecycle to cybersecurity resilience

1 Auditing

To take successful action against cyberthreats, you first need to understand your current risks and blind spots. A Sentis IT audit will assess your situation, help to determine priorities and provide guidance about where to invest.

2 Configuration and design

Using audit insights, Sentis designs a robust cybersecurity solution that protects your entire IT estate. Unlike some providers, we map cybersecurity measures against business objectives and any associated risks - such as IoT or blockchain implementation.

3 Software solutions

Because cyberthreats are always advancing, so is the technology that protects your digital perimeter. Sentis continually invests in intelligent firewalls, anti-malware and filtering software tailored to your digital transformation strategy.

4 Awareness and monitoring

Greater visibility means greater control over your IT environment. With us you can supplement perimeter software with solutions that monitor databases, web traffic, emails and any vulnerable entry points. And, we'll fully integrate everything.

5 Backup and recovery

Robust backup and recovery saves you the worry of data or system loss disrupting your business. Sentis always recommends cloud-based backup and can help develop your disaster recovery plan.

6 Policies and education

Only policy, process and education will protect you from cyberthreats such as phishing. Implement rigorous, relevant and ongoing policies for maximum vigilance and resilience against attack. Ask us about training sessions.

7 Proactive maintenance

Your cybersecurity technology isn't worth much if it's not up to date. Sentis handles your upgrades, patch management and updates which are essential to software effectiveness and performance.

Book an IT audit 0345 862 2930 itaudit@sentisms.com

The 5-point guide to disaster recovery

Manufacturing is big business in the UK. It directly employs 2.7 million people, contributes 11% of GVA (gross value added) and accounts for 45% of total exports. Its uniquely diverse, collaborative and wide-reaching nature means that when disaster strikes, it's rarely just the manufacturer and end customer who are affected.

Ripples will be felt throughout the entire supply chain – from raw materials providers to distribution – and, depending how large or connected a business is, could potentially cause disruptions on a national scale. In the manufacturing world, hardware and software outages are significant problems, and loss of functionality or access is considered "disaster" territory.

How would your operation hold up if you lost everything – your network, servers, desktops, data, software and applications? For the most part, you'd essentially cease to trade (whilst still paying all overheads) until a solution was found.

Therefore, it's critically important to include IT disaster recovery (DR) in your business continuity plan. A disaster recovery plan outlines the steps you must take to recover and can be created using the following 5-point guide tailored to manufacturers.

1 Establish potential threat sources

Begin by mapping out likely sources of threat. This may include:

- **Weather or natural disaster.** These might be more prominent in rural or coastal areas
- **Fire or electrical failure** caused by faulty plant equipment or machinery
- **Human error.** Manufacturing sites are complex, so don't forget how easily mistakes can occur
- **Technology failures.** You're likely to have multiple sites for the various elements of your operation, all of which must coordinate with technology. A single outage could slam on the brakes
- **Crime, such as theft and cyberattacks.** Manufacturing sites are concentrated with high value goods, materials and finance, so are attractive targets for criminals

2 Complete a continuity analysis

Manufacturers commonly reside over a swathe of assets – equipment, various sites, and product. So, success depends on a quick revival from disaster, with as much data and functionality restored as possible.

Perform a business impact risk analysis for each site (including priorities) and analyse the equipment and policies reliant on technology, the applications you run, where data is stored and how long you could operate without IT. With this visibility you can understand the true risk to operations, service, supply chain stability, brand and profitability and the DR solutions required.

With health and safety being so key for manufacturers too, ensure any continuity analysis and subsequent DR solution accounts for how "disaster" is categorised. If colleagues can't work because of an IT failure, you're in the same situation as if you'd had production software outage.

3 Implement DR technologies

Contemplating backup and recovery solutions can be truly daunting for a manufacturer. There's so much interconnectivity and consequences for third parties beyond your four walls. However, cloud-based DR and DR as a service have made reliable, resilient DR accessible and affordable regardless of complexity or budget. Cloud-based services allow you to backup applications and data at desired intervals. Should a disaster occur, you or your IT partner can access everything required to get up and running again.

This can be done from anywhere, even if your physical sites are inaccessible. Offsite backup in robust, reliable data centres should also be considered. You'll know that your data is replicated and protected physically and digitally – and often for a lower cost than on-premise infrastructure which will present significant CAPEX spend.

4 Test your DR plan

If your DR plan is only that, you'll never know if it's fit for purpose. We've heard many stories of DR technology becoming obsolete before it's activated – not that we'd want you to experience a disaster! When your plan, technologies and services are finalised, test thoroughly and do so regularly.

Testing doesn't have to be an intimidating task – despite the common misconception that DR plan testing is time-consuming and daunting. At Sentis, we automate our clients' DR plan tests and run one every single night. You can rest easy knowing that your IT continuity is in order.

5 Assign responsible owners

If something does go wrong, you need to trust that everybody will jump into position. You may want to ensure the following functions are covered:

- Calling in a disaster to all staff, service providers and if relevant, customers
- Organising the logistics of staff relocation
- Assigning workloads remotely
- Leverage outside sources to set DR into action. Working with a specialist means you'll benefit from the advanced technologies not commonly available to manufacturers, such as DR apps and cloud-based DR

Maximising ERP investments

Enterprise resource planning (ERP) software is the backbone of any manufacturer – allowing you to run, manage and integrate business operations from a central point. But it's not just about keeping the lights on and the engines running. Your ERP can be a key player in helping you to grow and overcome several potentially disruptive manufacturing problems.

The data it collects, organises and analyses informs decision making at all levels of a company to provide a competitive advantage and reduce harmful silos. It goes without saying, then, that a lacklustre ERP can have the opposite effect. When was the last time you reviewed your ERP? It could easily be failing you in these five areas, putting you at serious risk of some major disruption.

- **Can't meet complex needs.**
  To sustain competitiveness, your ERP should be an intelligent workhorse.
- **Has unreliable integration.**
  Don't waste time and money using separate systems. Benefit from powerful automation instead.
- **Can't accommodate change.**
  The manufacturing industry faces rapid, frequent change. The right ERP will make this an opportunity, not a disruption.
- **Isn't configured for success.**
  No two manufacturers are the same. So, that out-of-the-box ERP will fall short and leave you at risk of cyberattack.
- **Is difficult to install and use.**
  Remove any unnecessary barrier to full utilisation – your operations and bank balance will thank you.

5 quick tips to help your ERP run smoother

It's not just the big changes that can make a significant difference. Follow this advice and speak to an IT provider specialising in ERP for manufacturing for an ERP that's always delivering on its investment.

1. **Server hardware.** Check that your ERP is tuned to your specification, paying particular attention to hard drives, memory and CPU. This planning and specifying applies whether you're using on-premise server hardware, or cloud-based hardware.
2. **Databases.** Ensure that indexes are set correctly, and queries are defined to achieve optimum performance.
3. **Network.** Test that your network, switch, cabling and WiFi is configured optimally throughout your entire business. It all has a knock-on effect.
4. **Remote users.** Check how users working outside of the office are opening your ERP. VPN or remote desktop may deliver better results.
5. **End user devices.** If possible, try not to invest the bare minimum. The devices used to access your ERP can have a big impact on productivity.

The future of ERP in a connected world

The expansion of digital transformation means that it's no surprise that ERP remains one of the most important technologies manufacturers have at their disposal. Here are the developments to pay close attention to in the next 12 to 18 months.

Making cloud work:

The manufacturing industry typically prefers an on-premise ERP. This is because the scope and complexity of activity in manufacturing often calls for a highly customised ERP that's pretty much built for your specific processes. With cloud being so dependent on connectivity too, business continuity could be put at risk from a simple internet drop out.

However, as cloud ERP technology becomes more reliable, customisable and resilient, it is certainly gaining traction. Even if it's not the right fit today, keep your eye on manufacturing-specific cloud ERP developments so you don't miss an opportunity that could really transform customer journeys, operational efficiency and productivity.

Digital transformation:

Integrated ERP implementations will become a key aspect of digital transformation strategies and therefore essential to ensure consistent performance and favourable profit margins. Manufacturers will consider ERP configuration and implementation as being just as important as other technology upgrades but this doesn't mean ripping things out and starting again every year.

Aligning ERP more closely with digital transformation is more about continually reviewing how it's helping to support your company in meeting its business objectives. This could mean more regular audits and more holistic analysis.

Moving on up to the cloud?

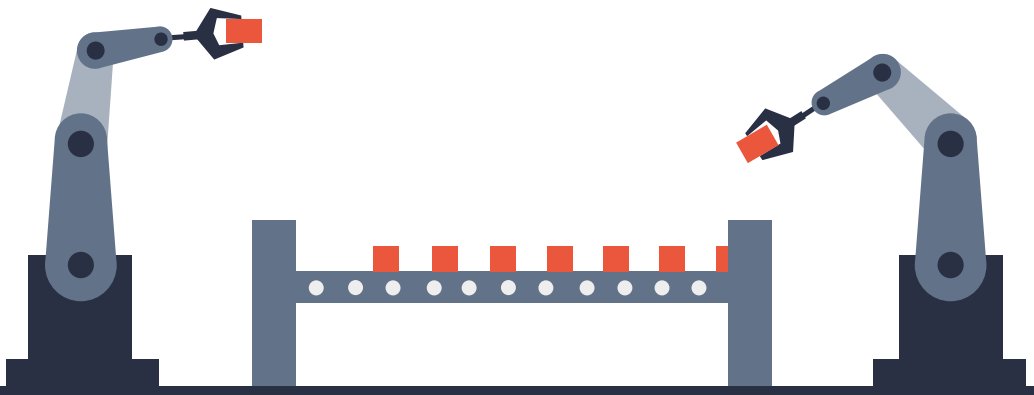
Even if your ERP is on-premise, the likelihood is that your business is moving in some way toward the cloud. Therefore, you need to consider how your ERP will integrate with cloud services and apps, and how this will seamlessly connect.

Integration is essential for efficient IT systems and in turn, an efficient business. But it also creates more doors. So, make sure that your cybersecurity is audited and accounted for at every stage of ERP planning. A provider like Sentis can even manage this on your behalf!

Smart manufacturing:

Rapid reactions and adaption are key to a manufacturer's success in a landscape that today, is changing more quickly, frequently and radically than ever in its history. As a result, manufacturers are increasingly adopting and integrating Internet of Things (IoT) devices, along with artificial intelligence and machine learning (AI/ML) technologies.

IoT and AI/ML integration is giving manufacturers access to unprecedented amounts of real-time data through ERP software, enabling them to make better, more data-driven decisions. This is helping to reduce errors, waste and downtime, boosting efficiency while also freeing up employees to take on other, less menial tasks.



Get started with transforming your IT

It makes sense to start from the beginning. So, we recommend getting an IT audit for your manufacturing business – and Sentis provides one for free, and with no obligations. We highlight where you can make improvements to enable efficient processes, remain competitive and build a robust cybersecurity defence in the process.

What will Sentis do?

- Explore your **applications**
- Establish where **data** is stored
- Analyse your **network**, infrastructure and recovery capability
- Calculate **how long you could live** without your IT
- Produce a **report** detailing our findings
- **Recommend** steps for the critical, short, medium and long term steps

> "A no-obligation IT audit confirmed some concerns that we had and more, with Sentis outlining in clear terms our current situation, strengths, risks and recommendations in the critical, short, mid and long term. Sentis' transparency, knowledge and willingness to go the extra mile gave me absolute peace of mind that I'd chosen the best guys. There was no doubt in my mind that they would deliver".

Emma Dixon,
Financial Controller at DataLase

To book a specialist manufacturing IT audit, please email itaudit@sentisms.com

As you'll know, being a manufacturer comes with a host of challenges that extend far beyond driving productivity and guaranteeing a quality product. Ethical, compliance and regulatory requirements have never been more complex and it's important that manufacturers understand the multitude of compliance factors that need to be implemented and managed in 2024 and beyond.

Compliance is changing manufacturing...

Workplace safety

Data security

GDPR protocols

Operational best practice

Business continuity and disaster recovery processes

Employing large numbers of staff in varying hands-on and high-risk roles across several locations means heavier regulation than most other industries - a reality that you'll be well accustomed to. Being awarded contracts and maintaining accreditations has always been dependent on meeting certain regulatory requirements but today, nothing can be taken for granted.

Rapidly advancing technology means that there's always new equipment and processes for staff to get to grips with, and safety protocols to meet on your part. Meanwhile, digital transformation and cyber attack prevalence has changed the landscape of business continuity and data security, leading to tighter contract requirements.

Manufacturers are now under persistent and increasing pressure to keep up with the pace of change, demonstrate ever-more precise compliance evidence and hold specific certifications in order to sustain business, remain competitive and avoid fines.

Our ERP and IT specialists

Our team are experts in preparing your IT landscape for change and ensuring that it's ready for ERP demands. We have worked to ISO27001, ISO9001, ITAR, ITIL and Prince 2 standards for many years and are unique in being a managed IT service provider with specialist, hands-on ERP knowledge too.

If you want to review your compliance measures, book a no-obligation audit with us today.

So, how can manufacturers intelligently manage this risk?

Compliance is first and foremost about safety. But it's also synonymous with competitiveness. Add these three important steps to your 2024 plan to ensure you're not left behind – or left with a nasty bill.

1. **Draft in a compliance expert to audit your operation** - and we don't just mean ticking boxes on a sheet. A consultant should go to great lengths to understand the inner workings of your business and should have considerable IT experience. They'll help you to implement a strategy that focuses on using IT to help meet safety requirements and achieve process improvements.

2. **Invest in cybersecurity and continuity:** The manufacturing sector is exceptionally vulnerable to cyberattackers looking to cause maximum disruption (in the hope of ransom), or to access the reams of valuable data and money circulating your IT systems. To maximise the opportunities of technology and to remain a relevant player, you must have effective cybersecurity and disaster recovery (DR) in place.

   If you're unsure about where improvements can be made, check out page 6 for your key manufacturing cyber security priorities, or page 9 to read our 5 point guide to DR in manufacturing.

3. **Get ISO27001 and ISO9001 certified:** Achieving ISO27001 and ISO9001 will help to give customers and prospects the confidence to give you their business and tick non-negotiable boxes in formal contracts – which are very much the standard. Without these two certifications, you'll face serious obstacles in winning orders and likely lose tenders.

   Today, the only way to make the grade is to demonstrate resilient and reliable business continuity and disaster recovery plan, watertight data security and stringent GDPR measures in addition to more traditional performance metrics such as quality, delivery and safety.

SENTIS
Managed Solutions

Do you have **cybersecurity concerns**, need to prepare your business for the future or want IT to work harder? **Find out where to start in enhancing performance and security with a free Sentis IT audit.**

Book a no-obligation audit today.

0345 862 2930 itaudit@sentisms.com www.sentisms.com