Sample Training Request Letter

Use the following sample request letter, or elements of it, to justify the time and budget required to complete SANS training to your manager. Simply copy and paste text into an email to your manager, then make any necessary adjustments to personalize the information. Once you hit send, you’ll be one step closer to gaining the skills required to protect your organization and advance your career.

**Subject: Request for cybersecurity training from SANS Institute**

[Decision Maker Name],

### I’m writing to request time and budget approval to take the SANS Institute’s information security course [AUD507: Auditing & Monitoring Networks, Perimeters & Systems](https://www.sans.org/cyber-security-courses/auditing-networks-perimeters-systems/) and its associated [GIAC Systems and Network Auditor (GSNA)](https://www.giac.org/certifications/systems-network-auditor-gsna/) exam.

**Why we need this course?**

Performing IT security audits at the enterprise level can be an overwhelming task. It’s difficult to know where to start and which controls should be audited first. Audits often focus on things that are not as important, wasting precious time and resources. Management is left in the dark about the real risk to the organization’s mission. Operations staff can’t use the audit report to reproduce or remediate findings. AUD507 gives the student the tools, techniques and thought processes required to perform meaningful risk assessments and audits. Learn to use risk assessments to recommend which controls should be used and where they should be placed. Know which tools will help you focus your efforts and learn how to automate those tools for maximum effectiveness. ***20 Hands-On Exercises***

**Once I’ve completed the course, I’ll be able to:**

* Apply risk-based decision making to the task of auditing enterprise security
* Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
* Conduct a proper risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
* Establish a well-secured baseline for computers and networks as a standard to conduct audit against
* Perform a network and perimeter audit using a repeatable process
* Audit virtualization hosts and container environments to ensure properly deployment and configuration
* Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
* Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
* Utilize scripting to build a system which will baseline and automatically audit Active Directory and all systems in a Windows domain
* Utilize scripting to build a system which will baseline and automatically audit Linux systems

**Which translate into business benefits for our company of:**

* Gain confidence in whether you have the correct security controls and they are working well
* Lower your audit costs with effective, efficient security audits
* Improve relevance of IT audit reporting, allowing the organization to focus on what really matters
* Improve security compliance while reducing compliance and security risks, protecting your reputation and bottom line

**Associated Certification:** [**GIAC Systems and Network Auditor (GSNA)**](https://www.giac.org/certifications/systems-network-auditor-gsna/)

The GIAC Systems and Network Auditor (GSNA) certification validates a practitioner's ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems. GSNA certification holders have demonstrated knowledge of network, perimeter, and application auditing as well as risk assessment and reporting.

* Auditing, risk assessments, and reporting
* Network and perimeter auditing and monitoring, web application auditing
* Auditing and monitoring in windows and Unix environments
* See the “Exam Certification Objectives and Outcomes Statements” section of the [**GIAC Systems and Network Auditor (GSNA)**](https://www.giac.org/certifications/systems-network-auditor-gsna/) page for a list of covered topics.

**Expected Cost**

I’d like to take AUD507 [fill in either: (1) “at [event name], from [start date] through [end date].” or (2) “online, with four months of access to the SANS OnDemand training platform.” or (3) “online, via Live Online from [start date] through [end date].”].

The attached unpaid invoice shows the cost of the course [retrieve this from the course registration page and attach]. Details include:

|  |  |
| --- | --- |
| Course fee  | [$X,XXX] |
| Subtract Early Bird / Online Training Discount | [-$XXX] |
| GIAC Certification fee | [$XXX] |
| OnDemand Bundle fee | [$XXX] |
| Travel and Hotel\* (for live training only)                            | [$XXX] |
| Meals (for live training only)                                                                     | [$XXX] |
| **Total estimated cost:** | **[$X,XXX]** |

\*Special hotel rates for conference attendees range from [$XXX]/night, but I must register before [xx/xx/xxxx].

**Testimonials**

**"AUD507 has obvious practical applications, and it's great to see some of the most infamous hacking methods explained and executed in real time. In the labs, I'm getting hands-on experience with the tools. The opportunity to learn how to interpret the results taught me more in one afternoon than I've picked up here-and-there over an entire career."** *- Tyler Messa, AWS*

**“The lab exercises were excellent because they provide knowledge, information and experience***.” – Amjad Awdhah Saeed Alshahrani, Site*

**"It's a ton of information that's applicable in the field, and not just theory."** *- Hatim Othman, Sony Interactive Entertainment*

I believe this course will substantially improve my ability to do the specific work we need. It’s written and taught by globally recognized experts and will deliver practical, hands-on training that I can apply as soon as I return to work.

Additional course information can be found on the SANS website at <https://www.sans.org/cyber-security-courses/auditing-networks-perimeters-systems/>

Thanks for your consideration,

[Add standard signature]

Attachment:

Unpaid Invoice for SANS training [find at <https://www.sans.org/cyber-security-courses/auditing-networks-perimeters-systems/> and attach to email]